00-0001919

RECEIVED
00 OCT -3 PM 12:09
DNF SAFETY BOARD

The Deputy Secretary of Energy
Washington, DC 20585

October 2, 2000

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

Dear Mr. Chairman:

Enclosed is the Department of Energy's (DOE) report addressing issues raised in the January 2000 Technical Report 25 – *Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities.* The Department acknowledges the concerns raised by the Board. This report outlines our actions that will ensure that software quality assurance is applied to DOE safety analysis and instrumentation and control (I&C) systems.

The Department's Chief Information Officer (CIO) and Lead Program Secretarial Officers will proceed with the initiatives to institute improvements in safety and software infrastructures, training, and safety analysis and I&C codes. One major action the Department has begun is the development of a DOE directive for Software Quality Assurance requirements and guidance. The directive will provide the authority and basis for guidance in developing software quality assurance programs at Department sites.

All actions are expected to be completed by December 31, 2001. Progress will be monitored and periodic reports will be provided to the Board. We appreciate the Board's support in this important matter. If you have any questions, please contact Nancy Tomford at 202-586-0166.

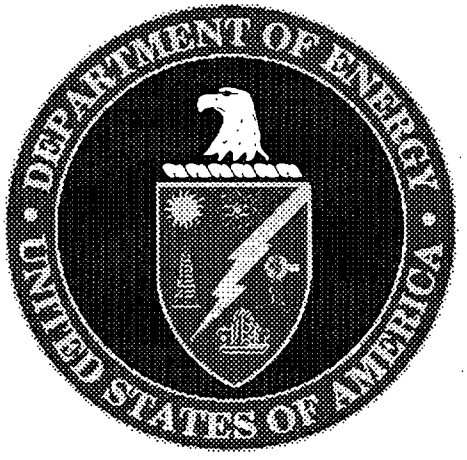
Sincerely,

T. J. Glauthier

Enclosure

00.1919

Department of Energy
QUALITY ASSURANCE FOR SAFETY-RELATED SOFTWARE AT THE DEFENSE NUCLEAR FACILITIES



June 2000

Department of Energy

QUALITY ASSURANCE FOR SAFETY-RELATED SOFTWARE

Table of Contents

Executive Summary

Safety analysis and instrumentation and control (I&C) software is used at Department of Energy (DOE) sites to help ensure safe operation of its facilities. DOE and its contractors perform hazardous work necessary for national security and for restoration of the environment at former defense nuclear production facilities. The performance of this work is of paramount importance to national interests, and it is equally important that this work be accomplished in a safe manner whereby the public, workers, and the environment are protected. Computer codes and their associated models and data are critical tools in fulfilling this important responsibility. Confidence in the adequacy of hazard, accident, and consequence analyses and the subsequent identification of preventive and mitigative controls can be impacted by the integrity of computational tools. Given the prominent role, it is imperative that a thorough and effective approach to guaranteeing their quality be implemented. This is the goal of software quality assurance (SQA).

SQA provides measures designed to ensure that computer software will perform its intended functions in a consistent and reliable manner and helps assure that software modifications will not result in unanticipated problems. SQA is an essential lifecycle process which must be applied during the systematic development, testing, documentation, maintenance, and use of software. In addition, SQA is a necessary element of an overall safety program.

In January 2000, the Defense Nuclear Facilities Safety Board (Board) released Technical Report 25 – *Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities* – that detailed some deficiencies in software QA and applications of it for safety analysis and I&C areas at DOE sites. While there are a limited number of safety-related I&C software systems, the in-facility I&C software systems add defense-in-depth in maintaining the facility authorization basis. Issues raised related to the fundamental physical models encoded in software for safety analyses. In addition, there were concerns with the use of codes in the performance of safety analyses because of an apparent lack of guidance and formal training of safety analysts. The Board felt these concerns are symptomatic of underlying deficiencies in the infrastructure supporting software quality at DOE.

In a January 20, 2000, letter to the Deputy Secretary of Energy, the Board requested a report from DOE that describes the actions that are needed to address the deficiencies and potential improvements identified in the Board's report and the schedule for completing these actions. In response, the Department has developed an approach that addresses the following issues:

- **Infrastructure.** The Board assigned a significant emphasis to the perceived lack of an adequate mechanism or effective infrastructure capable of providing oversight and enforcement with regard to software used for safety analysis (and supporting establishment of a sound analytical foundation for authorization basis documentation) and I&C. Section 2.0 discusses three actions for addressing this concern.

- **Software Quality Assurance Requirements.** The Board assigned the most emphasis to a need for a senior leader to accept responsibility for software quality assurance. The Chief Information Officer has accepted that responsibility and is developing requirements and guidance for software quality assurance for the Department which includes the National Nuclear Security Administration. This action is addressed in section 2.1.

- **Standards.** The Board found lack of an integrated and mandated or recommended comprehensive set of standards for ensuring quality software. The Board felt that DOE should clearly define requirements that are appropriate for use by its contractors. DOE does not entirely agree with the Board assertion that DOE does have requirements for software that is used in safety applications. However, DOE is investigating the Board's concern as discussed in Section 2.2.

