The Deputy Secretary of Energy
Washington, DC 20585

July 29, 2008

The Honorable A. J. Eggenberger
Chairman
Defense Nuclear Facilities Safety Board
625 Indiana Avenue, NW, Suite 700
Washington, DC 20004-2901

Dear Mr. Chairman:

Your letter to former Deputy Secretary Sell dated February 5, 2008, stated that the Defense Nuclear Facilities Safety Board (Board) felt that it was appropriate to require independent validation of the implementation of safety basis controls and that the Department of Energy (DOE) should consider performing independent validations on a recurring basis to ensure the facility, equipment, procedures, and personnel training have not degraded over time. The Board concluded that the defense nuclear complex would benefit from requirements and guidance from DOE Headquarters for independent validations of safety basis controls and requested a report on DOE's evaluation of the need for such requirements and guidance, and any action taken or to be taken by DOE in this area.

The Office of Health, Safety and Security (HSS) coordinated with the Central Technical Authorities for Energy, Science and the National Nuclear Security Administration to evaluate current requirements for validation of safety basis controls and their implementation. The results of the evaluation are provided in the enclosed report. We have concluded that existing requirements for the implementation of safety controls contained in 10 CFR 830, *Nuclear Safety Management*, and DOE Orders appropriately focus on holding contractors responsible for proper implementation and validation of controls as part of their work practices that are governed by their quality assurance programs. DOE Order 226.1A, *Implementation of Department of Energy Oversight Policy,* requires DOE to oversee contractors' implementation of nuclear safety requirements, but does not explicitly require validation of safety basis controls.

Even though DOE does not explicitly require validation of safety basis controls in its Directives, DOE site offices do evaluate the implementation of safety basis controls as part of their oversight of contractors' programs. However, given the importance of safety basis controls, we consider it appropriate to provide guidance in this area. We plan to complete such guidance next year. In addition, guidance on validation of safety controls will be added to DOE standards for performing facility startup reviews and for DOE's safety system oversight program, both of which are currently under development.

If you have any questions on this matter, please contact Dr. James O'Brien at (301) 903-1408.

Sincerely,

Jeffrey F. Kupfer

Enclosure

Enclosure

REPORT ON REGULATORY REQUIREMENTS AND PRACTICES FOR INDEPENDENT VALIDATION OF SAFETY BASIS CONTROLS

1. INTRODUCTION

This report evaluates the regulatory requirements, guidance, and current practices for the independent validation of safety basis controls to determine whether new Department of Energy (DOE) requirements or guidance are warranted.

2. BACKGROUND

In a letter to the Deputy Secretary dated February 5, 2008, the Defense Nuclear Facilities Safety Board (Board or DNFSB) stated that it felt that it was appropriate to require independent validation of the implementation of safety basis controls and that DOE should consider performing independent validations on a recurring basis to ensure the facility, equipment, procedures, and personnel training have not degraded over time. The Board concluded that the defense nuclear complex would benefit from requirements and guidance from DOE Headquarters for independent validations of safety basis controls and requested this report on DOE's evaluation of the need for such requirements and guidance and any action taken or to be taken by DOE in this area.

The Office of Health, Safety and Security (HSS) coordinated with the Central Technical Authorities for Energy, Office of Science, and the National Nuclear Security Administration (NNSA) to evaluate current requirements for validation of safety basis controls and their implementation.

3. ANALYSIS

The proper implementation of safety basis controls is very important to the assurance of the protection of workers and the public. Current requirements promote use of a graded approach that places emphasis on those controls that are most important for protection of the public and workers. These controls are identified as Technical Safety Requirements (TSRs) and include design features, safety system operability requirements, and specific administrative controls. The focus of this analysis is on these TSR controls. Attachment 1 provides a synopsis of the DOE Orders that were reviewed as part of this analysis.

Requirements for Implementation of Controls

DOE requirements for implementation of safety controls are contained in 10 CFR Part 830, *Nuclear Safety Management*, and associated DOE Orders (see attachment) and focus on holding contractors responsible for proper implementation of controls as part of their quality assurance program. Title 10 CFR Part 830 requires that the contractor quality assurance program must ensure that the contractor will (1) perform work consistent with the hazard controls adopted to meet regulatory or contract requirements, using approved instructions, procedures, or other appropriate means, (2) verify or validate the adequacy

of design products using individuals or groups other than those who performed the work, and (3) verify or validate work before approval and implementation of the design.

DOE Order 226.1A, *Implementation of Department of Energy Oversight Policy,* provides requirements for DOE oversight of contractors' safety performance. These oversight requirements encompass the review of safety basis control implementation, and DOE is planning to develop a guide that will provide details of acceptable methods for implementing DOE Order 226.1A's requirements.

