DEFENSE NUCLEAR FACILITIES SAFETY BOARD

625 Indiana Avenue, NW, Suite 700 Washington, D.C. 20004-2901
(202) 694-7000

March 4, 2009

Gerald L. Talbot Jr.
Assistant Deputy Administrator for
Nuclear Safety and Operations
National Nuclear Security Administration
1000 Independence Avenue, SW
Washington, DC 20585-0701

Dear Mr. Talbot:

Pursuant to the certification mandate provided in Section 3112 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009, the Defense Nuclear Facilities Safety Board's (Board) staff responsible for certification activities has reviewed Chemistry and Metallurgy Research Replacement (CMRR) design data provided to date by the National Nuclear Security Administration (NNSA). The Board's staff is focusing its review on topics previously raised regarding the CMRR nuclear safety design strategy, the Preliminary Documented Safety Analysis, and design of safety-class and safety-significant systems. Those topics were provided electronically to NNSA on November 20, 2008. The Board's staff has documented specific technical issues on a Findings Form. For purposes of the certification review, the Board's staff considers a Finding a design topic related to a concern raised by the Board's staff regarding the CMRR design that has not been adequately resolved and that could preclude Board certification.

Enclosed is a Findings Form with respect to the issue of Documenting and Maintaining Preliminary Documented Safety Analysis Safety-Related Functions and Requirements. We ask that you reply within seven calendar days from the date of Board's staff signature on the attached Findings Form, informing the Board's staff how long it will take to provide a complete NNSA response. The NNSA response should contain sufficient quantity and quality of technical information necessary for the Board's staff to determine whether the Finding can be resolved. The Findings Form contains a signature block for the NNSA individual with the authority and responsibility for addressing the Finding. Please ensure that this individual signs and dates the returned Findings Form.

Sincerely,

Roy E. Kasdorf
Nuclear Facility Design and
Infrastructure Group Lead

Enclosure:

c: Mr. Mike Thompson
Mr. James McConnell
Mr. Patrick Rhoads
Mr. Herman LeDoux
Mr. Mark B. Whitaker Jr.

SEPARATION

PAGE

Board Findings
Chemistry and Metallurgy Research Replacement Facility: Congressional Certification Review

Topic: Design Control

Finding Title: Documenting and Maintaining Preliminary Documented Safety Analysis Safety-Related Functions and Requirements

Finding: The overall approach to establishing and maintaining functional and operational requirements can be found in the following CMRR documents: (1) CMRR Program Requirements Document (PRD) (CMRR-PLAN-PM-0101, Rev. 0) January 2009, (2) CMRR Functional and Operational Requirements (F&OR) (CMRR-PLAN-ENG-2801, Rev. 0) January 2009, (3) CMRR Systems Engineering Management Plan (SEMP) (CMRR-PLAN-1905, Rev. 0) September 2007, (4) CMRR Configuration Management Plan (CMP) (CMRR-PLAN-ENG-0301, Rev. 0) December 2008, and (5) CMRR Facility Design Description (FDD) (CMRR-FDD-001, Rev. 0B) January 2009.

Review of these documents indicates that requirements generated through the safety basis development process are not adequately and explicitly integrated into the overall approach to Design Control.

The Preliminary Documented Safety Analysis (PDSA) is the fundamental document that identifies safety-class (SC) and safety-significant (SS) structures, systems, and components (SSCs). Once identified, the PDSA establishes an appropriate set of safety functions (see PDSA Table 3-37), and for each safety function a set of functional requirements and performance criteria are established (see PDSA Chapter 4). The safety envelope for CMRR depends on maintaining control of these functions, requirements, and criteria. Review of the PRD, F&OR, SEMP, CMP, and FDD indicates that this control has not been established.

The PRD requires that CMRR develop a SEMP, and that the SEMP (1) establishes the hierarchy of technical documents and demonstrates how requirements are flowed down, (2) explains how requirements are allocated down to SSCs, and (3) that commits to crosswalk the safety case for SSCs with the design features. As noted above, the PDSA establishes the safety case. Review of the SEMP indicates that the systems engineering process does not include information generated from the PDSA. The SEMP describes an approach that can be labeled "a classic project management approach" (top-down derivation of functions and requirements), silent on the overall roll and preeminence of requirements generated from the PDSA.

The CMRR F&OR is consistent with the PRD, largely silent on requirements generated from the PDSA. The F&OR does include a requirement (R.0.7.m) that "Prior to Title I design of the CMRR, facility design features pertaining to meeting safety, security, and quality assurance criteria shall be identified and tracked as part of the project's technical baseline." It is not clear that the project has met this functional requirement.

The CMRR CMP establishes the overall approach to design control, using the CORE database to establish relationships between functions, requirements, and systems. The CMP indicates that requirements from the PDSA should be explicitly incorporated in the CORE database. However, review of the CMRR FDD suggests that key safety terms such as "safety functions" and "functional requirements" may not be consistent with how this terminology is intended in the PDSA. Review of the FDD design requirements indicates that the basis for these requirements is "code/standard" driven; the link and integration from the PDSA is missing. Given this, integration between the PDSA and System Design Descriptions (SDDs) is questioned.

The CMRR CMP also establishes the overall approach to change control. It is not clear how the change control process establishes appropriate change control of the PDSA safety envelope, specifically change control of SC and SS SSCs, and their safety functions and functional requirements. The change control process should include the appropriate level of control for critical safety-related decisions (note that the

Safety Validation Report is how NNSA formally accepts the safety envelope).

Ultimately, SDDs have been developed for each CMRR structure and system. The content of SDDs is described in DOE-STD-3024; the intent of this standard is that SDDs should contain requirements that are derived from the PDSA. This requires that terminology (safety functions and functional requirements) between the PDSA and SDD be consistent to ensure that the safety envelope is properly translated into design requirements, and properly maintained throughout design and operation.

In conclusion, the CMRR project has not developed a requirements approach that formally integrates the safety envelope established by the PDSA. The SEMP is out-of-date and does not fulfill the requirements from the PRD. The CMRR FDD introduces terminology that results in inconsistency with the PDSA. As a result, there is lack of confidence that the FDD and SDDs will properly capture requirements from the PDSA.

Basis for Finding: (1) 10 CFR Part 830.122 (f) (2) Incorporate applicable requirements and design bases in design work and design changes.

(2) DOE Order 413.3A (5)(a) Requirements set forth in this Order are established to ensure adherence to the following principles: (2) Sound disciplined up-from planning, (4) Well-defined and managed performance baseline, and (5) Effective project management systems.

(3) DOE Order 413.3A (5)(i)(3) Change control ensure that project changes are identified, evaluated, coordinated, controlled, reviewed, approved/disapproved, and documented in a manner that best serves the project.

(4) DOE Standard 3024 The SDD is the central coordinating link among the engineering design documents, the facility authorization basis, and implementing procedures. The SDD should contain requirements that are derived from the associated safety analysis.

Suggested Resolution or Path Forward: The CMRR project needs to commit to revising the SEMP, CMP, and SDDs to explicitly incorporate requirements from the PDSA. The PDSA safety functions and functional requirements should be explicitly listed in the applicable SDDs. The CMRR project needs to develop a change control process that formally establishes an appropriate level of change control on SSC safety functions and functional requirements to maintain the safety envelope. Schedules for these revisions should be developed as part of the NNSA response.

NNSA Response:

DNFSB Final Resolution:

DNFSB: Roy F. Kasdorf (Roy Kasdorf) 3/4/09 (Date)	NNSA: _____ _____ (Date)