- **Organization.** The Board found only intermittent linkage between individuals responsible for preparing safety bases and those who serve as the stewards of the software tools used in developing the safety bases. Also, there appeared to be inadequacies in information exchange for software quality assurance implementation. A study is underway to investigate the Board's concern as discussed in Section 2.3.

- **Training.** The Board felt that problems with the implementation and use of software codes partially resulted from a lack of training of safety analysts and I&C personnel on the use of analytical and I&C codes, respectively. A study is underway to investigate the Board's concern as discussed in Section 3.0.

- **Safety Analysis and I&C Codes.** The Board felt that problems with the implementation and use of software codes partially resulted from deficiencies in the software and inadequacies in the fundamental physical models encoded for safety analyses. Section 4.0 discusses actions for addressing this concern.

Table 1 summarizes the details of these actions to be taken by the Department to resolve these issues in response to the Board's concerns.

1.0 Introduction

1.1 Background

On January 20, 2000, the Defense Nuclear Facilities Safety Board established a requirement for a report from the Department of Energy (DOE) of actions needed to address the deficiencies and potential improvements identified by the Board in Technical Report No. 25 – *Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities*. The Board expressed concerns related to software quality assurance and the guidance and training for the execution of codes related to safety analysis and instrumentation and control (I&C).

The Deputy Secretary assigned John M. Gilligan, the Department's Chief Information Officer (CIO), as the lead in developing and implementing an appropriate DOE-wide response on these issues. The CIO secured the assistance of the DOE Quality Assurance Working Group, as well as safety and quality assurance personnel from several DOE and contractor organizations, and staff in the program offices for evaluation and corrective action on cross-cutting issues.

A core response team was established to review and discuss the issues and has developed actions and identified deliverables, which are summarized in Table 1. These actions and deliverables are proposed for the Board's review and comment. The core response team categorized the issues into three focus areas, (1) infrastructure, (2) training, and (3) safety analysis and I&C codes, and established three teams to address these issues. In particular, the need for a Departmental software quality assurance policy was also identified. This report describes the policy and the three focus areas.

1.2 Survey

To sufficiently address the Board's concerns, as summarized in the Executive Summary, a survey will be conducted to obtain input regarding specific topics in the three main focus areas. The survey will be reviewed by the Department's Field Management Council (FMC) and will be distributed Departmentwide to assure all facilities are addressed. The survey has been piloted at one of the nuclear sites, namely Savannah River Site, to demonstrate its usefulness and to obtain the level of effort to respond to the survey. The FMC coordination and notification to all affected organizations in the field should benefit from this pilot.

The survey is designed to capture information on the current SQA policies, requirements, programs, practices, or procedures that are being locally implemented at DOE nuclear facilities for the development and maintenance of computer software for use in safety analysis, appropriate application of that software, as well as for software used in facility or process control systems that are considered to be either a safety structure, system, or component (SSC) or defense in-depth feature. The survey requires input on specific computer modeling codes that are utilized by the safety analysts for the most common accident types such as fire, spill, and explosion. It will also

capture information pertaining to training of safety analysts and software personnel. It is intended to be directed at contractor organizations that are responsible for developing and maintaining the authorization basis documentation and operating DOE nuclear facilities.

2.0 Infrastructure

To summarize concerns expressed in the Executive Summary of Technical Report 25 – *"Quality Assurance of Safety-Related Software at Department of Energy Defense Nuclear Facilities"* – the Board expressed concern that there is no adequate oversight mechanism or effective infrastructure capable of providing oversight and enforcement with regard to software used for safety analysis (and supporting establishment of a sound analytical foundation for authorization basis documentation) and Instrumentation and Control (I&C) (including, establishment of authorization basis calculations). Following a review of the Board's Technical Report 25, it was determined that infrastructure areas that needed to be assessed are requirements, standards, and organization.

2.1 Software Quality Assurance Requirements

Stated in the letter transmitting Technical Report 25, the Board expressed concern that no senior DOE leader has actively accepted responsibility for the function of software quality assurance (SQA). The Board cites various Orders and guides, in particular, DOE O 414.1A QUALITY ASSURANCE and DOE O 200.1 INFORMATION MANAGEMENT PROGRAM. The Board's criticism of these Orders is that although they set forth broad requirements for quality assurance and a policy for lifecycle management of software (respectively), they lack a practical focus. Overall, the Board emphasized a concern for a lack of clear SQA policy and configuration management for safety-related systems.

The Office of the CIO has the authority and responsibility for software policy and oversight per the Clinger-Cohen Act. The CIO has developed a draft directive of SQA requirements and guidance using selected expertise in safety software within the Department and the Software Quality Assurance Subcommittee (SQAS). The requirements and guidance will be proposed for incorporation in a new or revised directive. The new or revised directive provides authority and direction for establishing SQA programs at DOE sites. Implementation of the directive is site-specific and shall be commensurate with the risk involved in developing and using the software (i.e., risk-based). It provides requirements that are conducive to actions necessary for implementing improvements in guidance, processes, standards identification, training, and code development and maintenance. The requirement provides a framework for sites and organizations to make decisions for what needs to be included in an effective SQA program. It specifies the level of SQA needed for all software and emphasizes a risk-based approach to SQA.