In addition to DOE Order 226.1A, for the startup of new facilities and restart of facilities, DOE Order 425.1C, *Startup and Restart of Nuclear Facilities*, provides requirements for review of implementation of TSR controls by both the contractor and DOE. The breadth and depth of the review is identified in the Plan of Action, which is approved by the Startup Authorization Authority. DOE Order 425.1C, *Startup and Restart of Nuclear Facilities*, provides for various types of independent reviews from contractor-only Readiness Assessment to sequential contractor and DOE Operational Readiness. In addition, Facility Representative (FR) and Safety System Oversight (SSO) personnel provide oversight of contractor readiness reviews to verify that they address all Plan of Action requirements, including implementation of safety system controls and also participate in DOE's operational readiness reviews. These independent reviews are checks on the implementation of the controls to validate that the contractor quality assurance processes that ensure proper control implementation is appropriate and has been appropriately implemented.

Requirements for Periodic Validation of Controls

Contractors and DOE conduct periodic validation of controls per several DOE Orders; specifically, DOE Order 414.1C, *Quality Assurance*; DOE Order 226.1A, DOE Order 420.1B, *Facility Safety*, and DOE Manual 426.1, *Federal Technical Capability Manual.* Furthermore, the TSRs themselves contain facility-specific requirements for the validation of safety controls that the contractor must implement.

Independence

The concept of independent assessments is discussed in DOE G 414.1-2A, *Quality Assurance Management System Guide,* where it states that "individuals performing independent assessments should not currently perform, supervise, or be directly responsible for performing the activities being assessed. Independence is determined based on an individual not having bias, rather than on organizational affiliation. The independent assessor should have both the personal and organizational freedom to communicate with the management of the assessed organizations.

Review of Current Practices and Planned Enhancements

A review of current practices for conducting independent validation of safety basis controls was performed, including review of a sample of site procedures and discussions with Headquarters and field personnel involved in these validations.

Independent validations of safety basis controls occur at several levels to various degrees; e.g., by contractors (independent assessments per 10 CFR 830 and DOE Order 414.1C); by DOE Site Offices (by SSO, FR, and safety basis personnel during operational readiness reviews, safety basis approvals, and independent assessments); and by DOE Headquarters Programs Offices, DOE's Office of Chief of Nuclear Safety and NNSA's Office of Chief of Defense Nuclear Safety, and HSS's Office of Independent Oversight.

The primary means for DOE's validation of the initial implementation of safety basis controls are during startup readiness reviews, but that these reviews are not required to nor are they performing 100 percent validations. Rather, these checks are used as information for determining whether the contractor processes for ensuring hazard controls are properly implemented are appropriate and have been appropriately implemented.

DOE's FRs and SSO personnel are DOE's primary overseers of proper implementation of safety basis controls. This has proven to work well within DOE to ensure safety controls are maintained and provides for frequent in the field evaluation of operations and implementation of controls. The SSO program was established to ensure that safety systems will perform their safety function, and SSOs perform independent validations as well as oversight of the contractors system engineer program (the contractor system engineer has the primary responsibility for in-depth system knowledge). However, expectations for the scope, breadth and depth and periodicity of these reviews have not been defined in Headquarters guidance and site procedures.

NNSA is developing a new manual for safety oversight of its programs. The current draft includes requirements for assessments to validate the continuing effective implementation of TSRs for Hazard Category 2 and 3 nuclear facilities and for assessments of equipment configuration, material condition, maintenance and surveillance of safety class and safety-significant systems. The draft manual also discusses the expected periodicity for the assessment of safety class and safety significant controls.

HSS is working with the SSO community and DOE's Federal Technology Capability to develop a SSO standard that will assign the SSO duties and functions and provide guidance on best practices. HSS is also leading an effort to revise the readiness review standard and plans to review the current guidance provided on independent validation of safety controls as part of this effort. Furthermore, as part of its Directives Review process HSS is planning on evaluating and revising DOE Order 226.1A and developing a guide for its implementation. As the cornerstone of the DOE oversight program, this Order and its implementing guide are key to ensuring that independent validation of the implementation of safety basis controls are appropriately performed, in particular for safety basis control modification that do not fall under DOE Order 425.1C and for ensuring periodic review of safety basis controls.

4. CONCLUSION

DOE requirements for overseeing the implementation of safety controls contained in 10 CFR 830 and DOE Orders appropriately place primary responsibility for proper implementation and validation of hazards controls on contractors as part of work practices, which are governed by their quality assurance program. DOE Order 226.1A requires DOE to oversee contractors' implementation of nuclear safety requirements, but does not explicitly require validation of safety basis controls.

