Summary Report on Standards
to Department of Energy (DOE)
Lead Principal Secretarial Officers (LPSO)

Response to
Defense Nuclear Facilities Safety Board (DNFSB)
Technical Report 25, Focus Area No. 1 – Standards
Software – Safety Software – Safety Analysis

April 14, 2001

by
Standards Focus Area Team
Developed under the auspices of the
Office of the Chief Information Officer and the
Office of Environment, Safety and Health

Table of Contents

Attachments

Executive Summary

To address the concerns presented by the Defense Nuclear Facilities Safety Board (DNFSB) in Technical Report 25 "*Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities*", a Response Team was formed in February 2000. The Response Team was led by the Office of the Chief Information Officer (OCIO) and composed of participants from National Nuclear Security Administration/Defense Programs (NNSA/DP); Environmental Management (EM); Environment, Safety and Health (EH); and other Principal Secretarial Offices (PSO). The Response Team developed a three-pronged approach which investigated Infrastructure, Training, and Safety Analysis and Instrumentation and Control (I&C) codes. Three subteams were formed to address each of these focus areas. The Infrastructure Focus Team divided its efforts into three areas to review Software Quality Assurance (SQA) Requirements, Standards, and Organization.

This report is a Departmental perspective in regards to Standards for software, safety software, and safety analysis. Although discussed, this report does not endorse or provide consensus standards or guidance in regards to DOE safety analysis and I&C codes. The Safety Analysis Software Group (SASG), led by NNSA/DP, EM, and EH, will address this software and issue a report. The intent is to review the DOE standards programs and compare with standards of other government and industry organizations.

In summary, the Board stated a concern that there is a 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 did not entirely agree with the Board assertion that DOE does not have requirements for software or software quality, particularly for software that is used in safety applications. However, a study was undertaken by the Standards Focus Area Team (a subset of the Infrastructure Focus Team) to assess the Department's guidance for these standards; and a survey was developed to focus on standards for safety analysis and I&C codes in defense nuclear facilities.

This report is a compilation of the study and survey results. It is intended to be used as a resource by the SASG and others involved in managing, engineering, or assuring DOE software.

1.0 Standards Focus Area Description

The Standards Focus Area Team's direction was to review and assess directives and standards guidance for safety software, safety analysis, and software quality assurance (SQA) to ensure the pedigree of all DOE software, particularly safety software, and to understand the use of these standards on safety analysis and instrumentation and control (I&C) software. This review and assessment is focused at the Departmental level. Although discussed, a similar review will be conducted by the Safety Analysis Software Group (SASG) to specifically address safety analysis and I&C codes.

An independent evaluation by the Standards Focus Area Team was conducted to identify a set of foundation standards that could include DOE and other government and industry directives and to describe how the standards would be applied based on benchmark data. Attachment 1 lists the organizations reviewed and Attachment 2 lists the DOE directives and standards currently required. Directives and practices regarding Integrated Safety Management (ISM) and DOE's Functions, Responsibilities, and Authorities Manuals (FRAM) were included in the review. In addition, to determine whether the current set of DOE directives adequately address DOE expectations and are appropriately applied to safety analysis and I&C software, DOE surveyed contractor safety analysis and SQA practices. Attachment 3 is a compilation of the survey.

The Office of the Chief Information Officer (OCIO) 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 worked together to prepare this report and to make recommendations to the Lead Principal Secretarial Offices (LPSO) and also to recommend any specific line management follow-up actions to the Deputy Secretary (e.g., special assessments, contract changes, Safety Management System enhancements).

1.1 DOE Directives and Standards

DOE Federal directives and standards and contractor guidance organizations were reviewed to assess not just the guidance but the infrastructure for disseminating guidance. The review included directives for safety/safety analysis and software/SQA. It appears that there is an adequate number of organizations who have developed websites as their repository of standards information. However, better communication and connectivity among these groups is needed for information sharing.

1.1.1 Federal Directives and Standards Programs and Organizations

DOE has established three programs for defining Departmental requirements and expectations, which are the Departmental Directives repository system and two standards programs; i.e., DOE Technical Standards program and the DOE Information Architecture Standards program. These programs provide various Departmental directives and standards to DOE Federal and contractor staffs. Councils, committees, and working groups have also been established to interpret and implement the directives and standards. The most notable ones involved in software, quality assurance, and safety are discussed in this section.

DOE Directives. The DOE Directives System repository is managed by Management and Administration (MA) at Headquarters. DOE directives include Policies, Orders, Notices, Manuals, and Guides which are intended to direct, guide, inform, and instruct employees in the performance of their jobs, and enable them to work effectively within the Department and with agencies, contractors, and the public. Directives establish the minimum requirements that must be met and the results that must be accomplished to ensure successful and compliant solutions. Guides allow the most flexibility in implementation. Federal site and contractor implementations of DOE directives should address all aspects of the directives, including the reason(s) why specific aspects cannot be implemented or are not applicable to local needs. For information on DOE Directives, access the http://www.explorer.doe.gov:1776/htmls/directives.html website.

Safety and Safety Analysis. Below is a listing of directives for safety and safety analysis that contain software provisions or imply SQA. These directives are sponsored by EH and do not apply to the Naval Nuclear Propulsion Program.

- DOE P 450.4, SAFETY MANAGEMENT SYSTEM POLICY, defines the policy for integrating safety into management and work practices at all levels and all facets of work planning and execution based on six components. Quality assurance is implied in Component 3, Core Functions for Integrated Safety Management, by requiring a confirmation of readiness, feedback, oversight, and continuous improvement. DOE G 450.4-1A is the implementing guide.

- DOE P 450.5, LINE ENVIRONMENT, SAFETY AND HEALTH OVERSIGHT, defines the policy for Federal and contractor staffs to conduct Environment, Safety, and Health line oversight in a cost-effective, coordinated, integrated, and efficient manner. Quality assurance is implied by requiring compliance with applicable requirements, readiness assessments, verification reviews, for-cause reviews, and performance improvement.

- DOE O 420.1, FACILITY SAFETY, establishes facility safety requirements related to nuclear safety design, criticality safety, fire protection and natural phenomena hazards mitigation. It references standards required for certain safety applications, such as ANS-8.1-1983 that includes requirements for validating computer programs. DOE G 420.1-1 is the implementing guide.

- DOE O 5480.21, UNREVIEWED SAFETY QUESTIONS, sets forth the definition and basis for determining the existence of an Unreviewed Safety Question (USQ). The intent of this Order is to provide contractors with the flexibility needed to conduct day-to-day operations and to require that those issues with a potential impact on the authorization basis, and therefore the safety of the facility, be brought to the attention of DOE–thus maintaining the proper safety focus. The Order is focused on safety analysis of facilities, of which software could be a factor.

- DOE O 5480.22, TECHNICAL SAFETY REQUIREMENTS, states the requirements to have Technical Safety Requirements (TSR) prepared for DOE nuclear facilities and to delineate the criteria, content, scope, format, approval process, and reporting requirements of these documents and revisions thereof. The Order is focused on technical safety requirements of facilities, of which software could be a factor.

- DOE O 5480.23, NUCLEAR SAFETY ANALYSIS REPORTS, establishes requirements for contractors responsible for the design, construction, operation, decontamination, or decommissioning of nuclear facilities to develop safety analyses that establish and evaluate the adequacy of the safety bases of the facilities and to document this in Safety Analysis Reports (SAR), which includes addressing quality assurance.

- DOE M 411.1-A, SAFETY MANAGEMENT FUNCTIONS, RESPONSIBILITIES, AND AUTHORITIES, is a mechanism for implementing the Department's guiding principles established in DOE P 450.4, discussed above, and the safety management functions outlined in DOE P 411.1, SAFETY MANAGEMENT FUNCTIONS, RESPONSIBILITIES, AND AUTHORITIES POLICY.

- DOE G 421.1-1, GOOD PRACTICES GUIDE, is a comprehensive guidance document to assist in developing a criticality safety program to implement the DOE Order (or Rule) on nuclear criticality safety, and the invoked ANSI/ANS standards, through use of good practices. It provides brief information on SQA and verification, and an appendix on a software configuration control procedure.

Software and Software Quality Assurance. Below is a listing of directives for software and SQA or for quality assurance that imply SQA provisions.

- DOE O 200.1, INFORMATION MANAGEMENT, was canceled in FY 2000. It contained no explicit requirements for software development, but did reference DOE G 200.1-1, SOFTWARE ENGINEERING METHODOLOGY. DOE O 1330.1D, COMPUTER SOFTWARE MANAGEMENT, (superseded by DOE O 200.1) contained more explicit requirements for software development, including software quality assurance. A replacement Order is under development for DOE O 200.1.

- DOE N 203.1, SOFTWARE QUALITY ASSURANCE, specifies the requirements for an SQA program and SQA for projects. The Notice references DOE directives and industry standards applicable to safety or safety software. This Notice will be made into an Order.

- DOE G 200.1-1, SOFTWARE ENGINEERING METHODOLOGY, contains guidance in regards to the application of SQA on software projects. The Guide can and should be supplemented by site guidance to meet local needs. Included in the appendices in the guide are three SQA processes endorsed by the OCIO; i.e., In-Stage Assessment (ISA) process, Structured Walkthrough process, and the Stage Exit process.

- DOE O 414.1A, QUALITY ASSURANCE, states the requirements for DOE elements and contractors to develop Quality Assurance Programs (QAPs). The Order 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. It is consistent with the American Society of Mechanical Engineers (ASME) NQA-1 standard, which includes criteria for SQA. DOE O 5700.6C, QUALITY ASSURANCE (superseded by DOE O 414.1A), stated the quality criteria applied to all work and the items and services resulting from work. It referenced the national consensus standard ASME NQA-1.

- DOE G 414.1-2, QUALITY ASSURANCE MANAGEMENT SYSTEM GUIDE FOR USE WITH 10 CFR 830.120 AND DOE O 414.1 contains a section (4.6.3) related to the Design Process, which calls for validation of the software used in the design process and refers to ASME NQA-1 for acceptable methods. DOE G 830.120 (superseded by DOE G 414.1-2) was issued to implement 10 CFR 830.120, Quality Assurance. This guide clearly referenced the ASME NQA Part 2.7 for SQA.

Some Principal Secretarial Offices (PSO) have issued more specific guidance for their programs and field sites under their purview. For example, Civilian Radioactive Waste Management (RW) issued DOE/RW-0333P, "Quality Assurance Requirements and Description" as guidance for its programs such as the DOE Spent Nuclear Fuel and High

Level Waste program; and the former Office of Field Management issued a Good Practice Guide on Quality Assurance, which is available at the http://www.er.doe.gov/ website. (Once on the Office of Science website, at the end of the locator address type production/er-80/er-82/gpguides.html.)

Some sites have also issued specific guidance for their programs. For example, the Albuquerque Operations Office issued Quality Criteria (QC-1), invoked by reference in DOE/AL Supplemental Directive 56XB (Nuclear Weapon Development and Production Manual), which establishes general requirements for SQA of software used for specified functions in the design, production, and testing of weapons and weapons related materials; and the Development and Production (D&P) Manual, which references several Technical Business Practices (available on the official Nuclear Weapons Complex (NWC) http://prp.lanl.gov:8686/ website) for usage by the NWC.

DOE Technical Standards Program. The DOE Technical Standards program, which is managed by the Environment, Safety and Health (EH) organization at Headquarters, promotes the use of non-Government standards across the Department. The issuance of DOE standards is governed by Public Law 104-113, National Technology Transfer and Advancement Act of 1995; OMB Circular No. A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities; DOE O 252.1, TECHNICAL STANDARDS PROGRAM; DOE G 252.1-1, TECHNICAL STANDARDS PROGRAM GUIDE; and DOE's Technical Standards Program Procedures (TSPP). Public Law 104-113 requires that Federal agencies use existing voluntary consensus standards where they are available and suitable, and that Federal agencies work with standards development organizations to develop needed new standards.

EH also oversees the development of DOE technical standards, including information technology standards, as they relate to health and safety. The standards are not mandatory, but they can be mandated in an Order or clause. The process for proposing, developing, and maintaining DOE standards is contained in the TSPPs and explained in DOE G 252.1-1. Each organization's Technical Standards Manager is responsible for assisting in the implementation of the standards and assisting standards developers in their organization. Additional information on DOE Technical Standards and access to the Standards repository can be obtained on the http://tis.eh.doe.gov/techstds/ website.

Safety and Safety Analysis. Below is a listing of DOE standards on safety and safety analysis that contain provisions for software or imply software in the DOE Technical Standards program.

- DOE-STD-1027-92, HAZARD CATEGORIZATION AND ACCIDENT ANALYSIS TECHNIQUES FOR COMPLIANCE WITH DOE ORDER 5480.23, NUCLEAR SAFETY ANALYSIS REPORTS, establishes guidance for the preparation and review of hazard categorization and accident analyses techniques.

- DOE-STD-3009-94, PREPARATION GUIDE FOR U.S. DOE NONREACTOR NUCLEAR FACILITY SAFETY ANALYSIS REPORTS, establishes guidance for consistency with DOE O 5480.23 requirements and its safety guide, and describes a safety analysis report (SAR) preparation method for DOE. The standard contains a chapter on quality assurance.

Software and Software Quality Assurance. Below is a listing of DOE standards for software and SQA or for quality assurance that have SQA provisions in the DOE Technical Standards program.

- DOE-STD-4001-2000, DOE DESIGN CRITERIA STANDARD FOR ELECTRONIC RECORDS MANAGEMENT SOFTWARE APPLICATIONS, establishes the recommended method for meeting the functional requirements of the laws and regulations pertaining to managing records using electronic Records Management Application (RMA) software (submitted to the DOE Technical Standards program by the OCIO).

DOE Information Architecture (IA) Standards Program. The DOE IA Standards program is managed by the OCIO. The OCIO has the responsibility to lead, manage, integrate, and coordinate efforts centrally to achieve and implement standards to support the DOE IA. The purpose of the DOE IA is to ensure the wise stewardship of information technology resources by promoting a Departmental standards program that is participatory and consensus-based. The goal of the IA Standards program is to be flexible, forward thinking, and aligned with technology directions. The DOE IA Standards program applies to all DOE Elements, including contractors and laboratories.

The focus of the program is to establish a framework and best practices that will enable the overall accomplishment of the DOE mission and to avoid any unnecessary structural impediments. The IA Standards program sponsors and maintains a *DOE IA Profile of Adopted Standards* (latest is version *2000*) and an ongoing *IA Standards Adoption and Retirement Process.* The Profile consists of processes supported by representatives from the DOE community who are responsible for information technology standards activities. It is developed through consensus, with all of these representatives, thus ensuring that DOE Elements have a voice in the process. Recommendations for changes to the Profile are submitted according to the *IA Standards Adoption and Retirement Process*. The IA

Standards program manager can be contacted when, and if, new standards should be proposed for inclusion.

The *DOE IA Profile of Adopted Standards 2000* includes DOE standards, industry standards, and standards from recognized national and international bodies. These standards provide the framework and roadmap on how to accomplish successful projects and Departmental IA-compliant information technology solutions. The Profile is comprised of standards currently adopted in each of 10 service areas, reflecting the components of the Technical Reference Model necessary to build a complete technical infrastructure. The service areas are:

User	Application	Programming	Data Management	Data Interchange
Network	Operating System	Hardware Platform	Security	Management

For information on the *DOE IA Profile of Adopted Standards 2000*, access the http://cio.doe.gov/standards website. The *DOE IA Profile of Adopted Standards 2000*, DOE/SO-0002, January 2000 is available to DOE and DOE contractors from the Office of Scientific and Technical Information, P.O. Box 62, Oak Ridge TN 37831 (423) 576-8401.

Safety and Safety Analysis. Below is a listing of DOE consensus standards on safety and safety analysis in the *DOE IA Profile of Adopted Standards 2000* that contain provisions for software or imply software.

- None.

Software and Software Quality Assurance. Below is a listing of DOE consensus standards for software and SQA or for quality assurance that have SQA provisions in the *DOE IA Profile of Adopted Standards 2000*.

- DOE G 200.1-1A (Draft), DOE Software Engineering Methodology (SEM) Version 2 (1999), is a lifecycle methodology providing guidance for software engineering, project management, and quality assurance.

- DOE-STD-4001-2000, DOE Design Criteria Standard for Electronic Records Management Software Applications, March 2000, establishes the recommended method for meeting the functional requirements of the laws and regulations pertaining to managing records using electronic Records Management Application (RMA) software (submitted to the DOE Technical Standards program by the OCIO).

- IEEE 828-1988, IEEE Standard for Software Configuration Management Plans, establishes minimum required contents of a software configuration management plan and defines specific activities to be addressed.