2.2 Standards

In Technical Report 25, the Board expressed concern that there is no comprehensive set of standards in place for ensuring quality software. In regards to industry standards for SQA, DOE has not formally promulgated guidance that clearly defines which of those requirements are appropriate for use by its contractors. They further stated that there is a lack of guidance for

safety analysts on the use of codes for performing safety analyses. Also, the Board referenced instances in which requirements for rudimentary SQA have been contractually stipulated, but did not flow down to implementation at the floor level. In addition, although some quality processes are conducted, overall they are fragmented or isolated. Possible resolutions or improvements provided by the Board included better documentation that would address consistent interpretation of parameter values, proper code utilization, use in bounding value calculations, postprocessors, use of industry standards, and a special emphasis on accident analysis codes and instrumentation and control (I&C) codes.

In response to the Board, regular management attention from local DOE offices and its contractors is necessary to implement SQA. Proper contract requirements and implementing processes based on DOE rules, Orders, guides and reference standards must be established. In addition, assessment of proper implementation must be performed by local DOE organizations. DOE O 414.1A, QUALITY ASSURANCE, states the requirements for DOE elements and contractors to develop Quality Assurance Programs (QAPs). Specifically, section 4.a(8) states, "The QAPs must discuss how it integrates and satisfies quality requirements or similar management system requirements (such as environmental or safety) from sources other than this Order." The Order directs organizations to develop an integrated management approach or system to show linkage among various organization functions and programs. Also, DOE G 830.120 was issued to implement 10 CFR 830.120, Quality Assurance; the guide clearly references the ASME NQA Part 2.7 for SQA. In addition, DOE O 420.1, FACILITY SAFETY, references standards required for certain safety applications, such as ANS-8.1-1983 that includes requirements for validating computer programs.

DOE contractors have been consistently apprised by DOE rules, Orders, and guides of their responsibility to apply nationally recognized quality assurance standards to their work involving software. Prior to DOE O 414.1A, DOE O 5700.6C, QUALITY ASSURANCE (superseded by DOE O 414.1A), stated that the quality criteria applied to all work and the items and services resulting from work. It referenced the national consensus standard ASME NQA-1, which included criteria for SQA. DOE O 1330.1D, COMPUTER SOFTWARE MANAGEMENT, (superseded by DOE O 200.1 INFORMATION MANAGEMENT) contained explicit requirements for software development, including quality assurance. DOE O 200.1 contains no explicit requirements for software development, but does refer to DOE G 200.1-1, SOFTWARE ENGINEERING METHODOLOGY.

Web sites have been established for the exchange of information. The DOE Technical Standards program promotes the use of non-Government standards across the Department and has established a web site at http://tis.eh.doe.gov/techstds/. The Office of the Chief Information Officer (CIO) has established a web site for promotion of Departmental Information Technology (IT) standards at http://www-it.hr.doe.gov/Standards/index.html and has published a DOE Information Architecture (IA) Profile of Adopted Standards. In addition, the Office of the CIO has a web site for Departmental guidance on Software Quality and Systems Engineering at

http://cio.doe.gov/smp and provides support for the web site for the Software Quality Assurance Subcommittee (SQAS) of the Nuclear Weapons Complex at http://cio.doe.gov/sqas.

To better understand where the current set of DOE directives may not adequately express DOE expectations or may not be appropriately applied, DOE will survey contractor SQA practices, and obtain data needed to identify areas where additional requirements are warranted. In addition, an evaluation will be conducted to identify a set of foundation standards that includes DOE and Nuclear Regulatory Commission (NRC) directives and describe how the standards would be applied based on benchmark data. Directives and practices regarding Integrated Safety Management (ISM) and DOE's Functions, Responsibilities, and Authorities Manuals (FRAM) will be reviewed.

The Office of the CIO has primary responsibility for identifying software standards and guidance, and the Office of Environment, Safety and Health (EH) has primary responsibility for identifying safety standards and guidance, including those for safety software. These two Offices will work together and prepare a report of the survey results with recommendations to the Lead Principal Secretarial Offices (LPSO) for additional guidelines, clarifications, or other improvement actions. Also, the results will be used to recommend any specific line management follow-up actions to the Deputy Secretary (e.g., special assessments, contract changes, Safety Management System enhancements).

2.3 Organization

The Board also expressed concern that there does not appear to be a formal linkage between individuals responsible for preparing safety bases and those who serve as the stewards of the software tools used in developing the safety bases.

To address the Board's concern, the DOE Quality Assurance Working Group (QAWG) is currently conducting a study to identify various organizations and groups which may not be designated by name as having quality assurance (QA) responsibility, but who implement or support some component of QA. The outcome of the study will be a report and an integrated matrix QA organizational structure within the Department. The QAWG will also identify established safety groups within the Department and determine how to enhance relationships and improve information exchange between those groups and QA.

