Department of Energy
Washington, DC 20585
May 18, 2001

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

Dear Mr. Chairman:

Enclosed is a status report of the actions described in the Department of Energy's (DOE) report, dated October 2, 2000, addressing issues raised in the January 2000 Technical Report 25 – *Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities.*

In summary, Actions 1.0 to 5.0 are completed or nearing completion. As a result of the establishment of the Safety Analysis Software Group (SASG), Actions 6.0 to 11.0 have been revised. Consequently, a supplementary report, which will replace the October 2 report, will be forwarded by separate letter from the Secretary.

If you have any questions, please contact me at 202-586-0166.

Sincerely,

Howard Landon
Acting Chief Information Officer

Enclosures
1. Status Report
2. N 203.1, Software Quality Assurance
3. Summary Report on Standards
4. Summary Report on Training
5. DOE October 2 Memo Establishing SASG

STATUS UPDATE TO

THE OCTOBER 2, 2000 DOE RESPONSE TO

DNFSB TECHNICAL REPORT 25

May 1, 2001

Action 1.0: Develop an SQA directive

Purpose: To provide requirements that are conducive to actions necessary for implementing improvements in guidance, processes, standards identification, training, and code development and maintenance. To provide a framework for sites and organizations to make decisions for what needs to be included in an effective SQA program. To specify the level of SQA needed for all software and emphasize a risk-based approach to SQA.

Responsible Manager: Chief Information Officer (CIO)

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

Due Date: October 16,2000

Status: Completed. Notice signed by the Deputy Secretary on October 2, 2000 and placed into DOE Directives System. An announcement was provided verbally to DNFSB staff Deliverable is attached as Enclosure 2.

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

Purnose: To determine where the current set of DOE directives (including Integrated Safety Management (ISM) and DOE's Functions, Responsibilities, and Authorities Manuals (FRAM)) may not adequately express DOE expectations for SQA practices or may not be appropriately applied. To obtain data needed to identify areas where additional requirements are warranted. To identify a set of standards that includes DOE and Nuclear Regulatory Commission (NRC) directives and describe how the standards would be applied based on benchmark data.

Responsible Manager: EH and CIO

Deliverables: A list of Recommended Standards to the LPSOs

Due Date: October 30, 2000

Status: Completed. A survey was issued to determine what DOE, other government, or industry safety and SQA standards are used by the field for defense nuclear facilities. The survey compilation was completed on January 15,2001. Survey results revealed sites develop their own policies, requirements, and guidance to implement DOE directives and requirements. No other government or industry safety and SQA standards are used. A list of the current DOE directives and standards recommended for field usage was compiled. The survey results and deliverable are enclosed as attachments to the Summary Report on Standards, which is attached as Enclosure 3.

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

Purpose: Same as Action 2.0.

Responsible Manager: EH and CIO

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

Due Date: November 30, 2000

Status: Completed. In addition to the survey discussed in Action 2.0, an independent assessment was conducted to review other DOE contractor, other government, and industry standards organizations for safety/safety analysis and software/SQA standards. The results of the assessment and survey questions with responses were incorporated into the Summary Report on Standards, which is attached as Enclosure 3, on February 14, 2001. The report includes recommendations for improvements to the LPSOs. A memo has been prepared to transmit the Report to the LPSOs. Also, the Report was provided to the Safety Analysis Software Group (SASG) as a tool for their action in defining a toolbox of standards for defense nuclear facilities; i.e., safety analysis and I&C software.

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

Purpose: To identify organizations/groups which may not be designated by name as having QA responsibility, but who implement or support some component of QA. To identify safety groups and determine how to enhance relationships and improve information exchange between those groups and QA.

Responsible Manager: Chairman, QA WG

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

Due Date: November 30, 2000

Status: Incomplete. An integrated matrix QA organizational structure identifying interface/communication channels, reporting and working relationships, roles and responsibilities, sponsorship, and a central point-of-contact for resolving QA issues was developed. The matrix shows the QAWG as the central point-of-contact or central liaison, among other independent and interdependent organizations and groups. However; the reorganizations in NNSA/Defense Programs and DOE/Science are impacting the ability to produce a final charter. A summary report, which will include the matrix, will be developed once the revised charter is finalized.

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

Purpose: To obtain details on current practices and obtain data for identifying the need to establish a standardized and minimum level of training requirements for personnel using software associated with safety analysis (primarily accident and consequence analysis) and I&C systems.