Even though DOE does not explicitly require validation of safety basis controls in its Directives, DOE site offices do evaluate the implementation of safety basis controls as part of their oversight of contractors' programs. Given the importance of safety basis controls, it is appropriate to provide guidance in this area utilizing experience gained in performing independent validations by our site offices. In addition, appropriate documents to include this guidance are DOE standards for performing facility startup reviews and for DOE's safety system oversight program, both of which are currently under development.

Attachments

Attachment 1
Review of Requirements Related to Identification of Safety Basis Controls and Control Implementation and Validation

1.0 Requirements and Guidance for Identification of Safety Basis Controls

The safety basis for a nuclear facility includes the hazard controls upon which the contractor will rely to ensure adequate protection of workers, the public, and the environment during operations. As discussed in Appendix A to Subpart B of 10 CFR 830, hazard controls include:

- physical, design, structural, and engineering features;
- safety structures, systems, and components;
- safety management programs;
- technical safety requirements; and
- other controls necessary to provide adequate protection from hazards.

DOE Standard 3009, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, provides criteria for a contractor developing a documented safety analysis (DSA), which is where most if not all of the safety basis controls are specified (some additional controls may be imposed by DOE; e.g., in a safety evaluation report). Contractors perform a hazard analysis and an accident analysis as part of the development of a DSA to identify safety controls. Accident consequence and likelihood estimates developed during this process form the bases for grading the control. The result is documentation of the safety basis that emphasizes the controls needed to maintain safe operation of a facility in accordance with nuclear safety precepts (e.g., engineering controls closest to the source of the hazard are preferred over administrative controls). Contractors identify the most important controls and include them in technical safety requirements (TSRs).

2.0 Requirements and Guidance for Implementation and Periodic Validation of Safety Basis Controls

This section describes the Directives which provide requirements and guidance for implementation and periodic validation of Safety Basis Controls. HSS will be focusing its efforts on the programs established by DOE Order 226.1A, *Implementation of Department of Energy Oversight Policy* and DOE Manual 426.1, *Federal Technical Capability Manual*, with respect to the Safety System Oversight and Facility Representative programs to enhance DOE's independent validation of the implementation of safety basis controls become its efforts to ensure the facility, equipment, procedures and training.

DOE Order 226.1, *Implementation of Department of Energy Oversight Policy*
DOE Order 226.1 contains DOE oversight requirements. Several requirements are related to validation of proper implementation of safety basis controls.

- Central Technical Authorities must maintain awareness of the implementation of nuclear safety requirements and guidance, consistent with principles of Integrated Safety Management across the organization (including, for example, reviewing documented safety analyses, authorization agreements, and readiness reviews as necessary to evaluate the adequacy of safety controls and implementation).

- Contractors will be responsible for developing, implementing, and performing comprehensive assessments of all facilities, systems, and organizational elements, including subcontractors, on a recurring basis. Internal independent assessments will be performed by contractor organizations or personnel that have authority and independence from line management to support unbiased evaluations.

- Internal independent assessments will be performed by contractor organizations or personnel that have authority and independence from line management to support unbiased evaluations.

- DOE line management must establish and implement assessment programs to determine contractor compliance with requirements.

DOE Manual 426.1, *Federal Technical Capability Manual*
DOE Manual 426.1 defines the roles and responsibilities of personnel involved in oversight of safety basis controls (including Safety System Oversight [SSO] personnel, Facility Representatives [FRs] and Senior Technical Safety Managers [STSMs]) and provides requirements for the SSO Program.

SSO personnel are responsible for:

- Performing assessments, periodic evaluation of equipment configuration and material condition. The effect of aging on system equipment and components, the adequacy of application of work control and change control processes, and appropriateness of system maintenance and surveillance should be considered with respect to reliable performance of safety functions.

- Assessing contractor compliance with relevant DOE regulations, industry standards, contract requirements, safety basis requirements, and other system requirements.

- Coordinating with FRs to ensure, and report to STSMs, the operability of specific safety systems. SSO personnel focus on the details of safety system

operability implementation while FRs focus on the integrated operational aspects of these systems and programs.

- Overseeing assigned systems to ensure they will perform as required by the safety basis and other applicable requirements.

- Conducting (preferably leading) performance-based assessments (through walk-downs, interviews, document reviews, and field observations) to confirm that (a) authorization basis (AB) documents are accurate and adequately maintained; (b) system operation, maintenance, and performance is in accordance with this basis; (c) the effect of aging on system equipment and components is addressed; and (d) the contractor has an adequate Cognizant System Engineer Program (e.g., staffing, qualifications, responsibilities, programs) for monitoring, maintaining, and improving system performance.