The preliminary concept of an integrated matrix QA organizational structure will be plotted on a chart (matrix format) to identify interface/communication channels, working relationships, roles and responsibilities, sponsorship, and a central point-of-contact for resolving QA issues. The proposed matrix structure will show the QAWG as the central point-of-contact or central liaison organization, among other independent and interdependent organizations and groups. The QAWG may sponsor some groups. Some groups or organizations may have their own charter and sponsor, but still have a formalized working, communication, or reporting relationship with the QAWG.

Included in the study will be recommendations to improve information exchange among QA groups. The options may include identification and linkages of web sites, as well as maintaining support and instituting improvements in the working relationships between the Office of the CIO, QAWG, software quality assurance staffs, and personnel in safety analysis and I&C. The QAWG has established a web site at http://twilight.saic.com/qawg.

Early results of the study indicate that there may be more than twelve organizations or groups which could be depicted on the integrated QA organizational Structure. The major ones are the Office of the CIO, the Office of Environment, Safety and Health, QAWG, and SQAS. The CIO has the authority and responsibility for Departmentwide software policies and oversight. The Office of Environment, Safety and Health serves as the independent oversight organization and maintains responsibilities for DOE O 414.1A, QUALITY ASSURANCE, and various QA guidance documents that are non-software specific. The QAWG has overall responsibility for reporting on the condition of the Department's quality assurance program. The SQAS serves as a support organization for guidance of SQA across the nuclear weapons complex.

Also, there is an Energy Facility Contractors Group (EFCOG) formed by DOE contractors that has a sub-working group called the Safety Analysis Working Group (SAWG). Subcommittees within the SAWG address topics related to safety analysis methods and training. They provide annual training courses on accident analysis codes and methods. The SAWG has established a web site at http://www.efcog.org/wg/sawg/index.htm.

Action 1.0: Develop an SQA directive

Responsible Manager: Chief Information Officer (CIO)

Deliverables: Letter to the Board announcing placement of draft directive into the Directives System for DOE-wide review.

Due Date: October 16, 2000

Action 2.0: Identify industry safety and SQA standards used by the field (e.g., policies, requirements, and guidance).

Responsible Manager: EH and CIO

Deliverables: A list of Recommended Standards to the LPSOs.

Due date: October 30, 2000

Action 3.0: Evaluate survey results to confirm and/or identify policy/standard changes needed for SQA and safety.

Responsible Manager: EH and CIO

Deliverables: Survey results, Summary Report of Analysis with Recommendations for Improvements to the LPSOs.

Due date: November 30, 2000

Action 4.0 Develop and formalize a matrix of organizations (and identify coordinating points) cognizant of QA and capable of addressing issues as they are identified.

Responsible Manager: Chairman, QAWG

Deliverables: Revised QAWG Charter, Integrated QA Organizational Structure Matrix, Summary Report of Analysis with Recommendations to the LPSOs.

Due date: November 30, 2000

3.0 Training

The Board addressed a lack of a formal program for training Federal or contractor personnel who perform safety analysis or oversight functions. They concluded that issues of implementation and use of software partially resulted from a lack of training of safety analysts and instrumentation and control (I&C) personnel on the appropriate use of analytical codes for performing safety analysis and applying I&C software to assist in the control of DOE facility processes. Related to this concern is the degree of training by SQA staffs in the safety analysis and I&C systems.

In addressing the Board's concerns, it was ascertained that there are three basic issues related to training:

1. What training is currently provided by DOE facilities to personnel involved in development or use of software, especially software for safety-critical applications?

2. What training is available to DOE facility employees in the event DOE determines that its personnel need more training in SQA or in the use of safety-critical software, and what mechanisms exist to implement this training?

3. What are the training requirements and practices implemented at other safety-critical facilities for software development or use?

Preliminary investigation reveals that some training is being provided on SQA and software usage. In general, DOE neither controls nor establishes specific training requirements for contractor personnel. There is a general requirement in QA orders, among others, that contractor personnel are trained to perform their jobs. Issuance and implementation of the proposed directive on SQA will be a major step towards this goal. As it becomes apparent that SQA is part of safety analysis and other related job functions, it is expected that appropriate training will be added to the contractor's requirements.

In addition, there are a number of web sites, working groups, and other mechanisms to disseminate training issues, DOE's expectations, and best practices. Some are as follows:

> DOE safety training program has been established by the Office of Environment, Safety and Health. The program is available on a web site at http://www.pnl.gov/eshs/training.html.
>
> The Federal Technical Capabilities Board establishes general training requirements for DOE personnel involved in facility operations and safety oversight. Contact has been make with this Board. A proposal can be developed and submitted to this body to include software-specific elements in the required training once these elements are defined.

The database of existing training at the DOE Clearinghouse for Technical Education and Training (CTED) (http://cted.inel.gov/cted/) includes a number of courses related to SQA, hazard analysis, and safety analysis reports. This database provides a method to disseminate courses or work with the sponsors of existing courses to incorporate necessary software elements in training.