- IEEE 1042-1987 (R1993), Guide to Software Configuration Management, discusses context, process, implementation, tools, techniques, supplier control, records management, and planning methodologies for software configuration management.

- ISO 9000, Quality Management and Quality Assurance Standards - Guidelines for Selection and Use, contains a consensus on the essential features of a quality system to ensure the effective operation of a business, whether a manufacturer or service provider, or other type of organization, either in the public or private sector.

- ISO 10005:1995, Quality Management - Guidelines for Quality Plans, provides guidance for preparing quality plans for control of specific products, projects, or contracts.

Quality Assurance Working Group (QAWG). The QAWG is composed of senior QA professionals throughout DOE, both Federal and contractor staffs. The QAWG addresses QA problems as they arise and advises the Deputy Secretary (i.e., the Chief Operating Officer) on the health of DOE QA programs. In support of line management, the QAWG:

- Identifies and recommends resolution of crosscutting QA issues impacting the safety of the worker, the public, and the environment

- Provides appropriate recommendations to the Deputy Secretary through the Field Management Council (FMC) for action by Field Elements and/or their contractors

- Proposes and comments on Departmental positions on QA safety issues, policies, and guidance

- Periodically reports on the status of identified crosscutting QA safety issues requiring resolution

- Identifies other DOE crosscutting organizations and work on integrated efforts to improve the efficiency and effectiveness of the Department QA and Integrated Safety Management programs

- Assists with implementation of QA safety recommendations

The QAWG can issue QA requirements, guides, and standard documents, which would be issued through the DOE Directives System or DOE Technical Standards program. For more information on the QAWG, access the http://twilight.saic.com/qawg website.

Federal Technical Capability Panel. The Federal Technical Capability Panel was created by DOE P 426.1, FEDERAL TECHNICAL CAPABILITY POLICY FOR DEFENSE NUCLEAR FACILITIES, and is responsible for implementing the program supporting that policy. The Panel, which consists of senior technical managers from across the Department, oversees the implementation of the Senior Technical Safety Manager and Facility Representative programs. The elements of this program include recruiting and hiring technically capable personnel, continuously developing the technical expertise of the workforce, and retaining critical technical capabilities within the Department at all times. The Panel also performs periodic assessments of the effectiveness of the recruitment, development and retention of technically capable DOE personnel. The Panel is described in the DOE M 411.1-l, SAFETY MANAGEMENT FUNCTIONS, RESPONSIBILITIES, AND AUTHORITIES MANUAL. Information on the Panel can be obtained on the Environment, Safety, and Health http://tis.eh.doe.gov website.

Field Management Council (FMC). The FMC was created by a Secretarial memo dated April 21, 1999, and charged with "corporate program integration and the integration of support activities with line programs." It was established to ensure consistent implementation of DOE policy in environment, safety, and health; safeguards and security; and business management. All staff and support office policy and guidance which impact the field must flow through the FMC. Policies and guidance developed by the staff and support offices are reviewed by the FMC and, if approved, passed to the Lead Principal Secretarial Officers (LPSO) for implementation. It is the responsibility of the FMC to ensure consistency in the application of DOE policy and to maximize uniformity of operational management approaches. Any conflict between a Principal Secretarial Officer (PSO) and the LPSO, or among PSOs, concerning direction to the field is resolved by the FMC. The FMC is chaired by the Deputy Secretary, and includes the Under Secretary, the Assistant Secretaries for Defense Programs and Environmental Management, and the Director of the Office of Science. Two other members, one from among the other PSOs and the other a Field Element Manager (FEM), serve in rotation. The FMC recently assumed the responsibilities of the former Secretarial Safety Council, which was formed to provide DOE with leadership and guidance to meet integrated safety management targets; develop and maintain performance standards to be used to hold Federal personnel accountable for effective and timely implementation of integrated safety management, and to oversee the viability and effectiveness of the DOE employee concerns program. The Secretarial Safety Council was composed of the same senior managers as the FMC and chaired by the Deputy Secretary. The FMC is described in the DOE M 411.1-1, SAFETY

MANAGEMENT FUNCTIONS, RESPONSIBILITIES, AND AUTHORITIES MANUAL. The FMC does not have a website.

Departmentwide Systems Engineering Process Group (DSEPG). The DSEPG, which is sponsored by the OCIO, provides advice and support on the development and maintenance of DOE information systems and software management programs by developing DOE directives or recommending flexible and adaptable industry standard project management, information systems engineering, and quality assurance guidance, procedures and other support. The mission of the DSEPG is to move the Department towards achieving higher levels of capability, maturity, and quality in information system solutions provided to the DOE customer. Membership includes volunteers from Headquarters and field sites, both Federal and contractor staffs. Thus far, the DSEPG has developed one guidance document–*Volume 1, Information Systems Engineering Guide*, of the *Departmental Information Systems Engineering (DISE)* series. Both safety and SQA are addressed in this guide. Information on the DSEPG will be appearing on the http://cio.doe.gov/smp (soon to be http://cio.doe.gov/sqse) website.

1.1.2 Contractor Standards Programs and Organizations

Contractors are required to follow applicable DOE directives and standards, usually through a general statement or a specific listing in DOE contracts. Contractors also follow their own internal processes and procedures, which are generally based on industry standards. Several of the Management and Operating (M&O) contractors are moving toward Software Engineering Institute (SEI) or International Organization of Standards (ISO) 9000 certifications, which are intended to result in better management of software.

There are several contractor groups that meet regularly to establish and promote best practices for safety and software. The most notable for safety is the Safety Analysis Working Group (SAWG) of the Energy Facilities Contractor Group (EFCOG). Also, a new temporary group called the Safety Analysis Software Group (SASG), led by DP, EH, and EM, has been established to address software issues for safety analysis and I&C software. The most notable contractor groups for software and systems engineering are the Software Quality Assurance Subcommittee (SQAS) and the DOE International Council on Systems Engineering (DOE INCOSE).

The Energy Facility Contractors Group (EFCOG) and **The Safety Analysis Working Group (SAWG)**. The EFCOG is a self-directed group of Management and Operating (M&O) contractors, Management and Integrating (M&I) contractors, and Environmental Restoration Management Contractors (ERMC) of DOE facilities. The purpose of the EFCOG and the SAWG, a working group of EFCOG, is to promote excellence in all aspects of operation and management of DOE facilities in a safe, environmentally sound, more efficient and cost-effective manner through the ongoing exchange of information. Through meetings, workshops and conferences, working group participants share proven (not theoretical or philosophical) management and technical processes, procedures, and programs. They also share both positive and negative lessons learned. The exchange of best practices and information between EFCOG members across the DOE complex is achieved without regard to competitive boundaries. EFCOG/SAWG has a publications library on their website. For more information on EFCOG and SAWG, access the http://www.efcog.org website. (SAWG can be accessed after getting on the EFCOG website by clicking on Work Groups, then Working Groups and Subgroups, then Safety Analysis.)

Safety Analysis Software Group (SASG). The SASG is initially established as a temporary group to respond to the Defense Nuclear Facilities Safety Board (DNFSB) Technical Report 25 regarding issues for safety analysis and I&C software. The group is led by three Headquarters Federal employees (one each in DP (chair), EH, and EM) and is comprised of DOE and contractor subject matter experts in safety analysis, software development, SQA, and authorization basis implementation. Their task is challenging since 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, the SASG serves as a centralized group and will try to obtain coordinated support from the EFCOG. The SASG provides:

- Leadership for DOE and its contractors 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 safety and I&C software issues that have crosscutting impact across DOE

- Identification of support mechanisms and resource allocation from stakeholder contractors and line organizations in the Department

As part of its advisory activities, the SASG has responsibility for identifying model improvements, and recommending new software development. This activity incorporates not only DOE applicability and needs, but references "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 proper configuration management, that users are notified of changes, and earlier versions are retired. This configuration management process will follow software lifecycle protocol, per standards identified by the Software Quality Assurance Subcommittee

(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 i numbers and skill mix to meet these challenges at the appropriate level.

The SASG will use existing safety analysis Internet links to inform users of safety analy issues. Software user alerts will be communicated via the EFCOG/SAWG website, list above. This website will be expanded 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 use feedback.

Software Quality Assurance Subcommittee (SQAS). SQAS is sponsored by the DC Nuclear Weapons Complex (NWC) Quality Managers under the auspices of the Albuquerque Operations Office (now under the National Nuclear Security Administrati (NNSA)). The objectives of SQAS are to:

- serve as a technical advisory group to the Quality Managers, DOE Albuquerque Operations Office, and other DOE offices, as appropriate
- promote an understanding and awareness of software quality and its assurance
- identify and share tools, techniques, and methodologies for improving software qualit

SQAS has developed several guidance documents for the NWC, some of which can be and are recommended for Departmentwide use. Most of the documents were develope based on industry standards and guidance from the Software Engineering Institute (SE For more information on SQAS, access the http://cio.doe.gov/sqas website. Also, as stated previously, several Technical Business Practices used by the NWC (as reference the Development and Production (D&P) Manual) can be accessed on the official NWC http://prp.lanl.gov:8686/ website.

International Council on Systems Engineering (INCOSE) and the DOE INCOSE Systems Engineering (SE) Practices Interest Group. (See also 1.3.1 INCOSE.) DC employees participate in INCOSE and have formed the DOE SE Practices Interest Gro

(DOESEPIG), which is a technical committee of INCOSE. The DOESEPIG mission is to foster the application of good systems engineering practices within the U.S. Department of Energy complex. Their focus is on the waste management and environmental restoration applications. They can be accessed through the INCOSE website at http://www.incose.org by clicking on Table of Contents, then scrolling down to Working Groups and Interest Groups. The former Headquarters Field Management (FM) organization had close ties to this group. Some Headquarters members attend its annual meeting.

1.2 Other Government Standards

DOE interacts with other U.S. Government agencies on a regular basis in the course of fulfilling the DOE mission. These agencies develop and maintain standards to support the accomplishment of their missions, to enable computer systems to interface and communicate with each other, and to ensure the health and safety of the general public, where that is a concern. DOE also interacts with other agencies to both ensure standards compatibility and to assess the maturity of DOE processes and standards relative to other agencies.

Other Government agencies can be a good benchmark since they also must comply with the same legislation (such as the Clinger-Cohen Act and OMB Circular A-130, which specify information technology requirements and practices) and external agency direction and review such as OMB and GAO. In regards to nuclear safety management, DOE must comply with 10 CFR Part 830, Nuclear Safety Management (which includes guidelines on quality assurance) and the Price-Anderson Act. These legislative acts have been implemented through the DOE directives noted in Section 1.1.1.

Some of the government agencies DOE interfaces with are the Nuclear Regulatory Commission, Department of Defense, Department of Transportation, National Institutes of Standards and Technology, National Aeronautical and Space Administration, and Defense Threat Reduction Agency.

1.2.1 U.S. Nuclear Regulatory Commission (NRC)

The NRC is an independent agency established by the U.S. Congress under the Energy Reorganization Act of 1974 to ensure adequate protection of public health and safety, common defense and security, and the environment in the use of nuclear materials in the United States. The NRC's scope of responsibility includes regulation of commercial nuclear power reactors, nonpower research, test, and training reactors, fuel cycle facilities, medical, academic, and industrial uses of nuclear materials, and the transport, storage, and disposal of nuclear materials and waste.

The NRC provides a Standards website which supports NRC's strategy to increase involvement by licensees and others in its regulatory development process consistent with the National Technology and Transfer Act of 1995. Compiled on this website at http://www.nrc.gov/NRC/REFERENCE/STANDARDS/index.html is information on NRC's participation in the development and use of consensus standards. NRC also has developed several standards (1.168 through 1.173) for software used in safety systems that are available at the http://www.nrc.gov/NRC/RG/01/index.html website. In addition, the NRC has developed "NUREG-0800, the Standard Review Plan," that contains Section 7.0 Instrumentation and Control–Overview of Review Process, which is directed at the staff review of I&C safety systems (called BTP-14) in reactor designs. The review guidance is specialized to real-time process control safety (especially reactors).

1.2.2 U.S. Department of Defense (DOD)

The DOD is responsible for providing the military forces needed to deter war and protect the security of our country. In doing so, DOD interacts in joint DOE/DOD missions. Recognizing the importance of providing official, timely and accurate information about defense policies, organizations, functions and operations, DOD established an information repository called DefenseLINK. DefenseLINK is the single, unified starting point for finding military information online. It can be accessed on the http://www.defenselink.mil website.

In 1994, DOD began an effort to reform its standards and specifications program and established the DOD Standards Improvement Council. Within one year, 1200 commercial standards were adopted, and an initiative for a national software development standard was proposed. The Defense Standardization Program is managed by the Center for Information Technology Standards under the auspices of the Defense Information Systems Agency (DISA). The DISA Standards Library can be accessed on the http://www.itsi.disa.mil website. DOD also has another organization, the Defense Technical Information Center, which is under the auspices of DISA as well, to facilitate the exchange of scientific and technical information (see the http://www.dtic.mil website). DISA is available at the http://www.disa.mil website. Military specifications and standards, federal specifications and standards, QPLs, CIDs, DIDs, and other standardization documents, can be ordered by visiting the DOD Single Stock Point (DODSSP) website. Registration for an account and password for the Acquisition Streamlining and Standardization System (ASSIST), which will enable access to standardization documents directly through your Web Browser, is available. For additional information on U.S. DOD standards, access the http://dodssp.daps.mil or http://dodssp.daps.mil/assist.htm website.

1.2.3 U.S. Department of Transportation (DOT)

DOE must interact with DOT because of the transport of defense nuclear materials throughout the United States and the world. The mission of the DOT is to serve the United States by ensuring a fast, safe, efficient, accessible and convenient transportation system that meets our vital national interests and enhances the quality of life of the American people, today and into the future. The DOT consists of eleven individual operating administrations including the Bureau of Transportation Statistics, U.S. Coast Guard, the Federal Aviation Administration, the Federal Highway Administration, the Federal Railroad Administration, the Federal Transit Administration, the Maritime Administration, National Highway Traffic Safety Administration, the Research and Spec Programs Administration, the Saint Lawrence Seaway Development Corporation, the Surface Transportation Board and the Transportation Administrative Services Center. I more information on the DOT, access the http://www.dot.gov website.

To expedite the development and deployment of interoperable Intelligent Transportatio Systems (ITS) and services, the U.S. DOT supports standards activities in areas that hav significant public benefit. ITS standards are industry consensus standards that specify ho different technologies, products, and components interconnect so they can be used withi a consistent framework. The framework is known as the National ITS Architecture. Th standards can be accessed at the http://www.its.dot.gov/Standard/Standard.htm website.

1.2.4 The National Institutes of Standards and Technology (NIST)

NIST is an agency of the U.S. Department of Commerce's Technology Administration. Established in 1901, NIST strengthens the U.S. economy and improves the quality of lif by working with industry to develop and apply technology, measurements, and standard Under the Information Technology Management Reform Act (Public Law 104-106), known as the Clinger-Cohen Act, the Secretary of Commerce approves standards and guidelines that are developed by NIST for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) f use government-wide.

Also, the National Center for Standards and Certification Information (NCSCI) at NIST the ISO Information Network (ISONET) member for the United States (see http://ts.nist.gov/ts/htdocs/210/217/bro.htm website). ISONET is a worldwide netwo of national standards information centers which have cooperatively agreed to provide rapid access to information about standards, technical regulations, and testing and certification activities currently used in different parts of the world. NIST's Information Technology Laboratory (ITL) concentrates on developing tests and test methods for information technologies that are still in the early stages of development, and once products are available, tests to allow developers and users to evaluate how products perform and assess their quality based on objective criteria. For more information on ITL or NIST, access the http://www.nist.gov website.

NIST has recently prepared a study which examines the contents of an SQA standard for nuclear applications, available at http://hissa.ncsl.nist.gov/publications/nistir4909/ website. The study includes recommendations for the documentation of software systems. Background information on the standard, documentation, and the review process is provided. The report includes an analysis of the applicability, content, and omissions of the standard and compares it with a general SQA standard produced by the Institute of Electronics and Electrical Engineers (IEEE). Information is provided for the content of the different types of documentation. This report describes information for use in safety evaluation reviews. Many recommendations in this report are applicable for SQA in general.

1.2.5 National Aeronautical and Space Administration (NASA)

NASA is an independent agency established by the U.S. Congress in 1958 to conduct space missions and for national defense. It is a Federal research and engineering agency that accomplishes most of its space, aeronautics, science, and technology programs through Field Centers and contractors across the United States. It consists of the NASA Headquarters, nine Centers, the Jet Propulsion Laboratory (operated by the California Institute of Technology), and several ancillary installations and offices in the United States and abroad. Its mission is to advance and communicate scientific knowledge and understanding of the Earth, the solar system, and the universe; to advance human exploration, use, and development of space; and to research, develop, verify, and transfer advanced aeronautics and space technologies. For more information on NASA, access the http://www.nasa.gov or http://www.nasa.gov/search website.