Responsible Manager: EH and DP

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

Due Date: November 30,2000

Status: Completed. The survey was limited to an identification of safety and SQA training used by the field for defense nuclear facilities. Survey results revealed no defined safety analysis and SQA training requirements, including user training for specified software. In addition to the survey, an independent assessment was conducted to review other DOE contractor, other government, and industry training programs for safety/safety analysis and software/SQA standards. The results of the assessment and survey questions with responses were incorporated into the Summary Report on Training, which is attached as Enclosure 4, on March 30,2001. The report includes recommendations for improvements to the LPSOs. A memo has been prepared to transmit the Report to the LPSOs. Also, the Report was provided to the Safety Analysis Software Group (SASG) as a tool for their action in defining training requirements for defense nuclear facilities; i.e., safety analysis and I&C software.

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

Purpose: To establish a centralized group (comprised of DOE, contractors, and subject matter experts including expertise in safety analysis, software development and SQA, and authorization basis implementation), with coordinated support from the Energy Facilities Contractors Group (EFCOG), to take a leadership role for DOE and its contractors in the specific safety-related software areas of concern highlighted in Technical Report 25.

Responsible Managers: NNSA/DP, EM, EH

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

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

Status: Incomplete. A memorandum was signed by the Deputy Secretary on October 2, 2000 establishing the SASG and requesting that participants from NNSA/DP, EM, and EH be named by October 16,2000. The SASG is chaired by the NNSA/DP subject matter expert and held its first meeting February 14-15,2001. The SASG has revised Actions 6.0 through 11.0. Because of the revisions, the OCIO developed a supplementary report which supersedes the October 2, 2000 report. The supplementary report is being coordinated for the Secretary's signature. The activities for this action are addressed in the supplementary report as Actions 1.0,2.0,4.0, and 6.0.

Action 7 00: Identify software used for safety analysis and I&C processes. Compare practices and training for these codes and software. Analyze for deficiencies and improvements.

Purpose: To identify high-use software and relevant software standards and practices to determine specific remedial activities necessary to upgrade non-compliant safety-related software. To obtain data for assessing the degree of reliance on computer modeling for developing the safety bases for nuclear facilities.

Responsible Manager: Chair, Safety Analysis Software Group

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

Due Date: December 29, 2000

Status: Action not yet taken. The SASG has revised Actions 6.0 through 11.0. Because of the revisions, the OCIO developed a supplementary report which supersedes the October 2, 2000 report. The supplementary report is being coordinated for the Secretary's signature. The activities for this action are addressed in the supplementary report as Actions 4.0,5.0,6.0 and 7.0.

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

Purpose: To earmark candidate software for the software tool-box. To determine the adequacy of the tool-box software and individual site applications, and the impacts of the use of candidate software relative to the authorization basis for the facilities in question.

Responsible Managers: Chair, SASG

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

Due Date: March 1, 2001

Status: Action not yet taken. The SASG has revised Actions 6.0 through 11.0. Because of the revisions, the OCIO developed a supplementary report which supersedes the October 2, 2000 report. The supplementary report is being coordinated for the Secretary's signature. The activities for this action are addressed in the supplementary report as Action 5.0.

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

Purpose: To obtain best practices and other guidance for DOE safety analysts who are responsible for performing hazard, accident, and consequence analysis upon which the identification of control sets is based.

Responsible Managers: EH/NNSA-DP

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

Due Date: June 16,2001

Status: Action not due. The SASG has revised Actions 6.0 through 11.0. Because of the revisions, the OCIO developed a supplementary report which supersedes the October 2, 2000 report. The supplementary report is being coordinated for the Secretary's signature. The activities for this action are addressed in the supplementary report as Action 7.0.

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

Purpose: To establish a permanent expert advisory team in a DOE nuclear national laboratory.

Responsible Manager: Chair, SASG

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

Due Date: July 31,2001

Status: Action not due. The SASG has revised Actions 6.0 through 11.0. Because of the revisions, the OCIO developed a supplementary report which supersedes the October 2, 2000 report. The supplementary report is being coordinated for the Secretary's signature. The activities for this action are addressed in the supplementary report as Action 3.0.

Action 11.0: Perform backfit SQA program for MACCS2.

Purpose: To pilot the processes established by the SASG on MACCS2 code because it has widespread use for authorization basis calculations and has many documented deficiencies. To conduct a concentrated verification and validation effort to bootstrap MACCS2 into 'a level of compliance commensurate to safety-related software standards. To evolve the tool-box into a manageable number of one to two codes for each phenomenological area (e.g. fire, spill, deflagration/ detonation).