The Energy Facility Contractors Group (EFCOG) provides computer model training at its Annual Safety Analysis Workshop. During the past workshop in April 2000, four- and eight-hour training programs were conducted for four of the computer models used for safety analysis supporting DOE facilities. Included were GENII, RadCalc, MACCS2, and RSAC-6. Other training sessions were held to provide an overview on appropriate methodology and sources of data for accident analysis. The four days of training are designed to help ensure that safety analysis software and other tools and methods are used correctly to maintain a well-founded, accurate safety envelope.

Others include SQAS, the Quality and Safety Management Special Interest Group, and the QA Working Group.

These groups are aware of the issues raised in the Board's report. This awareness is the first step in ensuring that contractor training is evaluated and modified, if necessary, to be appropriate to the task involved.

With respect to benchmarking related training and requirements in other organizations, several organizations have been identified and contacted. These include the Nuclear Utilities Software Management Group (NUSMG, http://www.nusmg.org), National Aeronautical and Space Administration (NASA), Defense Threat Reduction Agency (DTRA), Department of Defense (DOD), and the Center for Chemical Process Safety (CCPS). There is no specific Nuclear Regulatory Commission (NRC) requirement for SQA training, other than a general requirement that people be trained appropriately for their job function. This approach is similar to the existing DOE training expectations.

DOE will survey to obtain details on current practices and obtain data for identifying the need to establish a standardized and minimum level of training requirements for personnel using software associated with safety analysis (primarily accident and consequence analysis) and I&C systems. Departmental practices concerning training and competency requirements for personnel using or reviewing application of computer codes for facility design and safety analyses, as well as I&C functions, are being reviewed. An assessment of the adequacy of SQA training available to Department staff and an identification of current processes designed to train users and reviewers with SQA standards will be conducted.

In addition, Departmental training practices and standards will be compared with current practices implemented by DOE contractors, as well as those employed by other Federal agencies and the commercial nuclear and chemical sectors. These comparisons will identify the areas to be

targeted to yield the most benefit in improving personnel training and competency for accident analysis and I&C areas.

Action 5.0: Identify appropriate types and levels of SQA training commensurate to the requirements of the safety analysis and I&C functions performed. Compare to current training programs available at DOE. Calibrate DOE SQA training practices with industry and those maintaining similar mission-critical facilities and processes in the nuclear and chemical sectors. The comparison would identify areas where additional emphasis is needed to correct deficiencies, or reduce "gaps".

Responsible Manager: EH and DP

Deliverables: Survey results, Summary Report of Analysis with Recommendations for additional guidelines, clarifications, or other improvement actions or a Profile of Training Requirements will be provided to LPSOs.

Due date: November 30, 2000

4.0 Safety Analysis and Instrumentation and Control (I&C) Codes

The major area of concern highlighted by the Board with respect to the use of computer software is in support of safety analysis and instrumentation and control (I&C) system processes for nuclear facilities in the DOE Complex. This section will identify the key requirements for software performing a safety-related function articulated by the Board, and provide background on the context for software use to support the overall safety basis and reflect sound Integrated Safety Management (ISM) practices. Then, the issue of centralizing safety-related software expertise and the dissemination of information is discussed. The software survey is noted as a mechanism to collect field information – the interpretation of information from responses is covered, and its use outlined. Finally, actions to be taken are identified.

4.1 Role of SQA in Safety Analysis and I&C Software

Technical Report 25 noted that computer codes play a prominent role in ensuring safe operation of DOE facilities. Furthermore, the Board indicated that a thorough and effective approach to guaranteeing software quality and appropriate use is imperative. In particular, the Board stated that SQA applied to safety-related functions should assure that:

- The numerical models are a valid representation of the physical phenomena of interest for the appropriate variables and within a defined applicable range (verification).
- The fundamental data used in the code are appropriate for the intended function.
- The results obtained when using the code within its established range of applicability are in reasonable agreement with available experimental benchmark data, other reference phenomenological data, alternative computer model predictions, or other independent data applicable (validation).
- Modifications of and improvements to software is tracked and documented in a central registry so that users will be aware of changes, physical and mathematical assumptions, and limitations of their analysis.
- Computer models are properly executed by safety analysts to support the authorization basis of the facility, and that the safety envelope is understood and appropriately interpreted. This understanding subsequently provides confidence that identified control sets are sufficient, and the safety basis is conservative.
- Principles comprising an acceptable set of applicable SQA standards flow down and are implemented in actual I&C systems.

The Board also suggested in Technical Report 25 that problems with the implementation and use of software for safety analysis and I&C functions partially resulted from deficiencies in the software and limitations of encoded physical models. The Board commented that a thorough and effective approach to maintaining sufficient software quality levels was needed. Improvements in the management of the codes that includes computer model support and guidance, adherence to software standards, configuration management, assessment of appropriate usage, audits, and training were suggested.

The Board stated that it was not considered appropriate that all safety analysis and process control software undergo a program to upgrade the SQA level. Specifically, the role of the software, the nature of the facility, and the site-specific requirements should be considered to determine the appropriate SQA level. However, software upgrades should be explored particularly for software that is widely applied in support of authorization basis documentation of DOE nuclear facilities.