NASA has developed an Information Technology program to enhance the safety and security of the National Airspace System through the development of technologies for systems control and operations, and flight critical software systems. Two significant projects are the Intelligent System Controls and Operations (ISCO) project and the Software Integrity, Productivity and Security (SIPS) project. The program can be viewed on the http://www.nas.nasa.gov/IT/test/index.htm website. Also, the NASA Ames Research Center (ARC) is NASA's "Center of Excellence" for information sciences and technologies, and is available at the http://www.arc.nasa.gov website. Contained within ARC are the System Safety and Mission Assurance Office, and the Quality Management Program Office. Additionally, information on High Performance Computing and Communications is available at the http://hpcc.arc.nasa.gov website.

1.2.6 Defense Threat Reduction Agency (DTRA)

DTRA was created to integrate and focus the capabilities of DOD which address the weapons of mass destruction (WMD) threat. DTRA safeguards the United States and its friends from WMD by reducing the present threat and preparing for the future threat. DTRA's work covers a broad spectrum of activities – shaping the international environment to prevent the spread of WMD; responding to military requirements to help the United States deter, withstand, prevail against and recover from the use of such weapons; and preparing the warfighter to counter the full spectrum of future WMD threats. DTRA can be accessed on the http://www.dtra.mil website.

One of DTRA's major mission areas is Technology Development which focuses on several areas, three of which are the Scientific Computing Program, Radiation Test Facilities and Capabilities, and Hazard Prediction Assessment Capability (HPAC). The DTRA Scientific Computing Program is responsible for DOD's High Performance Computing Modernization Program (HPCMP), whose mission is to modernize the total high performance computational capability of DOD Science and Technology (S&T), Development Test and Evaluation (DT&E) and Ballistic Missile Defense Organization (BMDO). Use of DTRA scientific computing resources at DTRA, Los Alamos National Laboratory (LANL) and the High Performance Computing (HPC) sites are available to both contractor and government organizations who are performing research under contract with DTRA. Two products that are readily available are a brochure describing the Radiation Test Facilities and Capabilities and its resources, and HPAC software which predicts the effects of hazardous material releases into the atmosphere and its collateral effects on civilian and military populations. The HPAC software is available by license from the DTRA, to U.S. government entities, their contractors, and educational institutions for non-commercial research. DTRA has published several documents in nuclear radiation and safety software but they are not listed on the website.

1.3 Industry Organizations and Standards

For compliance with legislation to use consensus standards and facilitate management improvements, DOE practices are generally based on guidance from industry organizations and standards. The following sections focus on industry organizations and standards for general software and safety software.

1.3.1 Software and Engineering Organizations and Standards

Major industry organizations, who address issues on various software topics regarding information systems engineering, project management, and quality assurance, include the Software Engineering Institute (SEI), International Council on Systems Engineering

(INCOSE), Electronic Industries Alliance (EIA), Institute of Electronics and Electrical Engineers (IEEE), the International Organization for Standardization (ISO), American Society of Mechanical Engineers (ASME), American National Standards Institute (ANSI), American Nuclear Society (ANS), Society for Automotive Engineers (SAE), American Society for Quality (ASQ), Quality Assurance Institute (QAI), and Project Management Institute (PMI®). DOE Federal and contractor organizations use standards and guidance from these organizations to accomplish missions.

Software Engineering Institute (SEI). The SEI is a Federally funded research and development center established in 1984 by the U.S. Congress, and placed under the management of the Department of Defense. The SEI has a broad charter to address the transition of software engineering technology and to advance the practice of software engineering because quality software that is produced on schedule and within budget is a critical component of U.S. defense systems. SEI is an integral component of the Carnegie-Mellon University. SEI has developed and published maturity models, technical reports, special reports, and handbooks. They do not issue standards but their products may be adopted by industry standards organizations. Searches for software information such as "defense nuclear facilities safety and safety analysis software" can be made by accessing the http://www.sei.cmu.edu/about/website/search.html website.

The SEI has developed Capability Maturity Models (CMMs) for software, people, software acquisition, systems engineering, and integrated product development. The intent of the CMMs is to assist organizations in maturing their people, processes, and technology assets to long-term business performance. Many Federal and contractor organizations are seeking improvement in their software projects by using the SEI Software CMM (SW-CMM). It is estimated that about 50 percent of software contractors nationwide are self-assessed at SW-CMM Level 2; i.e., they have the basic project management processes for project planning, project tracking and oversight, configuration management, requirements management, and quality assurance instituted in their organization. For more information on SEI, access the http://www.sei.cmu.edu website.

International Council on Systems Engineering (INCOSE). INCOSE is an international organization formed to develop, nurture and enhance the systems engineering approach to multi-disciplinary system product development. The INCOSE mission states that INCOSE shall foster the definition, understanding, and practice of world class systems engineering in industry, academia, and government. They do not issue standards but their products may be adopted by industry standards organizations.

There are several committees sponsored by INCOSE. In particular, the INCOSE Standards Technical Committee (STC) promotes the involvement in and influence on national, international, and other standards, handbooks, and guides. The STC encourages, guides, and assesses INCOSE's participation in standards activities, coordinates INCOSE's review of standards, and disseminates information on standards and standardization activities. Another is the Systems Engineering Management Methodology Working Group, whose purpose is to create, coordinate, and disseminate process definitions and methods for planning, organizing, integrating, and controlling the technical aspects of a project throughout a system's lifecycle. INCOSE has a publications library on its website. For more information on INCOSE, access the http://www.incose.org website.

Electronic Industries Alliance (EIA). The Electronic Industries Alliance (EIA) is a federation of associations and sectors that focuses on the electronics industry. Comprised of over 2,100 members, EIA has representatives from about 80% of the U.S. electronics industry. EIA member and sector associations represent telecommunications, consumer electronics, components, government electronics, semiconductor standards, as well as other vital areas of the U.S. electronics industry.

EIA is committed to promoting business opportunities for its industries. It provides a forum for industry to develop standards and publications in the major technical areas of electronic components, consumer electronics, electronic information, and telecommunications. Over 4,000 standards have been developed. Included in its resource listings are publications on system safety engineering and software. For more information on EIA and EIA standards, access the http://www.eia.org/ website.

Institute of Electronics and Electrical Engineers (IEEE). IEEE is a non-profit technical professional association of more than 330,000 individual members in 150 countries. Through its members, the IEEE is a leading authority in technical areas ranging from computer engineering, biomedical technology and telecommunications to electric power, aerospace and consumer electronics, and many other areas.

Through its technical publishing, conferences and consensus-based standards activities, the IEEE produces 30 percent of the world's published literature in electrical engineering, computers and control technology. It holds annually more than 300 major conferences and has more than 800 active standards with 700 under development. IEEE has issued several standards for software, SQA, and safety software. Two notable ones are IEEE 1228, Standard for Software Safety Plans, and IEEE 1044, Standard Classification for Software Anomalies. Additional information on IEEE standards can be viewed at the http://standards.ieee.org website. For more information on IEEE, access the http://www.ieee.org website.

International Organization for Standardization (ISO). The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies from about 130 countries. ISO is a non-governmental organization established in 1947. The mission of ISO is to promote the global development of standardization and related activities with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity. ISO's work results in international agreements, which are published as International Standards. The ISO 9000 series of standards provides a framework for quality management and quality assurance, as well as other related ISO standards. The 9000 series are "management" standards rather than project-application standards. For more information on ISO and ISO standards, access the http://www.iso.ch website.

American Society of Mechanical Engineers (ASME). Founded in 1880 as the American Society of Engineers, today ASME International is a nonprofit educational and technical organization serving a worldwide membership. The ASME conducts one of the world's largest technical publishing operations, holds some 30 technical conferences and 200 professional development courses each year, and sets many industrial and manufacturing standards. Since 1884, when the first performance test codes were developed, ASME International has pioneered the development of codes, standards and conformity assessment programs. ASME maintains and distributes 600 codes and standards used around the world for the design, manufacturing and installation of mechanical devices. Two notable standards are NQA-1-1994, Quality Assurance Program Requirements for Nuclear Facilities, and NQA-1-1997, Quality Assurance Requirements for Computer Software for Nuclear Facility Applications. For more information on ASME, access the http://www.asme.org/ website.

The American National Standards Institute (ANSI). ANSI has served in its capacity as administrator and coordinator of the United States private sector voluntary standardization system for more than 80 years. Founded in 1918, the Institute remains a private, nonprofit membership organization supported by a diverse constituency of private and public sector organizations. ANSI has as its primary goal the enhancement of global competitiveness of United States business and the American quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems and promoting their integrity. ANSI does not itself develop American National Standards; rather, it facilitates development by establishing consensus among qualified groups. ANSI-accredited developers support the development of national and, in many cases, international standards, addressing the critical trends of technological innovation, marketplace globalization and regulatory reform. ANSI has a website at http://www.nssn.org that allows searches for standards by title, designation, sponsoring organization, or key word. For more information on ANSI, access the http://web.ansi.org/ website.

American Nuclear Society (ANS). ANS is a not-for-profit, international, scientific and educational organization. It was established by a group of individuals who recognized the need to unify the professional activities within the diverse fields of nuclear science and technology. December 11, 1954, marks the Society's historic beginning at the National Academy of Sciences in Washington, D.C. ANS has since developed a multifarious membership composed of approximately 11,000 engineers, scientists, administrators, and educators representing 1,600 plus corporations, educational institutions, and government agencies. It is governed by three officers and a board of directors elected by the membership.

ANS creates only a portion of the standards for the nuclear industry, which can be viewed on the http://store.ans.org website. The NAS-10 standards address mathematics and computation, and include some computer programming. The ANS-8 standards address a Criticality Safety Committee. One notable standard used at DOE is ANSI/ANS-10.4-1987, Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry. For more information on ANS, access the http://www.ans.org website.

Society for Automotive Engineers (SAE). SAE provides technical information and expertise used in designing, building, maintaining, and operating self-propelled vehicles for use on land or sea, in air or space. Founded in 1905, nearly 80,000 engineers, business executives, educators, and students from more than 97 countries form a network of members who share information and exchange ideas for advancing the engineering of mobility systems. The SAE Cooperative Research Program helps facilitate projects that benefit the mobility industry as a whole. Also, technical committees are formed to write aerospace and automotive engineering standards, technical papers, books, and periodicals.

SAE maintains liaisons with a number of organizations to fully coordinate its standards and avoid duplication. The SAE Cooperative Engineering Program provides many standards each year that contain part and product qualification procedures. These procedures aid manufacturers in the production of quality products and save valuable engineering time. SAE publishes many new, revised, and reaffirmed standards each year in three categories: Ground Vehicle Standards (J-Reports); Aerospace Standards; and Aerospace Material Specifications (AMS). SAE Aerospace Standards are used extensively by the military services as well as by the private sector. Over 2,300 SAE Aerospace Material Specifications, covering a vast array of material and processes, are available to the aerospace engineer. Combine these with 2,100 more documents on a wide variety of subjects makes SAE the world's largest producer of non-government aerospace standards. For more about SAE, access the http://www.sae.org and http://www.normas.com websites.

1.3.2 Quality Organizations and Standards

There are several other well-recognized organizations that create or endorse best practices and standards for quality assurance and project management. The American Society for Quality (ASQ), the Quality Assurance Institute (QAI), and the Project Management Institute (PMI) are a few of these organizations.

American Society for Quality (ASQ). Founded in 1946, ASQ advances individual and organizational performance excellence worldwide by providing opportunities for learning, quality improvement, and knowledge exchange. ASQ has more than 120,000 individual and 1,100 sustaining members. Since the establishment of its first certification program in 1966, ASQ has certified more than 80,000 quality practitioners as quality engineers, quality auditors, reliability engineers, quality technicians, mechanical inspectors, quality managers, and software quality engineers.

ASQ is charged with administering the standards committees on behalf of the American National Standards Institute (ANSI). The committees can be grouped within four broad technical disciplines: Quality Management, Environmental Management, Dependability, and Statistics; i.e., QEDS. As the secretariat for the ANSI Accredited Standards Committee (ASC) Z1 Committee on QEDS, ASQ provides direction on and builds consensus for national and international standards. ASQ plays a key role in developing the ISO 9000 series standards, which were originally adopted nationally as the Q90 series standards, and recently revised and redesignated as the Q9000 series standards. They do so through their involvement in the U.S. Technical Advisory Group for ISO Technical Committee 176, administered by ASQ on behalf of ANSI. (ANSI represents the U.S. within ISO.) ASQ is also the secretariat for ISO Technical Committee 69 Subcommittee 1 on Terminology and Symbols. In addition, ASQ administers the U.S. Technical Advisory Groups for several committees. For more information on ASQ, access the http://www.asq.org/ website.

Quality Assurance Institute (QAI). QAI was founded in 1980, and is an international organization of member companies in search of effective methods for defect detection/software quality control and defect prevention/software quality assurance. QAI's goal is to become the international standard of definition for professional status as an information services quality practitioner, and to provide leadership to the information services profession in improving quality, productivity, and effective solutions for process management. QAI provides leadership and state-of-the-art solutions in the form of consulting, education services, and assessments. It is exclusively dedicated to partnering with the enterprise-wide Information Quality profession for improving enterprise-wide information quality.

QAI offers three professional level certifications; namely, Certified Quality Analyst (CQA) for competency in the principles and practices of quality assurance in the information technology profession; the Certified Software Test Engineer Program which is intended to establish standards for initial qualification and provide direction for the testing function; and the Certified SPICE Assessor Program for ISO/IEC TR 15504 conformant assessments. For more information on QAI, access the http://www.qaiusa.com/ website.

Project Management Institute (PMI®). Since its founding in 1969, PMI® has become the organization of choice for project management professionalism. With over 70,000 members worldwide, PMI® is the leading nonprofit professional association in the area of project management. PMI® establishes project management standards, provides seminars, educational programs and professional certification. PMI®'s "A Guide to the Project Management Body of Knowledge (PMBOK® Guide)" was approved by ANSI as an American National Standard, ANSI/PMI 99-001-1999.

In addition, the PMI® Education Department supports the development of standards for accrediting degrees in project management and approving curriculums for master certificates in project management. PMI® also conducts a certification program in project management. PMI®'s Project Management Professional (PMP) credential is the project management profession's most globally recognized and respected certification credential. Worldwide there are over 20,000 PMPs who provide project management services in 26 countries. For more information on PMI®, access the http://www.pmi.org/ website.

1.3.3 Software Safety Organizations and Standards

Several organizations have been established to specifically address software system safety. Among these are the System Safety Society, the National Safety Council, and the International Safety Council. Additionally, in 1999, a Software Safety System Handbook was developed through a joint effort of Federal government staffs.

System Safety Society. Founded in 1964, the System Safety Society is composed of membership extending to over a dozen countries and a variety of professional occupations. It is a professional organization dedicated to the promotion of the system safety concepts at the local, national and international level to:

- Advance the state-of-the-art of system safety
- Contribute to a meaningful understanding of system safety
- Disseminate newly developed knowledge to all interested groups and individuals
- Further the development of the professionals engaged in system safety
- Improve the public understanding of the system safety discipline

- Improve the communication of the system safety movement and discipline to all levels of management, engineering, and other professional groups

Avoiding hazards has been a concern for some time; however, formalized efforts to incorporate activities specifically oriented toward hazard identification and control on a comprehensive and total lifecycle basis has occurred only in recent times. Safety publications endorsed by the System Safety Society include:

- MIL-STD-882, DOD Standard Practice for System Safety - released February 2000

- Software System Safety Handbook - A Technical and Managerial Team Approach - released December 1999

- MIL-STD-1472F, DOD Design Criteria Standard Human Engineering - released August 1999

- System Safety Analysis Handbook, 2nd edition, - released August 1999

For more information on the System Safety Society, access the http://www.system-safety.org website.

National Safety Council (NSC). Founded in 1913, the NSC has served as the premier source of safety and health information in the United States. The Council is a nonprofit, governmental, international public service organization dedicated to improving the safety, health and environmental well-being of all people. An Act of Congress on August 13, 1953, created the Council as a body incorporated under Federal law; i.e., Public Law 259 of the 83rd Congress formally established NSC as a federally chartered organization. The charter mandates that the Council be nonpolitical and not contribute to or otherwise assist any political party or candidate. The mission of the NSC is to educate and influence society to adopt safety, health and environmental policies, practices and procedures that prevent and mitigate human suffering and economic losses arising from preventable causes. The Council has been working for generations to protect lives and promote health with innovative programs.

NSC does not issue standards, but does sell some ANSI standards. Various services, resources, and products are available. For more information on the NSC, access the http://nsc.org/ website.