Responsible Managers: Chair, SASG

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

Due Date: December 31,2001

Status: Action not due. The SASG has revised Actions 6.0 through 11.0. Because of the revisions, the OCIO developed a supplementary report which supersedes the October 2, 2000 report. The supplementary report is being coordinated for the Secretary's signature. The activities for this action are addressed in the supplementary report as Action 8.0.

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

NOTICE

DOE N 203.1

Approved: 10-02-00
Expires: 06-02-01

SUBJECT: SOFTWARE QUALITY ASSURANCE

1. OBJECTIVES. To define requirements and responsibilities for software quality assurance (SQA) within the Department of Energy (DOE) to ensure that—

   a. all software owned or maintained by DOE, as referenced in paragraph 3c, Applicability, is subjected to formal quality assurance;

   b. all DOE software engineering follows identified standards and best practices throughout the project and product lifecycle;

   c. due to the spectrum of requirements, the degree of SQA is risk-based; and

   d. personnel are capable of correctly developing, using, and managing software.

2. CANCELLATION. None.

3. APPLICABILITY.

   a. DOE Elements. This directive applies to Departmental elements that acquire, develop, modify, or maintain computer software.

   b. Contractors. The Contractor Requirements Document, Attachment 1, sets forth the requirements to be applied to all management and operating and other contracts that require the acquisition, development, modification, or maintenance of computer software, as provided by contract and as implemented by the appropriate contracting officer. Compliance with the Contractor Requirements Document will be required to the extent set forth in the contract.

   c. DOE Software. The provisions of this Notice apply to all DOE software or software customized for DOE use, proposed for use, under development, or being maintained and used, whether that software was developed in-house, licensed from a commercial vendor for customized use, obtained from another organization, or otherwise acquired. The type of software includes, but is not limited to (a) administrative/business-oriented software, (b) scientific/engineering software except as identified in paragraph 3.d. below, (c) manufacturing-oriented software, and (d) process control; (e.g., Programmable Logic Control instructions).

d. Basic Research Activities. The requirements of this Notice are not mandatory for basic scientific research and development activities conducted to support the Office of Science mission unless those activities are governed by the requirements in 10 CFR part 830. However, line management is encouraged to consider all or part of the Notice requirements in meeting its responsibilities to ensure the quality of the software developed for basic research. Business systems that support basic research are not exempted from the Notice requirements.

e. Exclusion. Executive Order 12344 (set forth in Public Law 106-65 of October 5, 1999 [50 U.S.C. 2406]) establishes the responsibilities and authority of the Director, Naval Nuclear Propulsion Program, for all facilities and work that comprise the Program, which is a joint Navy/DOE organization. The Director's responsibilities include the operating practices and procedures applicable to Naval nuclear propulsion plants. The Director must establish the quality assurance requirements implemented within the Program. Accordingly, this Notice does not apply to the Naval Reactors Program.

4. REQUIREMENTS.

a. This directive is effective upon issuance.

b. SQA Program. Each Departmental element shall develop, document, and implement an SQA program. Each SQA program will consist of an identified focal point of contact, defined authorities, policies, procedures, training, adopted standards, and conventions tailored to local needs. Each program will treat SQA initiatives appropriately, commensurate with their size, complexity, cost, degree of external impact, degree of customization, functions performed, and other factors important to local management. The SQA program will describe how project SQA plans are to be developed and implemented.

c. Risk-Based, Graded Approach. All software, which is owned or maintained by DOE, must be subjected to a degree of formal SQA commensurate with the safety, security, and risk involved in developing and using the software. This approach allows all software, including that which may be categorized as "research and development", to be assessed for and receive an appropriate and commensurate amount of SQA.

d. Lifecycle-Based SQA Processes and Procedures. The SQA processes and procedures used must be software product and project lifecycle based; documented to provide a baseline for auditing; and applied in a consistent, repeatable, and predictable manner. The adequacy of selected processes and practices, as well as their oversight, is the responsibility of each individual Departmental element.

e. Project SQA Plans. Project SQA plans will be developed and address testing (e.g., unit, integration, system, acceptance), verification and validation, structured walkthroughs, peer

reviews, inspections, audits and any other requirements specified for an application (e.g., by contract). Each plan should be commensurate with the level of the size, complexity, and scope of the software project.

f. Oversight. Each Departmental element will conduct systematic reviews to ensure that the requirements of this directive and DOE O 414.1A, QUALITY ASSURANCE, are met and determine the need to update its own SQA program. Relative to software, these reviews should also ensure that appropriate safety and security controls are in place, are effective, and reflect currently accepted industry practices. For line management assessment of an SQA program, the principles and guidelines in DOE P 450.5, LINE ENVIRONMENT, SAFETY AND HEALTH OVERSIGHT, will apply and should be followed.

g. Training. Sites are responsible for ensuring the adequacy of training programs to meet current and future personnel skill needs in the areas of SQA, software engineering, and software user training.

h. Integration. Sites must integrate the SQA program planning process with the strategic planning, Safety Management System, and budget process, as appropriate, to ensure that SQA program decisions are made, adequately funded, and executed to support DOE organizational and site missions and priorities.