In this regard, the concept of maintaining a set of computer software, or "tool-box", was suggested by the Board. This was defined as a tool-box of codes as a small number of standard computer models having widespread use and sufficient pedigree, that they are maintained, managed, and distributed for implementation by a central source. The tool-box software would constitute the top priority for focusing limited resources on pedigree upgrades, maintenance, and distribution to safety analysts and DOE reviewers.

4.2 Overall Safety Context

With respect to the operation of DOE nuclear facilities, safety-related software is undoubtedly an important aspect in building and maintaining a defensible, conservative authorization basis and for operating facilities safely. With respect to maintaining the safety basis, however, application of software and interpretation of results constitute only part of what should be a larger, integrated picture. There are many other factors to be considered in assuring safety at nuclear facilities and operations.

An adequate, technically defensible safety basis is in part described through Departmental Orders and underlying standards. The key Orders and Standard in this regard are:

- DOE O 5480.21, UNREVIEWED SAFETY QUESTIONS
- DOE O 5480.22, TECHNICAL SAFETY REQUIREMENTS
- DOE O 5480.23, NUCLEAR SAFETY ANALYSIS REPORTS
- DOE O 420.1, FACILITY SAFETY, and
- DOE-STD-3009-94, Preparation Guide for U.S. DOE Nonreactor Nuclear Facility Safety Analysis Reports.

The overarching philosophy is that of applying safety analysis and safety-related design software in the context of Integrated Safety Management (ISM) principles and guidelines. In the ISM

context, the line management has the responsibility of assuring safety. The DOE line managers are responsible for ensuring the contractors prepare adequate and defensible safety analyses. The safety analyses should systematically identify and analyze the hazards, quantify the source term and impacts of postulated accidents, and establish appropriate preventive and mitigative controls. To conduct these analyses, computer modeling is sometimes required to characterize the accident phenomenology and to estimate potential consequences. Consequence estimation is used primarily for the determination of Safety Class structures, systems, or components (SSCs) (DOE-STD-3009-94, Appendix A). One of the major areas of concern is whether the subsequent safety classification of required systems is made correctly, and with sufficient safety margin.

DOE personnel rarely develop or use the computer codes for performing safety analyses. DOE, however, is responsible for reviewing and approving safety basis documentation prepared by the management and operating (M&O) contractors. Since DOE has not formally "licensed" the codes that are used in safety analysis, code usage and associated results are reviewed for their technical accuracy or appropriateness as part of the safety analysis review process. DOE-STD-3009-94 provides guidance in terms of what is minimally expected to document when computer modeling is used in performing accident analyses.

4.3 Safety Analysis Software Group

The management of the safety analysis function and the organization of technical staff at M&O contractors in the DOE nuclear complex vary considerably. The spectrum spans a centralized safety analysis (or authorization basis) organization to individual facilities each relying on outside consultants. Since there are a large number of widely scattered analysts performing safety analyses, it is desirable to establish a centralized group with coordinated support from the EFCOG. A centralized group, to be comprised of DOE, contractors, and subject matter experts, would necessarily contain expertise in safety analysis, software development, and SQA, and authorization basis implementation. Its function would be to take a leadership role for DOE and its contractors in the specific safety-related software areas of concern highlighted in Technical Report 25. This group shall be identified as the Safety Analysis Software Group (SASG). The Group will be chaired by the National Nuclear Security Administration (NNSA/DP) subject matter expert.

The SASG shall provide:

- Leadership in safety analysis, design, and I&C software issues relating to safe design and operation of DOE nuclear facilities
- A mechanism to identify, address, and disposition major software issues that have cross-cutting impact across the DOE Complex
- Identification of support mechanisms and resource allocation from stakeholder contractors and line organizations in the Department

4.3.1 Survey Assessment

The survey is targeted at DOE M&O and laboratory contractor organizations responsible for safety analysis and facility management and is expected to provide the information necessary to determine the adequacy of DOE contractor's SQA practices, processes, and procedures for the development, maintenance, and usage of safety-related software. These identified practices, processes, and procedures will be compared to those promoted by the Software Quality Assurance Subcommittee (SQAS) and the working group on policy. The survey will also be a tool to flag areas for improvement in the application or use, or verification and validation, of software supporting: (1) safety analysis; (2) in-facility or process control systems that are categorized as safety SSCs, and (3) I&C software used for training. The results of the study will be useful to other components of the Department's action plan, specifically, infrastructure and training.

An initial task to be undertaken by the SASG is the review and assessment of the survey response from the field. It is expected that the responsible Program Secretarial Officers (PSOs) or DOE field organizations to ensure the survey responses from their contractor organizations are complete and accurate. Data obtained from the survey will be used to assess the degree of reliance on computer modeling for developing the safety bases for nuclear facilities. Category 2 facilities are expected to warrant the most frequent application of safety-related software. Conversely, Category 3 and lower facilities would merit relatively few applications of the same-level sophistication in software.

Upon receipt of all validated survey information, the most commonly used software would be earmarked as candidate software for the software tool-box. The SASG will perform an initial assessment of the adequacy of the software based on the following criteria:

- Model fidelity and fitness for various accident scenario and phenomenology types
- Software pedigree and level of SQA
- Confidence in local installation at the sites involved
- User-software metrics (user interface, software documentation and guidance on input and appropriate data sets).