Facility Representatives (FRs) are responsible for

- Oversight of their assigned facilities to ensure that the contractor operates facilities safely and efficiently (i.e., within the boundaries of those controls invoked in the facility AB), communicating system and facility status and operational performance information with STSMs.

Senior Technical Safety Managers (STSMs) are responsible for

- The status of safety systems and safety management programs. As such, they provide direction to SSO personnel and FRs to ensure that safety systems and safety management programs required by the facility safety basis are functional and fully implemented.

10 CFR 830, Subpart A, *Quality Assurance Requirements*
Contractors are required to establish and implement a quality assurance plan that addresses management, performance, and assessment criteria, including:

Criterion 3—Management/Quality

- Improvement to detect and prevent quality problems.
- Identify, control, and correct items, services, and processes that do not meet established requirements.

Criterion 4—Management/Documents and Records

- Prepare, review, approve, issue, use, and revise documents to prescribe processes, specify requirements, or establish design.
- Specify, prepare, review, approve, and maintain records.

Criterion 5—Performance/Work

- Perform work consistent with technical standards, administrative controls, and other hazard controls adopted to meet regulatory or contract requirements, using approved instructions, procedures, or other appropriate means.

Criterion 6—Performance/Design

- Verify or validate the adequacy of design products using individuals or groups other than those who performed the work.
- Verify or validate work before approval and implementation of the design.

Criterion 10—Assessment/Independent Assessment

- Plan and conduct independent assessments to measure item and service quality, to measure the adequacy of work performance, and to promote improvement.

These quality criteria place primary responsibility for proper development, implementation, and validation of hazard controls on the contractor.

10 CFR 830, Subpart B, *Safety Basis Requirements*

10 CFR 830 requires contractors for Hazard Category 1, 2, or 3 nuclear facilities to "perform work in accordance with the facility safety basis." Therefore, hazards controls must be in place before work commences and must remain in place. As discussed above, the most significant controls are captured in TSRs. TSRs for active safety systems and some passive safety systems will include surveillance and testing requirements to ensure the control is maintained operable.

DOE Order 425.1C, *Startup and Restart of Nuclear Facilities*

DOE Order 425.1C includes requirements for both DOE and Contractors to verify readiness to startup operations. Two of the "Core Requirements" (Number 4 and 5) in DOE Order 425.1C relate to validation of the safety basis controls.

- Facility safety documentation is in place **and has been implemented** that describes the "safety envelope" of the facility. The safety documentation should characterize the hazards/risks associated with the facility and should identify preventive and mitigating measures (systems, procedures, administrative controls, etc.) that protect workers and the public from those hazards/risks. Safety structures, systems, and components (SSCs) are defined and a system to maintain control over their design is established. *(Core Requirement #4)*

- A program is in place **to confirm and periodically reconfirm** the condition and operability of safety SSCs. This includes examinations of records of tests and calibration of these systems. The material condition of all safety, process, and utility systems will support the safe conduct of work. *(Core Requirement #5)*

These startup validation requirements will include checks on the TSR and other hazard controls, but are not designed to be 100 percent validations. These checks provide assurance that the contractor processes to ensure hazard controls are properly implemented, are appropriate, and have been appropriately implemented.

DOE Order 420.1B, *Facility Safety*
DOE Order 420.1B includes requirements for contractors to establish a system engineer program to ensure continued operational readiness of the systems within its scope. The systems within the scope are active safety class and safety-significant SSCs as defined in the facility's DOE-approved safety basis, as well as to other active systems that perform important defense-in-depth functions, as designated by facility line management.

As part of this, the contractor must periodically review system operability, reliability, and material condition. Reviews must assess the system for

- ability to perform design and safety functions,
- physical configuration as compared to system documentation, and
- system and component performance in comparison to established performance criteria.

Furthermore, the Order requires that system maintenance and repair be controlled through a formal change control process to ensure that changes are not inadvertently introduced, that required system performance is not compromised, and that systems be tested after modification to ensure continued capability to fulfill system requirements.

DOE Order 414.1C, *Quality Assurance*
This order is consistent with the quality assurance requirements in 10 CFR 830 and applies to both DOE and contractors. It requires the development of a quality assurance program that addresses ten criteria including:

- Criterion 5: Perform work consistent with technical standards, administrative controls, and hazard controls adopted to meet regulatory or contract requirements using approved instructions, procedures, etc.
- Criterion 10: Plan and conduct independent assessments to measure item and service quality and the adequacy of work performance and to promote improvement.

Therefore, the proper implementation of safety basis controls (and their periodic assessment) are also required under DOE Order 414.1C.