5. RESPONSIBILITIES.

a. Office of the Chief Information Officer.

(1) Establishes and maintains Departmentwide direction and guidance for SQA management processes.

(2) Periodically reviews the results of internal and external compliance assessments and determines if the Departmentwide direction and guidance need to be improved or assistance provided.

b. Power Marketing Administrations. Execute program office responsibility, accountability, and oversight for SQA management process compliance within their respective program areas.

c. Departmental Elements. Implement the appropriate level of management effort, and assume responsibility, accountability, and oversight for continued SQA management process compliance within their respective program areas. Specifically—

(1) Establish and document SQA programs.

(2) Identify a focal point of contact.

(3) Ensure that the SQA programs conduct risk assessments and determine the level of SQA to be applied.

(4) Ensure that the level of SQA is tailored to the site needs.

(5) Oversee development and implementation of SQA processes and procedures.

(6) Ensure the production and delivery of quality software products.

(7) Ensure that SQA programs are reviewed.

(8) Ensure SQA plans are approved.

(9) Relative to software, ensure that appropriate safety and security controls are in place, are effective, and reflect currently accepted industry practices.

(10) Ensure the adequacy of training programs for SQA, software engineering and software user training.

(11) Ensure that any SQA program related to safety is developed and implemented in a manner that is consistent with DOE P 450.4, SAFETY MANAGEMENT SYSTEM POLICY, and associated standards and manuals.

(12) Ensure that any nuclear software program related to safety is developed and integrated with existing nuclear safety policies and standards.

(13) Ensure that all SQA programs are developed and implemented in a manner that is consistent with applicable classified and/or unclassified policy.

d. Assistant Secretary for Environment, Safety, and Health (EH-1), acting as DOE's independent element responsible for safety aspects relative to public and worker health, and safety and environmental protection, shall provide advice and assistance to the Chief Information Officer concerning policy requirements and guidance necessary to implement this directive on software used for safety applications.

e. Deputy Assistant Secretary for Oversight, acting as the Department's independent element responsible for the oversight of environment, safety, and health has the following responsibilities.

(1) Assess and report to the Secretary of Energy on all aspects of safety related to implementation of this directive, including performance of the Secretarial Offices, field elements and contractors.

(2) Review and comment on proposed SQA policy, regulations, standards and requirements to assess their potential effects on the safety of operations at DOE facilities.

f. Director, Office of Independent Oversight and Performance Assurance, acting as the Department's independent element responsible for the oversight of safeguards and security has the following responsibilities.

(1) Assess and report to the Secretary of Energy on all aspects of safeguards and security related to implementation of this directive, including performance of the Secretarial Offices, field elements and contractors.

(2) Review and comment on proposed SQA policy, regulations, standards and requirements to assess their potential effects on the security of operations at DOE facilities.

6. IMPLEMENTATION. Implementation of this directive is site-specific. An implementation plan that describes the actions necessary to comply with this directive and the expected date for completing those actions must be submitted to the applicable Program Secretarial Office (PSO) or Power Marketing Administration management 90 days after the approval date of this directive. Where there are multiple programs, coordination should be implemented by the Lead Program Secretarial Officers. SQA program plans should be approved by PSOs within 120 days of receipt.

7. ASSESSMENTS OF SQA IMPLEMENTATIONS. Assessments of SQA implementations of this directive will be forwarded to the Office of the Chief Information Officer.