The determination of tool-box software adequacy and individual site applications may require an onsite technical review. Based on the initial assessment, the SASG will determine any specific need to conduct additional onsite reviews. Onsite reviews will be fully coordinated with the affected PSO or field organizations prior to the visit. Based on the survey results, review of pertinent safety-related software standards, and potential site visits, the SASG would be able to determine the impacts of the use of candidate software relative to the authorization basis for the facilities in question. An initial set of actions based on the software-site assessment is discussed in Section 4.6.

4.3.2 Remedial Actions

Identification of high-use software through the survey results shall be integrated with relevant software standards in the field. The purpose of this action shall be to determine specific remedial activities necessary to upgrade non-compliant safety-related software. For example, given the widespread use of the MACCS2 code for authorization basis calculations, it is anticipated that this model will be a candidate code for the tool-box. However, given the documented deficiencies of the MACCS2 code, a concentrated verification and validation effort will need to be performed. SASG representatives will outline the basic program for MACCS2 and determine schedule and resource allocation to bootstrap MACCS2 into a level of compliance commensurate to safety-related software standards.

Other candidate codes shall be assessed individually. The SQA improvement activities will necessarily be tailored to the deficiencies of each code. As each code is brought into compliance, the software will be placed into a configuration management program to maintain its pedigree. The tool-box in this manner will evolve to a manageable number of one to two codes for each phenomenological area (e.g. fire, spill, deflagration/detonation). The survey will be a major, but not the sole source of software use information to populate the tool-box. The SASG will also review the findings and recommendations from the Accident Phenomenology and Consequence (APAC) Evaluation Project. Although somewhat dated in the "snapshot" taken of individual code status, the APAC Project reports are invaluable in providing screening criteria in technical model adequacy, user interface and SQA, source term applicability, as well as other code-to-code test problem comparisons.

Whether MACCS2-based or otherwise, the SASG will identify the potential deficiencies of the tool-box codes and develop plans necessary to correct and remedy the problems. However, the determination of a site or facility specific safety impact or remedial actions will have to be made by the responsible DOE line management organizations. The SASG will be available to provide technical support to each PSO or field organization impacted to develop compensatory measures, based on the Unreviewed Safety Question evaluation process or other viable means, for those cases in which authorization basis deficiencies have been identified as a result of using a tool-box code. Compensatory measures may include independent recalculation using alternative methods, computer models, or engineering judgment. Some cases may require imposition of additional controls. It is, however, important to recognize that there may be a number of other deficiencies (non-code related) with respect to the overall quality of safety analysis reports and other authorization basis documents. In these cases, it would be prudent to prioritize specific commitments or actions based on their relative importance to improving the quality of authorization bases at each of affected nuclear facilities through existing safety analysis upgrade or annual update efforts.

4.4 Training and Information Enhancements

Use of safety-related software and the integration of these tools into the overall context of safety analysis has been discussed earlier from the perspective of training. It is also noted that the chief forum to provide cost-effective training on methods and use of software in this field is through the Department of Energy Facility Contractors Group (EFCOG) and its Safety Analysis Working Group (SAWG). The SAWG convenes an annual conference on issues pertinent to safety analysis in the DOE nuclear complex.

A cross-linked initiative should be undertaken to pilot an integrated accident/consequence analysis training course. This would contain best practices and other guidance for DOE safety analysts who are responsible for performing hazard, accident, and consequence analysis upon which the identification of control sets is based. The proper timing for this training is during SAWG's annual workshop. The pilot course to be offered at the next EFCOG SAWG Workshop would include testing to evaluate trainees in mastery of predefined enabling objectives. Upon completion of the pilot and evaluation of the pilot, a permanent offering of the material could be planned on a regular basis.

To remedy the lack of any formal reporting mechanisms, DOE shall use existing safety analysis Internet links to inform users of safety analysis issues. Software user alerts will be communicated via the EFCOG Safety Analysis Working Group website (http://www.efcog.org/sawg). This website will also serve to:

- Provide lessons learned in the application of codes in safety analysis
- Share benchmark data and test problem sets
- Maintain site-specific data sets such as site distances, meteorological data, etc.
- Message board features that communicate software news and developments, and user feedback.

4.5 Longer-Range Planning

As part of its advisory activities, the SASG will have responsibility for identifying model improvements, and recommending new software development. This activity will incorporate not only DOE applicability and needs, but reference "like" facilities and safety basis analytical support modeling advances found in commercial industry. The SASG will work with the EFCOG to ensure that the newer versions of tool-box software are placed into the proper configuration management, that users are notified of changes, and earlier versions are retired. This process will follow software lifecycle protocol, per standards identified by the SQAS and the working group on policy.

The initial activities by the SASG will eventually be the basis for a permanent expert and advisory team in a DOE nuclear national laboratory. As needs and specific issues arise, the advisory team will change in numbers and associated skill mix to meet these challenges at the appropriate level.

4.6 Safety-Related Software Actions

Several actions are required to meet the goals of this section. The survey and the creation of a Safety Analysis Software Group are critical to meeting these end-point objectives.