The International Safety Council (ISC). The ISC is the National Safety Council's global subsidiary. Established in 1913, ISC is a not-for-profit, nongovernmental, membership based organization committed to the mission of protecting life and promoting health. Over 17,000 members represent more than 70 countries around the world and include industry, labor, government, community groups and associations. They provide training, expertise, products and services related to all areas of safety, health and the environment. For more information on the ISC, access the http://safety.webfirst.com/isc.htm website.

Joint Software System Safety Handbook. The development of this Handbook is a joint effort by the U.S. Army, Navy, Air Force, and Coast Guard Safety Centers, in cooperation with the FAA, NASA, defense industry contractors and academia. The research involved captures the "best practices" pertaining to software safety systems program management and safety critical software design. The Handbook consolidates these contributions into a single, user-friendly resource guide for use in the understanding of both the complete software safety systems and the contribution of each functional discipline in identifying, controlling, and managing software-related hazards within safety-critical components of hardware systems.

For more information on, or to download the Joint Software System Safety Handbook, access the System Safety Society at the http://www.system-safety.org website. Other sources of the Handbook or safety information are the Navy Surface Warfare Center, which can be accessed at the http://www.nswc.navy.mil/safety website, and the Air Force Safety Center at the http://www.usaf.com/orgs/12.htm website.

2.0 Standards Analysis

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, the Board stated that DOE had 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. The Board further stated that although some quality processes are conducted, overall they are fragmented or isolated, and not integrated with safety.

The Board felt that DOE should clearly define requirements that are appropriate for use by its contractors. 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.

The independent evaluations and survey were conducted with these concerns in mind. This section addresses the findings, assessments, and gap analyses. Recommendations are provided.

2.1 Assessment of Independent Evaluation

Section 1.1 described the Departmental approach to software in general and in regards to safety software. The high-level directives infrastructure for safety and QA appears to be in place. The guidance in the QA rule, DOE O 414.1A, and other guidance issued by EH and the ASME NQA-1 standard are facility-oriented rather than product-oriented, such as Quality Criteria-1 (QC-1) issued by the Albuquerque Operations Office. Although the QA Rule and Order do not specify requirements and expectations for software, they apply to all work, and software development and use is considered one type of work. After the SASG reviews the directives infrastructure for safety software at the field sites, a determination should be made whether a Departmental directive is needed for safety software.

The OCIO agreed with the DNFSB that high-level direction for software needed to be improved. A replacement Order for DOE O 200.1, INFORMATION MANAGEMENT, is in process by the OCIO. DOE N 203.1, NOTICE FOR SOFTWARE QUALITY ASSURANCE, was issued to bring about improvement in software management. Further actions will be taken to assess the adequacy of DOE's expectations and requirements for software systems management. As a positive, although no data was collected, verbal exchanges and interactions with DOE Federal and contractor groups affirm that implementation of SEI Level 2 processes is taking place.

Several of the Other Government organizations have standards programs and have identified a set of consensus standards that can be used as benchmarks. Some of the websites provide contact names. Industry organizations are addressing safety software issues and have issued standards and guidance that appear to be very appropriate for the DOE environment. DOE contractor organizations have even participated in the development of some of the guidance.

2.2 Assessment of Survey Results

A compilation of the survey is contained in Attachment 3. The following questions were asked in the survey, and the tentative analysis results of the answers follow each question. As an overall, many sites have their own local standards, with an additional half-dozen industry standards being frequently mentioned by those sites not having local guidance. Also, about two dozen programs common to many sites both within and outside DOE are mentioned, exclusive of local spreadsheets and other software unique to single facilities (e.g., blast codes). Some of the former are NRC or proprietary codes with firm QA, others are ad hoc and not particularly QA-ed. It appears that the software that most strongly supports safety (as opposed to rough, conservative measures of release consequences) are the most reliable.

I.1 What documented SQA programs or procedures do you follow for computer codes used for safety analysis in the areas of:

a) Software Development
b) Software Testing
c) Software Documentation
d) Software Maintenance
e) Software Usage

For the above, identify (1) which are DOE, in-house, and industry developed; (2) which are mandatory, and (3) what is the nature of the software quality assurance processes; i.e., structured walkthrough, peer review, inspection, audit, testing, etc.

Results: Sites indicate they have mandated internal developed processes for lifecycle management of DOE software. They indicate they do some form(s) of QA activity but a formal SQA program appears to be lacking.

I.2 Do these procedures comply with the following (check compliance and indicate whether in whole or in part):

a. DOE Order 420.1, *Facility Safety*
b. DOE Order 414.1, *Quality Assurance*
c. DOE Order 200.1, *Information Management Program*
d. DOE Guide 200.1-1, *Department of Energy Software Engineering Methodology*
e. DOE Guide 414.1-1, *Assessment Guide for QA* (esp., section 4.6.3)
f. Other Industry Standards, Requirements, or Guidelines (including, but not limited to)
   - American Nuclear Society, ANSI/ANS-10.4-1987, *Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry*
   - American Society of Mechanical Engineers, 1997, *Quality Assurance Requirements for Computer Software for Nuclear Facility Applications*, NQA-1-1997 (esp. Part 2.7)

g. Others?

Results: Sites indicate a range of compliance with the above directives either "in part" or "whole". Some have mapped their directives to the Departmental directives. A couple of organizations indicate they are still under contract to adhere to canceled Orders such as:

- DOE 5480.28, *Natural Phenomena Hazards Mitigation*
- DOE 5480.7A, *Fire Protection*
- DOE 6430.1A, *General Design Criteria*
- DOE 5480.24, *Criticality Safety*

I.3 How frequently is compliance with these procedures audited?
Are audits performed by external groups?
What is the date (s) of your last SQA audit?

Results: Sites indicate that auditing does take place but may be inadequate for software assessment.

2.3 Gap Analysis of Survey Results and Independent Evaluation With the Directives and Standards Infrastructure

The OCIO has determined through an independent assessment that improvements need to be made in establishing a more adequate software standards infrastructure through the DOE Directives System and the Information Architecture (IA) Standards program. In regards to safety software, more investigation needs to take place. Organizations and processes are in place for disseminating and making improvements to DOE Directives, IA Standards program, and the DOE Technical Standards program. Auditing processes may need to be improved to get better communication of Departmental guidance to the floor level.

Departmental websites have been established for the exchange of information. The DOE Directives System is the repository of all DOE directives, which can be accessed at the http://www.explorer.doe.gov:1776/htmls/directives.html website. The DOE Technical Standards program promotes the use of non-Government standards across the Department and has established a website at http://tis.eh.doe.gov/techstds/. The Office of the Chief Information Officer (CIO) has established a website 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 website for Departmental guidance on Software Quality and Systems Engineering at http://cio.doe.gov/smp (soon to be http://cio.doe.gov/sqse) and provides support for the website for the Software Quality Assurance Subcommittee (SQAS) of the Nuclear Weapons Complex at http://cio.doe.gov/sqas.

2.4 Findings and Recommendations

It is the consensus of SQA and safety staffs that regular management attention from local DOE offices and its contractors is necessary to implement improvements in safety analysis and 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.

2.4.1 Findings

Several findings of governance and responsibility became apparent in the review of Departmental standards. These findings influence the implementation of standards since they establish protocols.

Finding No. 1: The Nuclear Safety Rule (10 CFR 830, Nuclear Safety Management) addresses the adequacy of "documented safety analysis" for nuclear facilities and activities and for non-nuclear hazardous facilities and activities, which could potentially impact the safety of nuclear operations. QA is very instrumental to assuring adequate documentation.

Finding No. 2: SQA needs to be addressed within the context of the overall quality assurance program for DOE's defense nuclear facilities, especially considering the criteria in 10 CFR 830, Nuclear Safety Management.

Finding No. 3: The Integrated Safety Management program, which evolved from DNFSB Recommendation 95-2, was expanded by the Safety Management Implementation Team (SMIT) to include both nuclear facilities and other hazardous (non-nuclear) facilities. The work of SMIT has been completed and implementation will be the responsibility of the DOE Cognizant Secretarial Offices (CSO) and contractors.

Finding No. 4: The DNFSB sent a letter to the Deputy Secretary on July 10, 2000, stating that ISM (includes QA integration) should be implemented by line management; i.e., each Program Secretarial Office (PSO), and not delegated to Environment, Safety and Health (EH) as it would be counter-productive. Because EH is not part of line management, the organization provides a better role as an independent assessor.

Finding No. 5: EH is the Office of Primary Interest (OPI) and owner of the QA rule (10 CFR 830.120); DOE O 414.1A, QUALITY ASSURANCE; and associated guides. Technical safety requirements are contained in the EH directives.

Finding No. 6: The OCIO has primary responsibility for software directives (e.g., Orders, Guides, Policies, etc.) per the Clinger-Cohen Act and must set expectations for software management, engineering, and assurance, and other information management requirements per OMB Circular A-130 and the Paperwork Reduction Act (as well as other legislation). The DOE computing environment has become very diverse and complex so that the software cannot be considered an entity of its own, but part of a larger total systems context that includes the infrastructure upon which it is executed. DOE is highly dependent on software not just only for information generation but to ensure that the software reflects the processes and scenarios needed for conducting its missions and businesses.

Finding No. 7: Information security; i.e., protecting the data, is a major issue for software systems. One of the strongest defenses against viruses and terrorist attacks is well-developed code that is structured, modular, and includes the inline information needed for understanding the code, as well as other documentation, so that updates can be made easily, swiftly, and cost-effectively. It is very beneficial for all software to undergo SQA, and of utmost importance that mission-critical, mission-essential, or high-risk code undergo SQA processes to ensure quality software is produced. SQA (as well as project management and software systems engineering) increases quality and saves time and money in the near and long term.

Finding No. 8: All Departmental Orders need to have the Secretary as the issuing authority for application to both DOE and NNSA.

2.4.2 Recommendations

As a result of the analysis of the data collected in the survey and the independent evaluation and the comparison of this information to the Departmental standards infrastructure, the following recommendations are made.

Recommendation No. 1: DOE Directives. DOE contractors have been consistently apprised by DOE rules, Orders, and guides of their responsibility to apply nationally recognized safety, safety analysis, and quality assurance standards to their work involving software. Departmental directives pertinent to software/SQA and safety/safety analysis are listed in Attachment 2.

Recommend DOE program and project managers become familiar with DOE directives as they relate to their projects and ensure their projects are in compliance with all applicable DOE directives. A memo from each LPSO to their organizations would be very conducive to ensuring this occurs.

Recommend the OCIO and EH conduct a more in-depth review of their directives for currency and ways to ensure their implementation.

Recommendation No. 2: DOE Standards. Before a project begins, the standards and processes that will be followed should be clearly defined. The DOE program manager and the DOE or contractor project manager should be aware of the international, national, Federal, and DOE information technology standards that should be specified or recommended for a particular type of project. There are several sources for determining these standards as noted in this study. Program and project managers should select and apply the most appropriate standards and best practices that will enable their projects to satisfy the requirements of DOE directives. Departmental standards and Departmental recommended standards pertinent to software/SQA and safety/safety analysis are listed in Attachment 2.

Recommend LPSOs affirm their support of OCIO and EH standards programs and processes. A memo from each LPSO reminding their staffs of these programs and encouraging participation would be conducive to ensuring DOE standards are consensus-based and appropriate and current for DOE.

Recommend the OCIO and EH conduct benchmarking activities of their standards program with other government organizations.

Recommendation No. 3: Other Government and Industry Standards and Best Practices. Adoption and tailoring of computer software engineering, project management, and quality assurance standards and best practices from related other government and industry are desirable. A consensus set of standards and best practices is conducive to ensuring consistency of practice and pedigree of DOE software. Software standards for adoption Departmentwide should be submitted to the Departmental Information Architecture (IA) Standards staff, located in the OCIO, for incorporation into the DOE IA Profile of Adopted Standards document. Website addresses for the government and industry organizations reviewed are contained in Attachment 1.

Recommend the OCIO review and solicit Departmental comments for a consensus set of standards for software project management, engineering, and quality assurance.

Recommend EH review and solicit Departmental comments for a consensus set of standards for safety software and for safety and safety analysis projects which involve software.

Recommendation No. 4: Quality Software Products. Production and delivery of quality software products should be ensured. Quality assurance alone will not provide a quality product. Quality software products are developed by applying quality processes throughout the software lifecycle. To build quality in throughout the lifecycle, a software engineering methodology should be used. This methodology should include software engineering and project management best practices (e.g., project planning, project tracking and oversight, configuration management, requirements management, quality assurance, risk management, and training) and incorporate SQA. Quality assurance of the software can and should extend beyond the software itself and into the infrastructure and environment in which it is executed to ensure successful integration of the software.

Recommend the draft update of DOE G 200.1-1, SOFTWARE ENGINEERING METHODOLOGY (SEM), be submitted to the Directives system in FY 2002. A memo from the LPSOs endorsing the SEM would be conducive to ensuring quality software is produced.

Recommendation No. 5: Tools/Automation. As the DOE computing environment becomes more complex, it is increasingly difficult to rely on manual processes. For all projects, the use of information technology to automate elements of the software quality assurance processes and procedures selected is encouraged wherever it is found to be effective.

Recommend that LPSOs consider and encourage new technologies which would be conducive to ensuring quality software.

Recommendation No. 6: Link Organizations and Websites and Improve Line Management. It appears DOE has an adequate Federal and contractor organizational infrastructure. However, there seems to be a lack of interaction among these organizations and staffs. Contractor organizations such as SQAS, DOE INCOSE, and EFCOG SAWG need to be better aligned with the OCIO, QAWG, and SASG for better communication and dissemination of software and safety information. The QAWG has revised its charter and developed an organizational matrix as guidance for improving this linkage.

Recommend that the various Federal and contractor organizations link themselves through their websites and the websites established by the Program Offices and field sites for software and safety for the purpose of improving communications.

Recommend that better communication lines are defined for line management organizations to ensure that everyone can be apprised of issues, concerns, new practices, etc.

Recommendation No. 7: Followup Study. A more in-depth study of software used in safety analysis and I&C software at defense nuclear facilities needs to be conducted. The survey provided some high-level information, but more details are needed. The Safety Analysis Software Group (SASG) has been formed to address standards for software used in safety analysis and I&C at defense nuclear facilities.

Recommend LPSOs endorse and support the SASG and that the SASG share SQA implementations for safety software with the OCIO and QAWG. Planned deliverables of the SASG are a report of their in-depth study, including training opportunities, and possibly a toolbox of codes and consensus set of standards.

Recommend the SASG answer the following questions: What improvements can be made? Are DOE directives and standards adequate? Is there an adequate infrastructure for disseminating and promoting standards? Is there adequate interaction with government and industry organizations? Are any joint ventures needed? Are standards adequately covered in contracts? What improvements are needed in safety software management? Is software management and SQA adequate? Does safety analysis and I&C have a foundation?

3.0 Institutionalization and Follow-through

In addition to the actions recommended in Section 2.4.2, there are various ways to institutionalize and ensure continuation of the recommendations. It is important to institutionalize and provide follow-through to ensure improvements occur.

3.1 Promotion and Awareness

DOE governance groups can be a source for providing promotion and awareness of the need to have quality software and standards. These groups include the Executive Committee for Information Management (ECIM), the DOE CIO Council, the Quality Assurance Working Group (QAWG), and potentially the Safety Analysis Software Group (SASG). The OCIO and EH should take advantage to bring software issues and concerns to these groups.

Contractor groups such as the Software Quality Assurance Subcommittee (SQAS) and the Energy Facilities Contractor Group (EFCOG) Safety Analysis Working Group (SAWG) can be very instrumental in institutionalizing software quality and safety management. The OCIO and EH should form closer working relationships with these groups.

3.2 Web Linkages

Most of the organizations above in Section 3.1 have established websites. All of these should be linked, which would be conducive to ensuring better communication and sharing.

3.3 Update and Adoption Processes

Both the OCIO and EH have a standards program and processes that provide for DOE participation in these programs to update or adopt new standards. These programs can and are very conducive for ensuring improvements are made in the way DOE does business. A better integration with the Directives system for information sharing should be considered by both organizations, such as a direct link from the Directives Explorer website to the OCIO and EH standards websites.

3.4 Auditing Processes

DOE Federal and contractor organization auditing processes can be used to ensure software and safety standards are reviewed, where applicable. This would help to promote, keep current, and continually provide an awareness of the importance of standards.

The following is a listing of the websites for the organizations discussed in this study report.