8. REFERENCES.

a. 10 CFR part 830, Nuclear Safety Management.

b. DOE O 414.1A, QUALITY ASSURANCE, dated 9-29-99.

c. DOE O 5480.23, NUCLEAR SAFETY ANALYSIS REPORTS, dated 4-10-92.

d. DOE P 450.4, SAFETY MANAGEMENT SYSTEM POLICY, dated 10-15-96.

e. DOE P 450.5, LINE ENVIRONMENT, SAFETY AND HEALTH OVERSIGHT, dated 6-26-97.

f. DOE S 1027-92, HAZARD CATEGORIZATION AND ACCIDENT ANALYSIS TECHNIQUES FOR COMPLIANCE WITH DOE ORDER 5480.23, NUCLEAR SAFETY ANALYSIS REPORTS, updated 9-97.

g. DOE G 200.1-1, DEPARTMENT OF ENERGY SOFTWARE ENGINEERING METHODOLOGY, dated 5-21-97.

h. DOE G 414.1-2, QUALITY ASSURANCE MANAGEMENT SYSTEM GUIDE FOR USE WITH 10 CFR 830.120 AND DOE O 414.1, dated 7-17-99.

i. Quality Criteria (QC-1), invoked via reference in DOE/AL Supplemental Directive 56XB (Nuclear Weapon Development and Production Manual).

9. CONTACT. For additional information or assistance in interpreting or implementing this directive, please contact the Office of the Chief Information Officer at 202-586-0166.

10. DEFINITIONS. To promote a common understanding of SQA and systems engineering concepts, the following definitions are provided.

a. Acceptance Testing. Formal testing conducted to determine whether or not a software product or system satisfies its acceptance criteria and to enable the system owner to determine whether or not to accept the product or system. *IEEE Standard Glossary of Software Engineering Terminology, Std. 610.12-1990.*

b. Configuration Management (CM). A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements. *IEEE Standard Glossary of Software Engineering Terminology, Std. 610.12-1990.*

c. Departmental Element. A Departmental Element is defined as a first-tier organization at Headquarters and in the Field. First-tier at Headquarters is the Secretary, Deputy Secretary, Under Secretary, and Secretarial Officers (Assistant Secretaries and Staff Office Directors). First-tier in the Field is Managers of the eight Operations Offices, Managers of the three Field Offices, and the Administrators of the Power Marketing Administrations. Headquarters and Field Elements are described as follows: (1) Headquarters Elements are DOE organizations located in the Washington Metropolitan Area; and (2) "Field Elements" is a general term for all DOE sites (excluding individual duty stations) located outside of the Washington, DC, Metropolitan Area. *DOE Glossary in the Directives System.*

d. Information System. A combination of information, computer, and telecommunications resources and other information technology and personnel resources that collects, records, processes, stores, communicates, retrieves, and displays information. *DOD Directive #7920.1, Life Cycle Management of Automated Information Systems, 1988.*

e. Integration Testing. Testing in which software components, hardware components, or both are combined and tested to evaluate the interaction between them. *IEEE Standard Glossary of Software Engineering Terminology, Std. 610.12-1990.*

f. Project Planning. The planning of project technical and management activities that are documented in a project plan. The plan typically describes the work to be done, the resources required, the methods to be used, the procedures to be followed, the schedules to be met, and the way the project will be organized. It includes a list of deliverables, actions required, and other key events needed to accomplish the project. *DOE Software Quality and Systems Engineering support team, 1999.*

g. Project Tracking and Oversight. The tracking and reviewing of accomplishments and results against documented estimates, commitments, and plans. Includes the adjusting of plans based on actual accomplishments and results. *DOE Software Quality and Systems Engineering support team, 1999.*

h. Quality Assurance. (1) A planned and systematic pattern of all actions necessary to provide adequate confidence that the item or product conforms to established operational, functional, and technical requirements. (2) A set of activities designed to evaluate the process by which products are developed or manufactured. *IEEE Standard Glossary of Software Engineering Terminology, Std. 610.12-1990.*

i. Quality Control.

(1) The process by which product correctness is determined and action is initiated when nonconformance is detected.

(2) A line function; the work done within a process to ensure that the work product conforms to standards/requirements. *Effective Methods for Software Testing by William Perry, John Wiley & Sons, 1995.*

j. Requirements Management. In system/software system engineering, the process of controlling the identification, allocation, and flowdown of requirements from the system level to the module or part level, including interfaces, verification, modifications, and status monitoring. *Software Requirements Engineering, edited by Thayer & Dorfman, IEEE Computer Society Press, 1997.*

k. Risk Management. An approach to problem analysis that is used to identify, analyze, prioritize, and control risks. *DOE Software Engineering Methodology, March 1999.*

l. Software Design. In software engineering, the process of defining the software architecture (structure), components, modules, interfaces, test approach, and data for a software system to satisfy specified requirements. *Software Requirements Engineering, edited by Thayer & Dorfman, IEEE Computer Society Press, 1997.*