Action 6.0: A memorandum from the Deputy Secretary will be sent to the Under Secretary (NNSA) and to Assistant Secretaries (EM and EH) to establish an initial Safety Analysis Software Group (SASG) to evaluate survey results and to assess requirements, attributes, and selection of tool-box computer models for accident and consequence applications. The group will be led by the NNSA representative.

Responsible Managers: NNSA/DP, EM, EH

Deliverable: A memorandum tasking NNSA, EM and EH to form the Group and to identify required DOE, contractor, and consultant representation for Safety Analysis Software Group. Develop selection criteria for tool-box codes. Identify software candidates for tool-box and outline remedial SQA activities for the tool-box codes

Due Date: September 30, 2000 for SASG establishment and **December 15, 2000** for the analysis results and recommendations.

Action 7.0: Identify software used for safety analysis and I&C processes. Compare practices and training for these codes and software. Analyze for deficiencies and improvements.

Responsible Manager: Chair, Safety Analysis Software Group

Deliverable: Survey results, Summary Report with Analysis and Recommendations for additional guidelines, clarifications, or other improvement actions and/or Profile of Safety and I&C Codes will be provided to affected PSOs

Due Date: December 29, 2000

Action 8.0: Safety Analysis Software Group (SASG) determine if any site visits are required to finalize the tool-box codes.

Responsible Managers: Chair, SASG

Deliverable: Conduct visits and make recommendations on the tool-box codes

Due Date: March 1, 2001

Action 9.0: Conduct Pilot Integrated Accident/Consequence Analysis Training.

Responsible Managers: EH/NNSA-DP

Deliverable: Provide pilot training at EFCOG SAWG Workshop on hazard, accident, and consequence methods.

Due Date: June 16, 2001

Action 10.0: Determine whether Safety Analysis Software Group (SASG) needs to be transitioned to a permanent organization.

Responsible Manager: Chair, SASG

Deliverable: Letter memorandum to LPSOs on permanent organizational make-up, roles and responsibilities and cross-ties to EFCOG

Due Date: July 31, 2001

Action 11.0: Perform backfit SQA program for MACCS2.

Responsible Managers: Chair, SASG

Deliverable: Provide SQA program documents and put required pedigree MACCS2 software into configuration control as initial code into DOE Software Tool-Box.

Due Date: December 31, 2001

Table 1 – Summary of Actions and Deliverables			
Action	**Responsible Manager**	**Deliverables**	**Due Date**
1.0 – Office of the CIO with Department expertise to develop an SQA policy.	Office of the CIO	Letter to the Board announcing placement of draft directive into the Directives system for DOE-wide review	October 16, 2000
2.0 – EH and CIO to identify industry safety and SQA standards used by the field (e.g., policies, requirements, and guidance) and identify a set of foundation standards and describe how the standards would be applied based on benchmark data.	EH and CIO	List of Recommended Standards	October 30, 2000
3.0 – EH and CIO to evaluate survey results to confirm and/or identify policy/standard changes needed for SQA and safety.	EH and CIO	Survey results Summary Report with Recommendations for Improvements and/or a Profile of Standards to the LPSOs	November 30, 2000
4.0 – Chairman, QAWG, to identify QA groups and prepare Integrated QA Organizational Structure matrix.	Chair, QAWG	Revised QAWG charter Integrated QA Organizational Structure matrix Summary Report with Recommendations to LPSOs	November 30, 2000
5.0 – EH and DP to identify SQA training needed to do SQA on safety analysis and process codes commensurate to the usage and safety functions performed, and identify areas for improvement.	EH and DP	Survey results Summary Report with Recommendations and/or Profile of Training Requirements to LPSOs	November 30, 2000

Table 1(Continued) – Summary of Actions and Deliverables			
Action	**Responsible Manager**	**Deliverables**	**Due Date**
6.0 – Establish Safety Analysis Software Group (SASG)	NNSA/DP	List of Department, contractor, and consultant personnel Board staff member invitation Meeting schedule. Identify candidate software for Tool-box.	December 15, 2000
7.0 – Assess software used for safety analysis and I&C processes and analyze practices and training for improvement	Chair, SASG, EM, EH	Survey results Summary Report with Recommendations and/or Profile of Safety and I&C Codes to LPSOs	December 29, 2000
8.0 – Visits to Sites having Most Category 2 Facilities	Chair, SASG, EM, EH	Assess impacts to Authorization Basis for Sites visited in report to LPSOs. Recommend compensatory measures as needed.	March 1, 2001
9.0 – Pilot training at EFCOG SAWG Workshop	NNSA/DP, EM, EH	Conduct pilot methods on integrated hazard, accident, and consequence methods Reformulate if necessary. Provide annually as lessons learned review recommends	June 16, 2001
10.0 – Transition Accident Analysis Software Group to permanent stature as part of field organization	Chair, SASG, EM, EH	Letter memorandum to LPSOs.	July 31, 2001
11.0 – Perform Backfit SQA program for MACCS2	Chair, SASG, EM EH	Issue SQA Documents Put MACCS2 into Configuration Management under control of SASG/SQAS	December 29, 2001