LISTING OF STANDARDS ORGANIZATIONS		
DOE Websites		
DSEPG	Departmentwide Systems Engineering Process Group	http://cio.doe.gov/smp (soon to be http://cio.doe.gov/sqse)
Explorer	Directives System	http://www.explorer.doe.gov:1776/htmls/directives.html
FTCP	Federal Technical Capability Panel	http://tis.eh.doe.gov/
Science	Good Practices Guides	http://www.er.doe.gov/ once on the site add production/er-80/er-82/gpguides.html
OCIO	Information Architecture Standards Program	http://cio.doe.gov/standards
QAWG	Quality Assurance Working Group	http://twilight.saic.com/qawg
EH	Technical Standards Program	http://tis.eh.doe.gov/techstds/
Contractor Websites		
EFCOG/SAWG	Energy Facilities Contracting Group/Safety Analysis Working Group	http://www.efcog.org/
SQAS	Software Quality Assurance Subcommittee	http://cio.doe.gov/sqas
NWC	Product Realization Process (includes Technical Business Practices, QC-1, and D&P Manual)	http://prp.lanl.gov:8686/
Other Government Websites		
Air Force	Air Force Safety Center	http://www.usaf.com/orgs/12.htm
DISA	Defense Information Systems Agency	http://www.disa.mil
DISA	Defense Information Systems Agency Standards Library	http://www.itsi.disa.mil
DISA	Defense Technical Information Center	http://www.dtic.mil
DTRA	Defense Threat Reduction Agency	http://www.dtra.mil
DOD	Department of Defense	http://www.defenselink.mil
DODSSP	DOD Single Stock Point	http://dodssp.daps.mil

LISTING OF STANDARDS ORGANIZATIONS		
DODSSP	DOD Single Stock Point - ASSIST	http://dodssp.daps.mil/assist.htm
DOT	Department of Transportation	http://www.dot.gov
DOT	Department of Transportation Standards	http://www.its.dot.gov/Standard/Standard.htm
Joint SSSH	Joint Software System Safety Handbook	http://www.system-safety.org
NASA	National Aeronautical and Space Administration	http://www.nasa.gov
NASA	National Aeronautical and Space Administration Search	http://www.nasa.gov/search
NASA	National Aeronautical and Space Administration Ames	http://www.arc.nasa.gov
NASA	National Aeronautical and Space Administration High Performance	http://hpcc.arc.nasa.gov
NASA	National Aeronautical and Space Administration ISCO and SIPS	http://www.nas.nasa.gov/IT/test/index.htm
NIST	National Institutes of Standards and Technology	http://www.nist.gov
NIST/ISO	National Institutes of Standards and Technology ISONET	http://ts.nist.gov/ts/htdocs/210/217/bro.htm
NIST/SQA	National Institutes of Standards and Technology SQA Standard	http://hissa.ncsl.nist.gov/publications/nistir4909/
Navy/NSWC	Navy Surface Warfare Center	http://www.nswc.navy.mil/safety
NRC	Nuclear Regulatory Commission Safety Standards	http://www.nrc.gov/NRC/RG/01/index.html
NRC	Nuclear Regulatory Commission Standards	http://www.nrc.gov/NRC/REFERENCE/STANDARDS/index.html
Industry Websites		
ANSI	American National Standards Institute	http://www.ansi.org
ANSI	American National Standards Institute Standards	http://www.nssn.org
ANS	American Nuclear Society	http://www.ans.org
ANS	American Nuclear Society Standards	http://store.ans.org
ASME	American Society of Mechanical Engineers	http://www.asme.org
ASQ	American Society for Quality	http://www.asq.org
EIA	Electronic Industries Alliance	http://www.eia.org
IEEE	The Institute of Electrical and Electronics Engineers	http://www.ieee.org

LISTING OF STANDARDS ORGANIZATIONS		
IEEE	The Institute of Electrical and Electronics Engineers Standards	http://standards.ieee.org
INCOSE	International Council on Systems Engineering	http://www.incose.org
ISO	International Organization for Standardization	http://www.iso.ch
ISC	International Safety Council	http://safety.webfirst.com/isc.htm
NSC	National Safety Council	http://nsc.org/
PMI	The Project Management Institute	http://www.pmi.org
QAI	The Quality Assurance Institute	http://www.qaiusa.com
SAE	Society for Automotive Engineers	http://www.sae.org or http://www.normas.com
SEI	Software Engineering Institute	http://www.sei.cmu.edu
SEI	Software Engineering Institute Search	http://www.sei.cmu.edu/about/website/search.html
SSS	System Safety Society	http://www.system-safety.org

Note: Check http://cio.doe.gov/smp (soon to http://cio.doe.gov/sqse) or http://cio.doe.gov/sqas or http://cio.doe.gov/asci for other useful webs links not reviewed for this report.

The following is a listing of the directives discussed in this study report.

LISTING OF DEPARTMENTAL DIRECTIVES AND STANDARDS		
DOE Safety and Safety Analysis Policies, Orders, Manuals, Standards		
DOE P 450.4	SAFETY MANAGEMENT SYSTEM POLICY	Defines the policy for integrating safety into management and work practices at all levels and all facets of work planning and execution based on six components. Quality assuran is implied in Component 3, Core Functions for Integrated Safety Management, by requiring a confirmation of readiness, feedback, oversight, and continuous improvement. DOE G 450.4-1A is the implementing guide.
DOE P 450.5	LINE ENVIRONMENT, SAFETY AND HEALTH OVERSIGHT	Defines the policy for Federal and contractor staffs to conduct Environment, Safety, and Health line oversight in a cost-effective, coordinated, integrated, and efficient manner. Quality assurance is implied by requiring compliance with applicable requirements, readiness assessments, verification reviews, for-cause reviews, and performance improvement.
DOE O 420.1	FACILITY SAFETY	Establishes facility safety requirements related to nuclear safety design, criticality safety, fire protection and natural phenomena hazards mitigation. It references standards requi for certain safety applications, such as ANS-8.1-1983 that includes requirements for validating computer programs. DOE G 420.1-1 is the implementing guide.
DOE O 5480.21	UNREVIEWED SAFETY QUESTIONS	Sets forth the definition and basis for determining the existence of an Unreviewed Safety Question (USQ). The intent of this Order is to provide contractors with the flexibility needed to conduct day-to-day operations and to require that those issues with a potential impact on the authorization basis, and therefore the safety of the facility, be brought to th attention of DOE–thus maintaining the proper safety focus. The Order is focused on saf analysis of facilities, of which software could be a factor.
DOE O 5480.22	TECHNICAL SAFETY REQUIREMENTS	States the requirements to have Technical Safety Requirements (TSR) prepared for DOE nuclear facilities and to delineate the criteria, content, scope, format, approval process, a reporting requirements of these documents and revisions thereof. The Order is focused o technical safety requirements of facilities, of which software could be a factor.

LISTING OF DEPARTMENTAL DIRECTIVES AND STANDARDS		
DOE Safety and Safety Analysis Policies, Orders, Manuals, Standards		
DOE O 5480.23	NUCLEAR SAFETY ANALYSIS REPORTS	Establishes requirements for contractors responsible for the design, construction, operati decontamination, or decommissioning of nuclear facilities to develop safety analyses thai establish and evaluate the adequacy of the safety bases of the facilities and to document t in Safety Analysis Reports (SAR), which includes addressing quality assurance.
DOE M 411.1-A	SAFETY MANAGEMENT FUNCTIONS, RESPONSIBILITIES, AND AUTHORITIES	Is a mechanism for implementing the Department's guiding principles established in DC P 450.4, discussed above, and the safety management functions outlined in DOE P 411.] SAFETY MANAGEMENT FUNCTIONS, RESPONSIBILITIES, AND AUTHORITIE POLICY.
DOE G 421.1-1	GOOD PRACTICES GUIDE	Is a comprehensive guidance document to assist in developing a criticality safety prograi to implement the DOE Order (or Rule) on nuclear criticality safety, and the invoked ANSI/ANS standards, through use of good practices. It provides brief information on S(and verification, and an appendix on software configuration control procedure.
DOE-STD-1027-92	HAZARD CATEGORIZATION AND ACCIDENT ANALYSIS TECHNIQUES FOR COMPLIANCE WITH DOE ORDER 5480.23, NUCLEAR SAFETY ANALYSIS REPORTS	Establishes guidance for the preparation and review of hazard categorization and accide analyses techniques.
DOE-STD-3009-94	PREPARATION GUIDE FOR U.S. DOE NONREACTOR NUCLEAR FACILITY SAFETY ANALYSIS REPORTS	Establishes guidance for consistency with DOE O 5480.23 requirements and its safety guide, and describes a safety analysis report (SAR) preparation method for DOE. The standard contains a chapter on quality assurance.

LISTING OF DEPARTMENTAL DIRECTIVES AND STANDARDS		
DOE Safety and Safety Analysis Policies, Orders, Manuals, Standards		
DOE Software and Quality Assurance Policies, Orders, Manuals, Standards		
DOE O 200.1	INFORMATION MANAGEMENT	Was canceled in FY 2000. It contained no explicit requirements for software developme but did reference DOE G 200.1-1, SOFTWARE ENGINEERING METHODOLOGY. DOE O 1330.1D, COMPUTER SOFTWARE MANAGEMENT, (superseded by DOE (200.1) contained more explicit requirements for software development, including softwa quality assurance. A replacement Order is under development for DOE O 200.1.
DOE N 203.1	SOFTWARE QUALITY ASSURANCE	Specifies the requirements for an SQA program and SQA for projects. The Notice references DOE directives and industry standards applicable to safety or safety software. This Notice will be made into an Order.
DOE G 200.1-1	SOFTWARE ENGINEERING METHODOLOGY	Contains guidance in regards to the application of SQA on software projects. The Guide can and should be supplemented by site guidance to meet local needs.
DOE O 414.1A	QUALITY ASSURANCE	States the requirements for DOE elements and contractors to develop Quality Assurance Programs (QAPs). The Order 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. It is consistent with the American Society of Mechanical Engineers (ASME) NQA-1 standard, which includes criteria for SQA. DOE O 5700.6C, QUALITY ASSURANCE (superseded by DOE O 414.1A), sta that the quality criteria applied to all work and the items and services resulting from wor It referenced the national consensus standard ASME NQA-1.
DOE G 414.1-2	QUALITY ASSURANCE MANAGEMENT SYSTEM GUIDE FOR USE WITH 10 CFR 830.120 AND DOE O 414.1	Contains a section (4.6.3) related to the Design Process, which calls for validation of the software used in the design process and refers to ASME NQA-1 for acceptable methods. This guide superseded DOE G 830.120, which was issued to implement 10 CFR 830.12(Quality Assurance. This guide clearly referenced the ASME NQA Part 2.7 for SQA.

LISTING OF DEPARTMENTAL DIRECTIVES AND STANDARDS		
DOE Safety and Safety Analysis Policies, Orders, Manuals, Standards		
DOE-STD-4001-2000	DOE DESIGN CRITERIA STANDARD FOR ELECTRONIC RECORDS MANAGEMENT SOFTWARE APPLICATIONS	Establishes the recommended method for meeting the functional requirements of the law and regulations pertaining to managing records using electronic Records Management Application (RMA) software (submitted to the DOE Technical Standards program by th OCIO).

LISTING OF DEPARTMENTAL DIRECTIVES AND STANDARDS		
DOE Safety and Safety Analysis Policies, Orders, Manuals, Standards		
DOE Information Architecture Profile of Adopted Standards 2000		
DOE G 200.1-1A (Draft)	DOE Software Engineering Methodology (SEM) Version 2 (1999)	Is a lifecycle methodology providing guidance for software engineering, project management, and quality assurance.
DOE-STD-4001-2000	DOE Design Criteria Standard for Electronic Records Management Software Applications, March 2000	Establishes the recommended method for meeting the functional requirements of the law and regulations pertaining to managing records using electronic Records Management Application (RMA) software (submitted to the DOE Technical Standards program by th OCIO).
IEEE 828-1988	IEEE Standard for Software Configuration Management Plans	Establishes minimum required contents of a software configuration management plan ar defines specific activities to be addressed.
IEEE 1042-1987 (R1993)	Guide to Software Configuration Management	Discusses context, process, implementation, tools, techniques, supplier control, records management, and planning methodologies for software configuration management.
ISO 9000	Quality Management and Quality Assurance Standards - Guidelines for Selection and Use	Contains a consensus on the essential features of a quality system to ensure the effective operation of a business, whether a manufacturer or service provider, or other type of organization, either in the public or private sector.
ISO 10005:1995	Quality Management - Guidelines for Quality Plans	Provides guidance for preparing quality plans for control of specific products, projects, o contracts.
EH Recommended Industry Standards (Not in the IA Profile of Standards)		
ANSI/ANS-10.4-1987	Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry	Contains guidelines for software used in nuclear applications
ASME NQA-1-1997	Quality Assurance Requirements for Computer Software for Nuclear Facility Applications	Contains guidelines for software used in nuclear applications

SURVEY RESULTS FOR STANDARDS AT DEFENSE NUCLEAR FACILITIES – Section 1

Survey on Software Quality Assurance (SQA) Practices, Processes, and Procedures Impacting Safety Analysis and Instrumentation and Control (I&C) Software Information Request for Response to Defense Nuclear Facilities Safety Board (DNFSB) Technical Report 25

Note: The response to the survey should not include non-nuclear facilities since the DNFSB issues are exclusively with nuclear facilities. The survey, however, does include hazardous chemicals present at nuclear facilities. The survey is directed at contractors; however, DOE Federal organizations may complete the survey as their input might provide additional insight.

Survey Targets: LLNL, LANL, SNL, SRS, Pantex, Rocky Flats, Y-12, INEEL, Nevada Test Site, Hanford (including ORP), WIPP, and ORNL. Only response from ORNL is the Y-12 survey. The Nevada Test Site stated they had no nuclear facilities. Although not a major target, YMP submitted a survey.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION		
1. What documented SQA programs or procedures do you follow for computer codes used for safety analysis in the areas of software development, testing, documentation, maintenance, and usage?		
Development	LLNL	HCD/ABS--One code, HOTSPOT, was developed within HCD. No formal QA procedures.
	LANL	Varies by customer (note the majority of safety codes used for safety analysis of LANL nuclear facilities are not LANL developed codes). For specific customers, "Manufacturing Manual: Software Quality Assurance"; MFG-AP-0014 Rev. 0; and "Tru Waste Characterization Program: TWCP Quality Procedure", TWCP-QP-1.1-006 Rev. 7 are used.
	SNL	TA-V RREP QA Procedure, RREP 3-2, Computer Software Control; developed in-house, is mandatory for all software associated with the TA-V Nuclear Facilities; QA processes are peer review and testing.
	SRS	WSMS follows WSRC requirements on developing, testing, documenting, maintaining, and using computer codes used for safety analysis. Requirements are specified in standalone WSMS QA documentation, or are cited and referenced in WSRC documentation. This includes but is not limited to, the WSRC 1Q Manual, 11Q, Section 20-1, the E7 Manual, and WSMS Quality Assurance Procedures. Procedures are in-house developed and mandatory; QA processes are peer review.
	Pantex	In-house developed Software Quality Life Cycle (SQLC) Plant Standard STD-1875. Mandatory for all site-developed software, purchased software, contractor developed software, or design agency furnished software. The SQA process consists of peer reviews and approvals, and auditing.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION

	Rocky Flats	The Computer Software Management Manual (1-MAN-004-CSMM) contains the procedures followed for software development, testing, documentation, and maintenance. This manual was developed in-house using best industry practices and is mandatory; QA processes are peer review and independent verification and validation. The processes invoked by the CSMM have been reviewed and audited by the Software Engineering Institute at Carnegie-Mellon University and given a SEI Level certification. They have also been reviewed and audited for Software Quality Assurance by the Carlsbad Area Office for WIPP certification. Since virtually all of the codes used in the nuclear safety areas are provided by outside sources (Oak Ridge, Los Alamos, RSICC, etc.) we cannot vouch for the SQA processes used by those developers. However, the implementation of the codes on site is guided by the CSMM and V&V testing is performed as part of the installation and configuration management process mandated by the CSMM.
	Y-12	Y80-100, *Project Initiation*, Y80-200, *Feasibility Study/Requirements Definition*, Y80-400, *Functional System Design*, Y80-500, *Computer System Design*, Y80-515, *Manufacturing Applications User Interface Standard*, and Y80-600, *Programming and Implementation*. The current software control program is defined by the, *Software Development and Control*, Y80 Series procedures; the upcoming revision will be based on DOE's Software Engineering Methodology (SEM). The Nuclear Criticality Safety organization uses the following safety-related software: (1) SCALE/KENO: Standard Computer Analyses for Licensing Evaluation and (2) MCNP: Monte Carlo N-particle Transport Code System. This software is controlled by the Y80 Series procedures including the Nuclear Criticality Safety organization procedures. The procedures were developed in-house at Y-12, based on software industry practices at the time. The procedures determine a software classification for each system based on various criteria. This classification is then used to drive the mandatory portions of the actual development process. It is mandatory that all Y-12 software use the Y80 procedures for guiding development. A combination of walkthroughs, reviews, and testing regimens are used as the basis for ensuring quality, per the Y80 procedures.
	INEEL	INEEL Program Requirements Document (PRD)-115, "Configuration Management;" INEEL Standard (STD)-107, "Configuration Management Program;" INEEL Management Control Procedure (MCP) 550, "Software Management"; INEEL MCP-3630, "Computer System Change Control;" INEEL Guide (GDE)-59, "Guide for Computer System Change Control;" DOE-STD-1073-93, "Guide for Operational Configuration Management Program;" ANSI/IEEE STD-828-1998;" IEEE Standard for Software Configuration Plans;" ANSI/ANS-10.4-1987, "Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry." Compliance with the INEEL documents is mandatory. Software packages developed and maintained at INEEL that are used for nuclear facility safety analysis or for control of active Safety SSCs are subject to the INEEL CM Program, have received verification and validation (V&V), and have CM Plans in place. See survey for description of INEEL documents.
	YMP/TESS	•NQA-2, Subpart 2.7 •OCRWM Quality Assurance Requirements & Description •OCRWM AP-SI.1Q Software Management •NQA-2, Subpart 2.7 is the NRC Standard for software development, testing, documentation, maintenance and usage. OCRWM Quality Assurance Requirements & Description (QARD) reflects in total the requirements of NQA-2, Subpart 2.7. AP-SI.1Q Software Management is the implementing procedure for Supplement I of the QARD. Compliance with AP-SI.1Q is mandatory. SQA processes include independent peer review, inspection, audit, and verification and validation of software.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION

	Hanford/RL	•Fluor Hanford--Primarily HNF-PRO-2778, *IRM Application System Life Cycle Standards* and HNF-PRO-309, *Computer Software Quality Assurance Requirements*. Procedures are in-house developed based on DOE Orders and other government agencies' requirements and mandatory. All the SQA processes listed in the survey are accepted in the procedures - they are based on defined scope and risk. The procedure requires that some form of change control and review process be established. Each project is allowed to define in their implementing procedures the specific configuration management processes they will apply. •Bechtel Hanford--In-house BHI-AT-01 Procedure 1.7 *Software Development & Maintenance*, and Bechtel Corp. Software Development Methodology Framework (SDMF). Procedures are based on industry standards and are mandatory. •PNNL Hanford–Any software developed or used at the Laboratory is required to be controlled in accordance with the Computer Software and Database Control subject area, which is aligned with the Software Systems Engineering Process (SSEP). The subject area was derived largely from the SSEP. The SSEP addresses each of the issues identified above. The subject area is mandatory for all PNNL staff. The SSEP is mandatory for all projects in the Information Science and Engineering Division and for all projects done for the Information Systems Engineering product line. The SSEP is more rigorous and more flexible than the subject area. However, each is based on the fundamental premise of defining a plan based on specific project or activity needs and executing the plan to develop, acquire, or use the software in involved. Both the subject area and the SSEP were developed at PNNL. The primary standard for the SSEP is the Software Engineering Institute's Capability Maturity Model for Software (see http://www.sei.cmu.edu/cmm/). It's also based to lesser extent on elements of IEEE standards, Department of Defense MIL-STD-498 (since replaced), and Iterative Process Models like the "Spiral Model" by Boehm and "Managed Evolutionary Development" by U.S. Patent Office.
	Hanford/ORP	•Tank Farm–HNF-PRO-309, *Computer Software Quality Assurance Requirements* and HNF-PRO-2778, *IRM Application System Life Cycle Standards*. Procedures developed in-house based on DOE Orders and other government agency requirements and are mandatory. Varying degrees of SQA processes are used based on the defined scope and risk of the specific project application. •Tank Waste–Procedure K70C515, *Code of Practice for Computer Program Use,* addresses all the elements of ASME NQA-1-1994, Part II, Subpart 2.7, including software life cycle, development and maintenance, software testing, software verification and validation, documentation, error identification and notification. Procedure was developed in-house based on the requirements of NQA-1-1994, Part II, Subpart 2.7 and DOE/RW/0333P, *Quality Assurance Requirements and Description (QARD)*, Supplement I. It is mandatory. SQA activities are installation testing and validation.
	WIPP	WP 16-IT3117, WIPP internal, mandatory, use-dependent; WP 16-2, WIPP internal, optional, use-dependent.
Testing	LLNL	HCD/ABS--HOTSPOT, EPI runs compared against ARAC runs by developer. Other codes (MACCS, MACCS II, ALOHA, GEN II) are widely used and accepted, but have no formal QA.
	LANL	Varies by customer. For specific customers, "Manufacturing Manual: Software Quality Assurance"; MFG-AP-0014 Rev. 0; and "Tru Waste Characterization Program: TWCP Quality Procedure", TWCP-QP-1.1-006 Rev. 7 are used.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION		
	SNL	TA-V RREP QA Procedure, RREP 3-2, Computer Software Control; developed in-house, is mandatory for all software associated with the TA-V Nuclear Facilities; QA processes are peer review and testing.
	SRS	WSMS follows WSRC requirements on developing, testing, documenting, maintaining, and using computer codes used for safety analysis. Requirements are specified in standalone WSMS QA documentation, or are cited and referenced in WSRC documentation. This includes but is not limited to, the WSRC 1Q Manual, 11Q, Section 20-1, the E7 Manual, and WSMS Quality Assurance Procedures. Procedures are in-house developed and mandatory; QA processes are peer review.
	Pantex	In-house developed Software Quality Life Cycle (SQLC) Plant Standard STD-1875. Mandatory for all site-developed software, purchased software, contractor developed software, or design agency furnished software. The SQA process consists of peer reviews and approvals, and auditing.
	Rocky Flats	The Computer Software Management Manual (1-MAN-004-CSSM) contains the procedures followed for software development, testing, documentation, and maintenance. This manual was developed in-house using best industry practices and is mandatory; QA processes are peer review and independent verification and validation.. The processes invoked by the CSMM have been reviewed and audited by the Software Engineering Institute at Carnegie-Mellon University and given a SEI Level certification. They have also been reviewed and audited for Software Quality Assurance by the Carlsbad Area Office for WIPP certification. Since virtually all of the codes used in the nuclear safety areas are provided by outside sources (Oak Ridge, Los Alamos, RSICC, etc.) we cannot vouch for the SQA processes used by those developers. However, the implementation of the codes on site is guided by the CSMM and V&V testing is performed as part of the installation and configuration management process mandated by the CSMM.
	Y-12	Y80-700, *Validation and Acceptance*. The current software control program is defined by the, *Software Development and Control*, Y80 Series procedures; the upcoming revision will be based on DOE's Software Engineering Methodology (SEM). The Nuclear Criticality Safety organization uses the following safety-related software: (1) SCALE/KENO: Standard Computer Analyses for Licensing Evaluation and (2) MCNP: Monte Carlo N-particle Transport Code System. This software is controlled by the Y80 Series procedures including the Nuclear Criticality Safety organization procedures. The procedures were developed in-house at Y-12, based on software industry practices at the time. The procedures determine a software classification for each system based on various criteria. This classification is then used to drive the mandatory portions of the actual development process. It is mandatory that all Y-12 software use the Y80 procedures for guiding development. A combination of walkthroughs, reviews, and testing regimens are used as the basis for ensuring quality, per the Y80 procedures.
	INEEL	INEEL Program Requirements Document (PRD)-115, "Configuration Management;" INEEL Standard (STD)-107, "Configuration Management Program;" INEEL Management Control Procedure (MCP) 550, "Software Management"; INEEL MCP-3630, "Computer System Change Control;" INEEL Guide (GDE)-59, "Guide for Computer System Change Control;" DOE-STD-1073-93, "Guide for Operational Configuration Management Program;" ANSI/IEEE STD-828-1998;" IEEE Standard for Software Configuration Plans;" ANSI/ANS-10.4-1987, "Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry." Compliance with the INEEL documents is mandatory. Software packages developed and maintained at INEEL that are used for nuclear facility safety analysis or for control of active Safety SSCs are subject to the INEEL CM Program, have received verification and validation (V&V), and have CM Plans in place. See survey for description of INEEL documents.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION

	YMP/TESS	•NQA-2, Subpart 2.7 •OCRWM Quality Assurance Requirements & Description •OCRWM AP-SI.1Q Software Management •OCRWM AP-SV.1Q Control of Electronic Management of Data •NQA-2, Subpart 2.7 is the NRC Standard for software development, testing, documentation, maintenance and usage. OCRWM Quality Assurance Requirements & Description (QARD) reflects in total the requirements of NQA-2, Subpart 2.7. AP-SI.1Q Software Management is the implementing procedure for Supplement I of the QARD. Compliance with AP-SI.1Q is mandatory. SQA processes include independent peer review, inspection, audit, and verification and validation of software.
	Hanford/RL	•Fluor Hanford--Primarily HNF-PRO-2778, *IRM Application System Life Cycle Standards* and HNF-PRO-309, *Computer Software Quality Assurance Requirements*. Procedures are in-house developed based on DOE Orders and other government agencies' requirements and mandatory. All the SQA processes listed in the survey are accepted in the procedures - they are based on defined scope and risk. The procedure requires that some form of change control and review process be established. Each project is allowed to define in their implementing procedures the specific configuration management processes they will apply. •Bechtel Hanford--In-house BHI-AT-01 Procedure 1.7, BHI-AT-01 Procedure 1.8 *Software Acquisition and Maintenance*, and BHI-DE-01-EDPI-4.36-01, *Project Calculations*. Procedures are based on industry standards and are mandatory. •PNNL Hanford–Any software developed or used at the Laboratory is required to be controlled in accordance with the Computer Software and Database Control subject area, which is aligned with the Software Systems Engineering Process (SSEP). The subject area was derived largely from the SSEP. The SSEP addresses each of the issues identified above. The subject area is mandatory for all PNNL staff. The SSEP is mandatory for all projects in the Information Science and Engineering Division and for all projects done for the Information Systems Engineering product line. The SSEP is more rigorous and more flexible than the subject area. However, each is based on the fundamental premise of defining a plan based on specific project or activity needs and executing the plan to develop, acquire, or use the software in involved. Both the subject area and the SSEP were developed at PNNL. The primary standard for the SSEP is the Software Engineering Institute's Capability Maturity Model for Software (see http://www.sei.cmu.edu/cmm/). It's also based to lesser extent on elements of IEEE standards, Department of Defense MIL-STD-498 (since replaced), and Iterative Process Models like the "Spiral Model" by Boehm and "Managed Evolutionary Development" by U.S. Patent Office.
	Hanford/ORP	•Tank Farm–HNF-PRO-309, *Computer Software Quality Assurance Requirements* and HNF-PRO-2778, *IRM Application System Life Cycle Standards*. Procedures developed in-house based on DOE Orders and other government agency requirements and are mandatory. Varying degrees of SQA processes are used based on the defined scope and risk of the specific project application. •Tank Waste–Procedure K70C515, *Code of Practice for Computer Program Use,* addresses all the elements of ASME NQA-1-1994, Part II, Subpart 2.7, including software life cycle, development and maintenance, software testing, software verification and validation, documentation, error identification and notification. Procedure was developed in-house based on the requirements of NQA-1-1994, Part II, Subpart 2.7 and DOE/RW/0333P, *Quality Assurance Requirements and Description (QARD)*, Supplement I. It is mandatory. SQA activities are installation testing and validation.
	WIPP	WP 16-IT3117, WIPP internal, mandatory, use-dependent; WP 16-2, WIPP internal, optional, use-dependent.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION

Documentation	LLNL	HCD/ABS--Manuals are available for codes. No formal QA was done for manual content.
	LANL	Varies by customer. For specific customers, "Manufacturing Manual: Software Quality Assurance"; MFG-AP-0014 Rev. 0; and "Tru Waste Characterization Program: TWCP Quality Procedure", TWCP-QP-1.1-006 Rev. 7 are used.
	SNL	TA-V RREP QA Procedure, RREP 3-2, Computer Software Control; developed in-house, is mandatory for all software associated with the TA-V Nuclear Facilities; QA processes are peer review and testing.
	SRS	WSMS follows WSRC requirements on developing, testing, documenting, maintaining, and using computer codes used for safety analysis. Requirements are specified in standalone WSMS QA documentation, or are cited and referenced in WSRC documentation. This includes but is not limited to, the WSRC 1Q Manual, 11Q, Section 20-1, the E7 Manual, and WSMS Quality Assurance Procedures. Procedures are in-house developed and mandatory; QA processes are peer review.
	Pantex	In-house developed Software Quality Life Cycle (SQLC) Plant Standard STD-1875. Mandatory for all site-developed software, purchased software, contractor developed software, or design agency furnished software. The SQA process consists of peer reviews and approvals, and auditing.
	Rocky Flats	The Computer Software Management Manual (1-MAN-004-CSSM) contains the procedures followed for software development, testing, documentation, and maintenance. This manual was developed in-house using best industry practices and is mandatory; QA processes are peer review and independent verification and validation.. The processes invoked by the CSMM have been reviewed and audited by the Software Engineering Institute at Carnegie-Mellon University and given a SEI Level certification. They have also been reviewed and audited for Software Quality Assurance by the Carlsbad Area Office for WIPP certification. Since virtually all of the codes used in the nuclear safety areas are provided by outside sources (Oak Ridge, Los Alamos, RSICC, etc.) we cannot vouch for the SQA processes used by those developers. However, the implementation of the codes on site is guided by the CSMM and V&V testing is performed as part of the installation and configuration management process mandated by the CSMM.
	Y-12	Required deliverables provided at the end of each procedure. The current software control program is defined by the, *Software Development and Control*, Y80 Series procedures; the upcoming revision will be based on DOE's Software Engineering Methodology (SEM). The Nuclear Criticality Safety organization uses the following safety-related software: (1) SCALE/KENO: Standard Computer Analyses for Licensing Evaluation and (2) MCNP: Monte Carlo N-particle Transport Code System. This software is controlled by the Y80 Series procedures including the Nuclear Criticality Safety organization procedures and Y/DD-834 "LMES Y-12 Nuclear Criticality Safety Software application Software Document for the HP C-180 Workstation". The procedures were developed in-house at Y-12, based on software industry practices at the time. The procedures determine a software classification for each system based on various criteria. This classification is then used to drive the mandatory portions of the actual development process. It is mandatory that all Y-12 software use the Y80 procedures for guiding development. A combination of walkthroughs, reviews, and testing regimens are used as the basis for ensuring quality, per the Y80 procedures.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION		
	INEEL	INEEL Program Requirements Document (PRD)-115, "Configuration Management;" INEEL Standard (STD)-107, "Configuration Management Program;" INEEL Management Control Procedure (MCP) 550, "Software Management"; INEEL MCP-3630, "Computer System Change Control;" INEEL Guide (GDE)-59, "Guide for Computer System Change Control;" DOE-STD-1073-93, "Guide for Operational Configuration Management Program;" ANSI/IEEE STD-828-1998;" IEEE Standard for Software Configuration Plans;" ANSI/ANS-10.4-1987, "Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry." Compliance with the INEEL documents is mandatory. Software packages developed and maintained at INEEL that are used for nuclear facility safety analysis or for control of active Safety SSCs are subject to the INEEL CM Program, have received verification and validation (V&V), and have CM Plans in place. See survey for description of INEEL documents.
	YMP/TESS	•NQA-2, Subpart 2.7 •OCRWM Quality Assurance Requirements & Description •OCRWM AP-SI.1Q Software Management •NQA-2, Subpart 2.7 is the NRC Standard for software development, testing, documentation, maintenance and usage. OCRWM Quality Assurance Requirements & Description (QARD) reflects in total the requirements of NQA-2, Subpart 2.7. AP-SI.1Q Software Management is the implementing procedure for Supplement I of the QARD. Compliance with AP-SI.1Q is mandatory. SQA processes include independent peer review, inspection, audit, and verification and validation of software.
	Hanford/RL	•Fluor Hanford--Primarily HNF-PRO-2778, *IRM Application System Life Cycle Standards* and HNF-PRO-309, *Computer Software Quality Assurance Requirements.* Procedures are in-house developed based on DOE Orders and other government agencies' requirements and mandatory. All the SQA processes listed in the survey are accepted in the procedures - they are based on defined scope and risk. The procedure requires that some form of change control and review process be established. Each project is allowed to define in their implementing procedures the specific configuration management processes they will apply. •Bechtel Hanford--In-house BHI-AT-01 Procedure 1.7, BHI-AT-01 Procedure 1.8 *Software Acquisition and Maintenance*, and BHI-DE-01-EDPI-4.36-01, *Project Calculations.* Procedures are based on industry standards and are mandatory. •PNNL Hanford--Any software developed or used at the Laboratory is required to be controlled in accordance with the Computer Software and Database Control subject area, which is aligned with the Software Systems Engineering Process (SSEP). The subject area was derived largely from the SSEP. The SSEP addresses each of the issues identified above. The subject area is mandatory for all PNNL staff. The SSEP is mandatory for all projects in the Information Science and Engineering Division and for all projects done for the Information Systems Engineering product line. The SSEP is more rigorous and more flexible than the subject area. However, each is based on the fundamental premise of defining a plan based on specific project or activity needs and executing the plan to develop, acquire, or use the software in involved. Both the subject area and the SSEP were developed at PNNL. The primary standard for the SSEP is the Software Engineering Institute's Capability Maturity Model for Software (see http://www.sei.cmu.edu/cmm/). It's also based to lesser extent on elements of IEEE standards, Department of Defense MIL-STD-498 (since replaced), and Iterative Process Models like the "Spiral Model" by Boehm and "Managed Evolutionary Development" by U.S. Patent Office.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION		
	Hanford/ORP	•Tank Farm–HNF-PRO-309, *Computer Software Quality Assurance Requirements* and HNF-PRO-2778, *IRM Application System Life Cycle Standards*. Procedures developed in-house based on DOE Orders and other government agency requirements and are mandatory. Varying degrees of SQA processes are used based on the defined scope and risk of the specific project application. •Tank Waste--Procedure K70C515, *Code of Practice for Computer Program Use,* addresses all the elements of ASME NQA-1-1994, Part II, Subpart 2.7, including software life cycle, development and maintenance, software testing, software verification and validation, documentation, error identification and notification. Procedure was developed in-house based on the requirements of NQA-1-1994, Part II, Subpart 2.7 and DOE/RW/0333P, *Quality Assurance Requirements and Description (QARD)*, Supplement I. It is mandatory. SQA activities are installation testing and validation.
	WIPP	WP 16-IT3117, WIPP internal, mandatory, use-dependent; WP 16-2, WIPP internal, optional, use-dependent.
Maintenance	LLNL	HCD/ABS–HOTSPOT and EPI are tested by the developer with standard runs after modification. No formal QA documentation. Other codes are purchased or adopted when they become available. They are informally QA'd by comparison with older versions and other applicable codes.
	LANL	Varies by customer. For specific customers, "Manufacturing Manual: Software Quality Assurance"; MFG-AP-0014 Rev. 0; and "Tru Waste Characterization Program: TWCP Quality Procedure", TWCP-QP-1.1-006 Rev. 7 are used.
	SNL	TA-V RREP QA Procedure, RREP 3-2, Computer Software Control; developed in-house, is mandatory for all software associated with the TA-V Nuclear Facilities; QA processes are peer review and testing.
	SRS	WSMS follows WSRC requirements on developing, testing, documenting, maintaining, and using computer codes used for safety analysis. Requirements are specified in standalone WSMS QA documentation, or are cited and referenced in WSRC documentation. This includes but is not limited to, the WSRC 1Q Manual, 11Q, Section 20-1, the E7 Manual, and WSMS Quality Assurance Procedures.
	Pantex	In-house developed Software Quality Life Cycle (SQLC) Plant Standard STD-1875. Mandatory for all site-developed software, purchased software, contractor developed software, or design agency furnished software. The SQA process consists of peer reviews and approvals, and auditing.
	Rocky Flats	The Computer Software Management Manual (1-MAN-004-CSSM) contains the procedures followed for software development, testing, documentation, and maintenance. This manual was developed in-house using best industry practices and is mandatory; QA processes are peer review and independent verification and validation.. The processes invoked by the CSMM have been reviewed and audited by the Software Engineering Institute at Carnegie-Mellon University and given a SEI Level certification. They have also been reviewed and audited for Software Quality Assurance by the Carlsbad Area Office for WIPP certification. Since virtually all of the codes used in the nuclear safety areas are provided by outside sources (Oak Ridge, Los Alamos, RSICC, etc.) we cannot vouch for the SQA processes used by those developers. However, the implementation of the codes on site is guided by the CSMM and V&V testing is performed as part of the installation and configuration management process mandated by the CSMM.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION

	Y-12	Y80-800, *Configuration Control*. The current software control program is defined by the, *Software Development and Control*, Y80 Series procedures; the upcoming revision will be based on DOE's Software Engineering Methodology (SEM). The Nuclear Criticality Safety organization uses the following safety-related software: (1) SCALE/KENO: Standard Computer Analyses for Licensing Evaluation and (2) MCNP: Monte Carlo N-particle Transport Code System. This software is controlled by the Y80 Series procedures including the Nuclear Criticality Safety organization procedures. The procedures were developed in-house at Y-12, based on software industry practices at the time. The procedures determine a software classification for each system based on various criteria. This classification is then used to drive the mandatory portions of the actual development process. It is mandatory that all Y-12 software use the Y80 procedures for guiding development. A combination of walkthroughs, reviews, and testing regimens are used as the basis for ensuring quality, per the Y80 procedures.
	INEEL	INEEL Program Requirements Document (PRD)-115, "Configuration Management;" INEEL Standard (STD)-107, "Configuration Management Program;" INEEL Management Control Procedure (MCP) 550, Software Management"; INEEL MCP-3630, "Computer System Change Control;" INEEL Guide (GDE)-59, "Guide for Computer System Change Control;" DOE-STD-1073-93, "Guide for Operational Configuration Management Program;" ANSI/IEEE STD-828-1998;" IEEE Standard for Software Configuration Plans;" ANSI/ANS-10.4-1987, "Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry." Compliance with the INEEL documents is mandatory. Software packages developed and maintained at INEEL that are used for nuclear facility safety analysis or for control of active Safety SSCs are subject to the INEEL CM Program, have received verification and validation (V&V), and have CM Plans in place. See survey for description of INEEL documents.
	YMP/TESS	•NQA-2, Subpart 2.7 •OCRWM Quality Assurance Requirements & Description •OCRWM AP-SI.1Q Software Management •NQA-2, Subpart 2.7 is the NRC Standard for software development, testing, documentation, maintenance and usage. OCRWM Quality Assurance Requirements & Description (QARD) reflects in total the requirements of NQA-2, Subpart 2.7. AP-SI.1Q Software Management is the implementing procedure for Supplement I of the QARD. Compliance with AP-SI.1Q is mandatory. SQA processes include independent peer review, inspection, audit, and verification and validation of software.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION

	Hanford/RL	•Fluor Hanford--Primarily HNF-PRO-2778, *IRM Application System Life Cycle Standards* and HNF-PRO-309, *Computer Software Quality Assurance Requirements*. Procedures are in-house developed based on DOE Orders and other government agencies' requirements and mandatory. All the SQA processes listed in the survey are accepted in the procedures - they are based on defined scope and risk. The procedure requires that some form of change control and review process be established. Each project is allowed to define in their implementing procedures the specific configuration management processes they will apply. •Bechtel Hanford--In-house BHI-AT-01 Procedure 1.7, BHI-AT-01 Procedure 1.8 *Software Acquisition and Maintenance*, and BHI-DE-01-EDPI-4.36-01, *Project Calculations*. Procedures are based on industry standards and are mandatory. •PNNL Hanford–Any software developed or used at the Laboratory is required to be controlled in accordance with the Computer Software and Database Control subject area, which is aligned with the Software Systems Engineering Process (SSEP). The subject area was derived largely from the SSEP. The SSEP addresses each of the issues identified above. The subject area is mandatory for all PNNL staff. The SSEP is mandatory for all projects in the Information Science and Engineering Division and for all projects done for the Information Systems Engineering product line. The SSEP is more rigorous and more flexible than the subject area. However, each is based on the fundamental premise of defining a plan based on specific project or activity needs and executing the plan to develop, acquire, or use the software in involved. Both the subject area and the SSEP were developed at PNNL. The primary standard for the SSEP is the Software Engineering Institute's Capability Maturity Model for Software (see http://www.sei.cmu.edu/cmm/). It's also based to lesser extent on elements of IEEE standards, Department of Defense MIL-STD-498 (since replaced), and Iterative Process Models like the "Spiral Model" by Boehm and "Managed Evolutionary Development" by U.S. Patent Office.
	Hanford/ORP	•Tank Farm–HNF-PRO-309, *Computer Software Quality Assurance Requirements* and HNF-PRO-2778, *IRM Application System Life Cycle Standards*. Procedures developed in-house based on DOE Orders and other government agency requirements and are mandatory. Varying degrees of SQA processes are used based on the defined scope and risk of the specific project application. •Tank Waste--Procedure K70C515, *Code of Practice for Computer Program Use,* addresses all the elements of ASME NQA-1-1994, Part II, Subpart 2.7, including software life cycle, development and maintenance, software testing, software verification and validation, documentation, error identification and notification. Procedure was developed in-house based on the requirements of NQA-1-1994, Part II, Subpart 2.7 and DOE/RW/0333P, *Quality Assurance Requirements and Description (QARD)*, Supplement I. It is mandatory. SQA activities are installation testing and validation.
	WIPP	WP 16-IT3117, WIPP internal, mandatory, use-dependent; WP 16-2, WIPP internal, optional, use-dependent.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION		
Usage	LLNL	•HCD/ABS--Printouts of ALOHA, HOTSPOT, and EPI code runs are included with the safety basis documents and QA'd as part of the document. •HCD/ABS--HOTSPOT is an LLNL-developed code adopted by DOE for evaluation of potential doses (50-yr CEDE based on ICRP-30 dose conversion factors). HCD uses it when reviewing radioactive material releases. •HCD/ABS--EPI is a commercially available code (by the developer of HOTSPOT) that models toxic material releases, giving respirable airborne material concentration as a function of distance from release point. •HCD/ABS--ALOHA is a NOAA product that models toxic material releases, giving respirable airborne material concentration as a function of distance from release point. One of its uses at LLNL is to model liquid and condensed gas releases from tanks. •HCD/ABS--GEN II and MACCS are more complex codes that are not generally used by HCD analysts for safety basis documents.
	LANL	Varies by customer. For specific customers, "Manufacturing Manual: Software Quality Assurance"; MFG-AP-0014 Rev. 0; and "Tru Waste Characterization Program: TWCP Quality Procedure", TWCP-QP-1.1-006 Rev. 7 are used.
	SNL	TA-V RREP QA Procedure, RREP 3-2, Computer Software Control; developed in-house, is mandatory for all software associated with the TA-V Nuclear Facilities; QA processes are peer review and testing.
	SRS	WSMS follows WSRC requirements on developing, testing, documenting, maintaining, and using computer codes used for safety analysis. Requirements are specified in standalone WSMS QA documentation, or are cited and referenced in WSRC documentation. This includes but is not limited to, the WSRC 1Q Manual, 11Q, Section 20-1, the E7 Manual, and WSMS Quality Assurance Procedures. Procedures are in-house developed and mandatory; QA processes are peer review.
	Pantex	In-house developed Software Quality Life Cycle (SQLC) Plant Standard STD-1875. Mandatory for all site-developed software, purchased software, contractor developed software, or design agency furnished software. The SQA process consists of peer reviews and approvals, and auditing.
	Rocky Flats	This is determined by the specific software used by the analysts.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION		
	Y-12	Y80-900, *Post-Implementation Review*. The current software control program is defined by the, *Software Development and Control*, Y80 Series procedures; the upcoming revision will be based on DOE's Software Engineering Methodology (SEM). The Nuclear Criticality Safety organization uses the following safety-related software: (1) SCALE/KENO: Standard Computer Analyses for Licensing Evaluation and (2) MCNP: Monte Carlo N-particle Transport Code System. This software is controlled by the Y80 Series procedures including the Nuclear Criticality Safety organization procedures and Y70-68-005, *Quality Assurance for Nuclear Criticality Safety Computer Calculations*, Y/DD-833, Lockheed Martin Energy Systems Y-12 Nuclear Criticality Safety Organization Plan for Administration of the HP Workstation, Y/DD-573, *MMES Y-12 Nuclear Criticality Safety Software Validation of Keno V.a on the HP 9000/Series 700 Workstation*, Y/DD-790, *Validation of MCNP4A for Criticality Safety and Shielding Analyses on the HP-735*, and Y/DD-860, *Validation of MCNP4B2 for Criticality Safety and Shielding Analyses on the HP C-180*. The procedures were developed in-house at Y-12, based on software industry practices at the time. The procedures determine a software classification for each system based on various criteria. This classification is then used to drive the mandatory portions of the actual development process. It is mandatory that all Y-12 software use the Y80 procedures for guiding development. A combination of walkthroughs, reviews, and testing regimens are used as the basis for ensuring quality, per the Y80 procedures.
	INEEL	INEEL Program Requirements Document (PRD)-115, "Configuration Management;" INEEL Standard (STD)-107, "Configuration Management Program;" INEEL Management Control Procedure (MCP) 550, "Software Management"; INEEL MCP-3630, "Computer System Change Control;" INEEL Guide (GDE)-59, "Guide for Computer System Change Control;" DOE-STD-1073-93, "Guide for Operational Configuration Management Program;" ANSI/IEEE STD-828-1998;" IEEE Standard for Software Configuration Plans;" ANSI/ANS-10.4-1987, "Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry." Compliance with the INEEL documents is mandatory. Software packages developed and maintained at INEEL that are used for nuclear facility safety analysis or for control of active Safety SSCs are subject to the INEEL CM Program, have received verification and validation (V&V), and have CM Plans in place. See survey for description of INEEL documents.
	YMP/TESS	•NQA-2, Subpart 2.7 •OCRWM Quality Assurance Requirements & Description •OCRWM AP-SI.1Q Software Management •OCRWM AP-SV.1Q Control of Electronic Management of Data •NQA-2, Subpart 2.7 is the NRC Standard for software development, testing, documentation, maintenance and usage. OCRWM Quality Assurance Requirements & Description (QARD) reflects in total the requirements of NQA-2, Subpart 2.7. AP-SI.1Q Software Management is the implementing procedure for Supplement I of the QARD. Compliance with AP-SI.1Q is mandatory. SQA processes include independent peer review, inspection, audit, and verification and validation of software.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION

	Hanford/RL	•Fluor Hanford--Primarily HNF-PRO-2778, *IRM Application System Life Cycle Standards* and HNF-PRO-309, *Computer Software Quality Assurance Requirements*. Procedures are in-house developed based on DOE Orders and other government agencies' requirements and mandatory. All the SQA processes listed in the survey are accepted in the procedures - they are based on defined scope and risk. The procedure requires that some form of change control and review process be established. Each project is allowed to define in their implementing procedures the specific configuration management processes they will apply. •Bechtel Hanford--In-house BHI-AT-01 Procedure 1.7, BHI-AT-01 Procedure 1.8 *Software Acquisition and Maintenance*, and BHI-DE-01-EDPI-4.36-01, *Project Calculations*. Procedures are based on industry standards and are mandatory. •PNNL Hanford--Any software developed or used at the Laboratory is required to be controlled in accordance with the Computer Software and Database Control subject area, which is aligned with the Software Systems Engineering Process (SSEP). The subject area was derived largely from the SSEP. The SSEP addresses each of the issues identified above. The subject area is mandatory for all PNNL staff. The SSEP is mandatory for all projects in the Information Science and Engineering Division and for all projects done for the Information Systems Engineering product line. The SSEP is more rigorous and more flexible than the subject area. However, each is based on the fundamental premise of defining a plan based on specific project or activity needs and executing the plan to develop, acquire, or use the software in involved. Both the subject area and the SSEP were developed at PNNL. The primary standard for the SSEP is the Software Engineering Institute's Capability Maturity Model for Software (see http://www.sei.cmu.edu/cmm/). It's also based to lesser extent on elements of IEEE standards, Department of Defense MIL-STD-498 (since replaced), and Iterative Process Models like the "Spiral Model" by Boehm and "Managed Evolutionary Development" by U.S. Patent Office.
	Hanford/ORP	•Tank Farm–HNF-PRO-309, *Computer Software Quality Assurance Requirements* and HNF-PRO-2778, *IRM Application System Life Cycle Standards*. Procedures developed in-house based on DOE Orders and other government agency requirements and are mandatory. Varying degrees of SQA processes are used based on the defined scope and risk of the specific project application. •Tank Waste--Procedure K70C515, *Code of Practice for Computer Program Use,* addresses all the elements of ASME NQA-1-1994, Part II, Subpart 2.7, including software life cycle, development and maintenance, software testing, software verification and validation, documentation, error identification and notification. Procedure was developed in-house based on the requirements of NQA-1-1994, Part II, Subpart 2.7 and DOE/RW/0333P, *Quality Assurance Requirements and Description (QARD)*, Supplement I. It is mandatory. SQA activities are installation testing and validation.
	WIPP	WP 16-IT3117, WIPP internal, mandatory, use-dependent; WP 16-2, WIPP internal, optional, use-dependent.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION		
2. Do these procedures comply with the following guidelines?		
DOE O 420.1	LLNL	CSG--Criticality safety software complies with DOE O 420.1 requirements.
	LANL	In part
	SNL	Yes
	SRS	Yes
	Pantex	See "Other" below.
	Rocky Flats	In Whole
	Y-12	See "Other" – Y80 Series based on DOE guidance indicated below.
	INEEL	Implemented but not mapped
	YMP/TESS	Not Applicable
	Hanford/RL	•Fluor Hanford--DOE Order 420.1 is not in the Project Hanford Management Contract (PHMC); however, the following DOE Orders and FH procedures are in compliance with them: DOE 5480.28, *Natural Phenomena Hazards Mitigation* DOE 5480.7A, *Fire Protection* DOE 6430.1A, *General Design Criteria* DOE 5480.24, *Criticality Safety* •Bechtel Hanford--DOE Order 420.1 is not included in the ERC Contract at this time. However, the ERC procedures identified above are consistent with the requirement of DOE Order 420.1 •PNNL Hanford--Not in PNNL's contract yet. Not applicable. (DOE Orders 5480.24 and 5480.7A have been implemented.)
	Hanford/ORP	•Tank Farm–The SQA program was not written to satisfy DOE O 420.1 specifically, but in that DOE O 420.1 invokes 10CFR830.120, the SQA program does comply with DOE O 420.1. Specifically, DOE O 420.1 requires design of safety structures, systems and components (SSCs) to be performed under a quality assurance program that satisfies 10 CFR830.120. Our quality assurance program satisfies 10 CFR830.120. Specifically, under design, SQA requirements are addressed to ensure that safety SSCs that are designed with the use of software are properly controlled. •Tank Waste–Under the privatization concept and under the current "bridge" design effort the cited DOE Orders are not applicable; see section V, Additional Comments.
	WIPP	Yes, compliance in whole.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION		
DOE O 414.1	LLNL	HCD/ABS--Compliance with applicable sections of 10 CFR 830.120 — on-the-job training, peer and independent review of calculations, record keeping, approved procedures for use of codes
	LANL	In part
	SNL	Yes
	SRS	In part
	Pantex	Mapped, see "Other" below
	Rocky Flats	In Whole
	Y-12	See "Other", based on DOE O 5700.6C
	INEEL	Implemented but not mapped
	YMP/TESS	Full compliance
	Hanford/RL	•Fluor Hanford--This Order is implemented through HNF-MP-599, *PHMC Quality Assurance Program Description*. The applicable requirements of HNF-MP-599 are implemented by HNF-PRO-2778, *IRM Application System Life Cycle Standards* and HNF-PRO-309, *Computer Software Quality Assurance Requirements.* •Bechtel Hanford--DOE Order 414.1 is not included in the ERC Contract at this time. The ERC procedures are compliant with DOE Order 5700.6C as required by the Contract. •PNNL Hanford--The "Computer Software and Database Control" subject area is compliant with this order.
	Hanford/ORP	•Tank Farm–Yes •Tank Waste–Under the privatization concept and under the current "bridge" design effort the cited DOE Orders are not applicable; see section V, Additional Comments.
	WIPP	Yes, compliance in whole.
DOE O 200.1	LLNL	HCD/ABS–Yes
	LANL	In part
	SNL	Yes
	SRS	Uncertain
	Pantex	See "Other" below

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION

	Rocky Flats	In Whole
	Y-12	See "Other", based on DOE O 1360.1A
	INEEL	Implemented but not mapped
	YMP/TESS	Full compliance
	Hanford/RL	•Fluor Hanford--HNF-PRO-2778, *IRM Application Software System Life Cycle Standards* implements this Order. •Bechtel Hanford--DOE Order 200.1 is not included in the ERC Contract at this time. The ERC procedures are based on the Bechtel Corporate SDMF, which is consistent with DOE Order 200.1. •PNNL Hanford–Not in PNNL's contract yet. Not applicable. (DOE Order 1330.1D has been implemented.)
	Hanford/ORP	•Tank Farm–HNF-PRO-2778 implements this Order. •Tank Waste--Under the privatization concept and under the current "bridge" design effort the cited DOE Orders are not applicable; see section V, Additional Comments.
	WIPP	Yes, compliance in whole.
DOE G 200.1-1	LLNL	HCD/ABS--Not appropriate for desktop computing software
	LANL	In part
	SNL	No
	SRS	Uncertain
	Pantex	Mapped, see "Other" below
	Rocky Flats	In Whole
	Y-12	See "Other"
	INEEL	Implemented but not mapped
	YMP/TESS	Full compliance
	Hanford/RL	•Fluor Hanford--The FH procedures comply with DOE Order 200.1. The Guide is not in the PHMC. •Bechtel Hanford--DOE Order 200.1 is not included in the ERC Contract at this time. The ERC procedures are based on the Bechtel Corporate SDMF, which is consistent with DOE Order 200.1. •PNNL Hanford–The SSEP complies.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION

	Hanford/ORP	•Tank Farm–Yes •Tank Waste–Under the privatization concept and under the current "bridge" design effort the cited DOE Orders are not applicable; see section V, Additional Comments.
	WIPP	No
DOE G 414.1-1	LLNL	HCD/ABS–DOE G 414.1 does not have a section 4.6.3. DOE G 414.2 *Quality Assurance Management System Guide* does have a section 4.6.3 related to the Design Process. It calls for validation of the software used in the design process. As noted above, informal validation is attained by comparison with standard output results, widespread use for exposure and dose calculations, and review and approval of output during the approval of the safety basis documents.
	LANL	In part
	SNL	No
	SRS	Uncertain
	Pantex	See "Other" below
	Rocky Flats	In Whole
	Y-12	See "Other", based on DOE AL QC-1
	INEEL	Implemented but not mapped
	YMP/TESS	Full compliance
	Hanford/RL	•Fluor Hanford–The FH procedures comply with section 4.6.3 of DOE G 414.1-2. •Bechtel Hanford–DOE Order 414.1 is not included in the ERC Contract at this time. The ERC procedures are compliant with DOE Order 5700.6C as required by the Contract. •PNNL Hanford–Was considered when developing the Integrated Assessment System within PNNL. (Note: August 1996 version does not contain a section 4.6.3)
	Hanford/ORP	•Tank Farm–Yes •Tank Waste–Under the privatization concept and under the current "bridge" design effort the cited DOE Orders are not applicable; see section V, Additional Comments.
	WIPP	Yes, compliance in whole.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION		
ANSI/ANS-10.4-1987	LLNL	–
	LANL	In part
	SNL	No
	SRS	In part
	Pantex	See “Other” below
	Rocky Flats	Yes
	Y-12	See “Other”
	INEEL	Implemented but not mapped
	YMP/TESS	Full compliance
	Hanford/RL	•Fluor Hanford–No response. •Bechtel Hanford–No. •PNNL Hanford–No response.
	Hanford/ORP	•Tank Farm–No response. •Tank Waste–No response.
	WIPP	–
NQA-1-1997	LLNL	CSG—Criticality safety software meets ANSI/ANS 8.1, Nuclear Criticality Safety in Operations with Fissionable Materials Outside Reactors
	LANL	In part
	SNL	Yes
	SRS	In part
	Pantex	Mapped, see “Other” below
	Rocky Flats	Yes
	Y-12	See “Other”
	INEEL	Implemented but not mapped

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION

	YMP/TESS	Full compliance
	Hanford/RL	•Fluor Hanford–The FH procedures comply with NQA-1-97, Subpart 2.7, *Quality Assurance Requirements of Computer Software for Nuclear Facility Application* with NQA-1-99 Addendum •Bechtel Hanford–No •PNNL Hanford–This can be applied on a project specific basis, as needed, but it is not a foundation for the entire Laboratory. For example, analysis for criticality and shielding is done using MCNP and SCALE. Control and maintenance of these codes is performed by the following procedure, PNL-MA-875 "Computer Code Maintenance Quality Assurance Manual". This manual is NQA-1 Part 2.7 Compliant.
	Hanford/ORP	•Tank Farm–The CHG quality assurance program invokes NQA-1-89 as a consensus standard for implementing 10CFR830.120 and utilizes the FH procedures for implementing the NQA-1-89 requirements. The FH procedures comply with NQA-1-97, Subpart 2.7, Quality Assurance Requirements of Computer Software for Nuclear Facility Application with NQA-1-99 Addendum. •Tank Waste–ASME NQA-1-1994, Part II, Subpart 2.7.
	WIPP	Yes, compliance in whole, where required.
Other	LLNL	No
	LANL	QC-1, IEEE STD 730-1998, IEEE STD 730.1-1995, IEEE STD 828-1998, ASME NQA-2-1989, NQA-2a-1990, NUREG/CR-0178, NUREG/CR 6463, NUREG/CR 4640, IEEE Std. 610.12-1990
	SNL	–
	SRS	–
	Pantex	The in-house developed Software Quality Life Cycle Plant standard has been mapped to the following: ANSI/ISO/ASQC Q9001 –1994 Quality Systems, DOE/HQ Software Engineering Methodology 3/96, DOE Order 5700.6C Quality Assurance (10 CFR 830.120, Quality Assurance Requirements), ASME NQA-1 Addenda Part 2.7, DOE/AL Quality Criteria (QC-1), and the Software Engineering Institute's (SEI) Capability Maturity Model's eighteen Key Process Areas.
	Rocky Flats	–
	Y-12	The current software procedures were issued in early 1991 and revised in early 1995. The procedures have not been evaluated against the above requirements. The new Y80 Series procedures, expected to be issued end of CY2000, will address the above requirements and be in line with the current safety criteria such as those required by Integrated Safety Management (ISM) processes. The revised procedures will incorporate the latest QA, security, and software engineering requirements.
	INEEL	–

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION

	YMP/TESS	–
	Hanford/RL	•Fluor Hanford–The FH procedures also comply with Office of Civilian Radioactive Waste Management (OCRWM) QA Requirements and Description, Section 3 - Design Control, Section 11 - Test Control, and Supplement 1 - Software, and with Title 10, Code of Federal Regulations, Part 830.120 - *Quality Assurance Requirements.* •Bechtel Hanford–ISO 9000. The ERC has not developed in-house computer codes for safety analysis applications. All software in use for safety analysis was developed by third parties and is either in the public domain or commercially available. The ERC specifies, procures, and validates such software consistent with our SQA program. The minimum requirements are: •A determination by the applicable functional manager that the documentation supplied by the third party includes a description of the theoretical basis for the software package, instructions in the use of the package, and that the extent of software validation and verification is adequate for the ERC application. •Confirmation that the software as delivered reproduces the results of tests conducted as part of the software validation/verification. BHI's Automation Technology group is in the process of updating the SQA program, and existing procedures are being reviewed/ revised. The plan is to adopt the following DOE documents in their entirety: DOE Order 200.1 *Information Management Program*, and DOE Guide 200.1-1 *Department of Energy Software Engineering Methodology*. •PNNL Hanford–The primary standard for the SSEP is the Software Engineering Institute's Capability Maturity Model for Software (see http://www.sei.cmu.edu/cmm/)
	Hanford/ORP	•Tank Farm–The FH procedures comply with 10CFR830.120, Quality Assurance Requirements. Subsequent to creation of the DOE Office of River Protection (ORP) and changing the Tank Farm Contractor from a subcontractor under Fluor Hanford, Inc. (FH) to a prime contractor under ORP, the Tank Farm Contractor (now CH2M HILL Hanford Group, Inc. [CHG]) and FH agreed that common use of some existing FH procedures would facilitate consistency among interfacing Hanford contractors. CHG utilizes SQA programs that were written by FH for use with the Project Hanford Management System. •Tank Waste–DOE/RW/0333P, *Quality Assurance Requirements and Description (QARD)*, Supplements I and V.
	WIPP	N/A

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION

3.	How frequently is compliance with these procedures audited?	Are audits performed by external groups?	What is the date(s) of your last SQA audit?
LLNL	•HCD/ABS--No formal audit program •CSG--Criticality safety is audited by both LLNL ARO and DOE-Oakland Operations Office. The ARO audit is on a three-year cycle. •HWM--Multiple times per year through assessments, audits, and surveillance. Audits are directly and indirectly performed of HWM's QA Program by DOE, State of CA/DTSC, internal and external audits of the Waste Certification Program, internally by Hazards Control and Assurance Review Office. SQA has not been the main subject of an audit, but some components of SQA have been assessed as part of a audit.	•HSD/ABS –No •CSG–Yes, Criticality safety audit by LLNL Assurance Review Office which did include external experts. •HWM--Yes, by the Assurance Review Office (ARO) and State and Federal agencies.	•HCD/ABS --N/A •CSG–Last ARO audit on Criticality safety was in January of 2000.
LANL	Varies by customer	Varies by customer	Varies by code, by as an example TWCP was audited in August 2000.
SNL	Once per Year	No – Internal Independent	January, 2000
SRS	Compliance with WSRC software and practices, and evolving WSMS procedures are audited in part every 3 to 4 years.	The audits are usually performed by external groups (WSRC, others). Occasionally, self-assessments are conducted by WSMS. The latter are mostly spot-checks of some software users and only apply to a few software packages.	Compliance has been checked once (~ 1998) since the formation of WSMS (1 October 1997). It's unclear to the degree this activity was an audit.
Pantex	As determined by the Internal Auditing department relative to the risk assessment process (Criticality Safety – annually).	Several Y2K audits were conducted by external groups.	9/00 by DOE/AAO relative to QC-1 compliance. Criticality Safety – 2/00.
Rocky Flats	Audits are conducted on various aspects of SQA and Nuclear Safety matters throughout the year according to the site Master Audit Schedule.	Yes, both actual external groups (EPA, CAO, etc.), as well as internal, but independent, groups (K-H Internal audit, Independent Safety Oversight)	June 26, 2000.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION

Y-12	SQA is not singled-out as a specific entity. It is integrated into the overall software control process. Therefore, an assessment just on the SQA elements of the software control program would not be performed.	The Plant Quality Assurance Organization assesses software associated with a work process when the work process is being assessed.	November 1999 (QAS-2)
INEEL	Compliance with INEEL procedures is a typical subject for facility self-assessments.	Not specified	No comprehensive sitewide audit has been performed. Flowdown review conducted in FY 99.
YMP/TESS	Monthly	Yes	8/25/2000
Hanford/RL	•Fluor Hanford--There isn't a set frequency; however, audits have occurred approximately annually. •Bechtel Hanford--Comprehensive compliance audits, as referred to here, are not routinely scheduled. Audits for software licensing are performed annually. •PNNL Hanford--Assessment for Laboratory compliance to the subject area has not been conducted. However, there is a SSEP assessment program that focuses on projects performed by IS&E and for the ISE product line.	•Fluor Hanford--Yes, audit groups include: Fluor Corporate Auditors, DOE-RL Auditors, IG Auditors, DNFSB Auditors, OCRWM Auditors, and other oversight agencies. The frequency and schedule of audits are not known until an audit notification is sent. •Bechtel Hanford-No •PNNL Hanford--The SSEP assessments are performed by representatives from the Quality organization.	•Fluor Hanford--1997 - Fluor Corp (97-001-1), General and Applications Controls Audit; June, 1999 - DOR-AUD-PAD-99-021, Software Quality Assurance; July, 2000 - IA2000-06, Software Acquisition/Development •Bechtel Hanford--The last documented SQA audit was performed in February 1996. •PNNL Hanford--SSEP assessments are performed continually. There are currently several in progress. In FY00 Internal Auditing performed an audit on General Information Systems Controls which included looking at the subject area and SSEP, but did not cover them in depth or specifically focus on them.

I. SOFTWARE QUALITY ASSURANCE (SQA) INFORMATION

Hanford/ORP	•Tank Farm–Specific frequencies for audits of the SQA program are not set. However, as a program implementing quality assurance requirements, the implementation of these requirements are required to be audited on an annual basis.	•Tank Farm–CHG has performed no audits on SQA since October 1,1999. Prior to October 1, 1999, the SQA program was under FH and was audited by internal and external groups.	•Tank Farm–June 1999
	•Tank Waste–No frequency is established; however, audits have been performed approximately annually. In addition, management assessments and surveillance have been performed more frequently.	•Tank Waste–Yes. Audit groups included DOE/RL-Regulatory Unit, DOE-Office of River Protection	•Tank Waste–External audit: 11/4/99; internal audit: 2/16/00
WIPP	Periodically.	Sometimes external, sometimes internal.	External, Environmental Protection Agency, March 1999 --WWIS Programmatic Audit; Internal, WID QA, November 2000 – WWIS Programmatic audit to NQA-2A; Each Software Quality Assurance plan (per WP 16-IT3117) is reviewed and approved by WID QA.