m. Software Engineering. (1) The application of a systematic, disciplined, quantifiable approach to the development, operation, and maintenance of software; that is, the application of engineering to software. (2) The study of approaches as in (1). *IEEE Standard Glossary of Software Engineering Terminology, Std. 610.12-1990.*

n. Software Quality Assurance. See Quality Assurance. *IEEE Standard Glossary of Software Engineering Terminology, Std. 610.12-1990.*

o. System Testing. Testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. *IEEE Standard Glossary of Software Engineering Terminology, Std. 610.12-1990.*

p. Unit Testing. Testing of individual hardware or software units or groups of related units. The isolated testing of each flowpath of code with each unit. The expected output from the execution of the flowpath should be identified to allow comparisons of the planned output against the actual output. *DOE Software Engineering Methodology, March 1999.*

q. Validation. The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements. *IEEE Standard Glossary of Software Engineering Terminology, Std. 610.12-1990.*

r. Verification. (1) The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. (2) Formal proof of program correctness. *IEEE Standard Glossary of Software Engineering Terminology, Std. 610.12-1990.*

BY ORDER OF THE SECRETARY OF ENERGY:

T.J. GLAUTHIER
Deputy Secretary

CONTRACTOR REQUIREMENTS DOCUMENT
DOE N 203.1, SOFTWARE QUALITY ASSURANCE

The requirements in this Contractor Requirements Document must be applied to all management and operating and other contracts that require the acquisition, development, modification, or maintenance of computer software, as provided by contract and as implemented by the appropriate contracting officer. Compliance with this Contractor Requirements Document will be required to the extent set forth in the contract.

1. The provisions of this Contractor Requirements Document apply to DOE software or software customized for DOE use, proposed for use, under development, or being maintained and used, whether that software was developed in-house, licensed from a commercial vendor for customized use, obtained from another organization, or otherwise acquired shall be subjected to formal quality assurance. The type of software includes, but is not limited to—

   (a) administrative/business-oriented software,

   (b) scientific/engineering software within the context of considerations identified in number 2,

   (c) manufacturing-oriented software, and

   (d) process control (e.g., Programmable Logic Control instructions).

2. The provisions of this Contractor Requirements Document are not mandatory for basic scientific research and development activities conducted to support the Office of Science mission unless those activities are governed by the requirements in 10 CFR part 830. However, as directed, contractor line management is encouraged to consider all or part of the Notice requirements in meeting its responsibilities to ensure the quality of the software developed for basic research. Business systems that support basic research are not exempted from the Contractor Requirements Document provisions.

3. The contractor must develop, document, and implement an SQA program for projects under its contract. Each SQA program will consist of an identified focal point of contact, defined authorities, policies, procedures, training, adopted standards, and conventions tailored to local needs. Each program will treat SQA initiatives appropriately, commensurate with their size, complexity, cost, degree of external impact, degree of customization, functions performed, and other factors important to the site's management.

4. The contractor must ensure all software, which is owned or maintained by DOE, is subjected to a degree of formal SQA commensurate with the safety, security, and risk involved in developing and using the software. This approach allows all software, including that which may be categorized as "research and development", to be assessed for and receive an appropriate and commensurate amount of SQA.

5. The contractor must ensure the SQA processes and procedures are software product and project lifecycle based; documented to provide a baseline for auditing; and applied in a consistent, repeatable, and predictable manner. The contractor must ensure the adequacy of selected processes and practices, as well as their oversight.

6. The contractor must develop project SQA plans and address testing (e.g., unit, integration, system, acceptance), verification and validation, structured walkthroughs, peer reviews, inspections, audits and any other requirements specified for an application (e.g., by contract). The contractor must ensure that each plan is commensurate with the level of the size, complexity and scope of the software project. As appropriate, a standard SQA plan may be adopted and/or adapted for subsequent projects within a program.

7. The contractor must conduct systematic reviews to ensure that the requirements of this directive and DOE O 414.1A, QUALITY ASSURANCE, are met and determine the need to update its own SQA program. Relative to software, these reviews should also ensure that appropriate safety and security controls are in place, are effective, and reflect currently accepted industry practices.

8. The contractor must ensure the adequacy of training programs to meet current and future personnel skill needs in the areas of SQA, software engineering, and software user training.

9. The contractor must ensure the integration of the SQA program planning process with DOE strategic planning, Safety Management System, and budget process, as appropriate, to ensure that SQA program decisions are made, adequately funded, and executed to support DOE organizational and site missions and priorities.