A.J. Eggenberger, Chairman
John E. Mansfield
Joseph F. Bader
Larry W. Brown
Peter S. Winokur

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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

July 30, 2007

The Honorable Samuel W. Bodman
Secretary of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

Dear Secretary Bodman:

The prevention and mitigation of potential accidents inherent in the mission activities at defense nuclear facilities is a fundamental objective that requires the Department of Energy (DOE) and its contractors to identify accident scenarios and then establish effective and reliable safety controls to address them. Engineered controls are preferred over administrative controls because, in general, engineered controls are considered to be more reliable and effective than administrative controls. At times, administrative controls will be required to perform specific safety functions. Examples of administrative controls include discrete operator actions, or programmatic controls such as combustible loading programs (associated with fire protection programs), operator training programs, and inservice inspection programs.

Observations relevant to the development and implementation of administrative controls in the DOE defense nuclear complex were the basis for the Defense Nuclear Facilities Safety Board's (Board) Recommendation 2002-3, *Requirements for the Design, Implementation, and Maintenance of Administrative Controls*. On January 4, 2007, DOE informed the Board that all of its actions and commitments associated with the Implementation Plan for Recommendation 2002-3 had been completed and proposed that the Recommendation be closed. In a letter dated January 22, 2007, the Board acknowledged the progress made by DOE in response to the Recommendation, and indicated that the Board's staff would conduct field reviews of a representative sample of defense nuclear facilities to independently assess the adequacy and effectiveness of DOE's efforts in implementing the Recommendation before reaching a decision on closure. Based on those field reviews, the Board has determined that Recommendation 2002-3 must remain open.

The results of the staff's reviews, which is enclosed with this letter, indicate that a number of systemic weaknesses exist in the Recommendation's implementation across the defense nuclear complex. Examples of these include, but are not limited to, deficiencies in developing programs to ensure (1) the long-term effectiveness of specific administrative controls and (2) the appropriate classification of critical support systems for specific administrative controls. Further, it appears that a number of major defense nuclear facilities have not yet fully

implemented the Recommendation. Moreover, the Board is concerned that DOE audits and self-assessments, as specified in Commitment 4.7 of the Implementation Plan to assess the overall effectiveness of the program, were ineffective in identifying the implementation issues cited in the enclosed report.

Therefore, pursuant to 42 U.S.C. § 2286b(d), the Board requests a briefing within 45 days of receipt of this letter describing the specific actions DOE will take to further ensure the implementation of Recommendation 2002-3 in the field.

Sincerely,

A. J. Eggenberger
Chairman

c: The Honorable J. Clay Sell
The Honorable James A. Rispoli
The Honorable Thomas P. D'Agostino
Mr. Mark B. Whitaker, Jr.

Enclosure

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

June 22, 2007

MEMORANDUM FOR: J. K. Fortenberry

COPIES: Board Members

FROM: J. L. Shackelford

SUBJECT: Review of the Implementation of Recommendation 2002-3, *Requirements for the Design, Implementation, and Maintenance of Administrative Controls*

This report documents a series of reviews of the Department of Energy's (DOE) implementation of the Defense Nuclear Facilities Safety Board's (Board) Recommendation 2002-3, *Requirements for the Design, Implementation, and Maintenance of Administrative Controls*, at selected facilities in the defense nuclear complex.

Background. On December 11, 2002, the Board issued Recommendation 2002-3 to DOE, which DOE accepted on January 31, 2003. On June 26, 2003, DOE issued an Implementation Plan for the Recommendation. Subsequently, DOE issued a letter, dated January 4, 2007, informing the Board that all of the commitments in the Implementation Plan had been completed and proposing that the Recommendation be closed. On January 22, 2007, the Board responded to DOE's request for closure. The Board acknowledged that progress had been made in response to the issues addressed by the Recommendation. However, the Board indicated that its staff would conduct field reviews of a representative sample of defense nuclear facilities to independently assess the adequacy and effectiveness of DOE's efforts in implementing the Recommendation before reaching a decision on closure. The results of the staff's reviews are summarized below.

Review of the Implementation of Recommendation 2002-3 at Selected Defense Nuclear Facilities. The central element of DOE's response to the Board's Recommendation dealing with administrative controls was the development of the concept of a specific administrative control (SAC). In general terms, a SAC is an administrative control that would be categorized as either safety-significant or safety-class if the function it served were implemented through an engineered structure, system, or component. The staff reviewed the policies, programs, and processes for the development and implementation of SACs at the Pantex Plant, Savannah River Site (SRS), and Y-12 National Security Complex. These reviews encompassed an assessment of the general process for developing SACs, including how the hazard and accident analysis processes flowed into the development of SACs. The reviews also focused on the activities associated with procedure development, training and qualification, assessment of the adequacy of SACs, implementation of SACs, and root-cause assessments and lessons-learned efforts associated with identified weaknesses in SACs. The staff selected a number of SACs for

detailed evaluation and assessment to determine whether all of the expectations and requirements embodied in the Board's Recommendation were being met. The staff also assessed the respective DOE Site Office's oversight of SACs.

At each of the sites reviewed, the staff found that the contractor had formulated and implemented a systematic process for the development of safety bases that addressed the guidance and requirements associated with SACs as defined in DOE Standard 3009, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, Change Notice 3, and DOE Standard 1186, *Specific Administrative Controls*. At the same time, however, the staff noted a number of weaknesses in the implementation of the Recommendation. Examples of these weaknesses are summarized below.

Pantex Plant

- The contractor's definition of SACs was limited to those controls that serve a safety-class function. This approach effectively reduces the scope of SACs as defined in the currently approved guidance, which includes both safety-class and safety-significant functions. The staff discussed this issue with DOE and the contractor, noting that the site's interpretation of the scope of SACs represents a fundamental flaw in the implementation of the Recommendation. Subsequent to the staff's review, DOE directed the contractor to revise applicable site specific guidance documents to better align with DOE Standard 1186 requirements for safety-significant SACs.

- Neither DOE nor the contractor had developed any programs, plans, or schedules to ensure or assess the ongoing adequacy of the SACs. The staff concluded that the long-term effectiveness of the SACs would require a robust, ongoing, periodic assessment to verify that operators are maintaining the proficiencies required to implement the controls. Subsequent to the staff's review, DOE directed the contractor to periodically verify the effectiveness SACs.

- The contractor asserted that SACs could be made more reliable by requiring an independent verification, concurrent verification, or second checker for some important operator actions. In some cases, this second verification was accomplished through a separate signoff step in the applicable procedures or by having the second operator "stamp" the applicable step in accordance with the established plant process of procedural verification and compliance. In other cases, the verification was simply directed by procedures and did not require either signoff or stamping. Although the intent, and the credit taken, for the second verification was identical in both of these cases, the methods used to accomplish the verification and document its completion were inconsistent and did not necessarily reflect the same level of assurance.

Savannah River Site

- The contractor had credited a safety management program in lieu of an engineered feature or SAC in the hazard analysis, contrary to the approved guidance and expectations. Specifically, the radiological protection program was credited with protecting facility workers in a scenario associated with the dropping of a non-3013 storage container in the K-Area Interim Surveillance Project. When the staff raised this issue, the contractor reevaluated the scenario and addressed the issue with a new SAC and Limiting Condition for Operation. Additionally, the contractor initiated a series of facility assessments to determine the extent of the issue and review the basis for its SACs.

- The implementing guidance for at least one SAC lacked the level of detail necessary to accomplish its safety function. In this example, periodic inspection of the Old HB-Line exhaust system duct in Building 292-H was identified as a SAC in the facility Technical Safety Requirements (TSR). The intent of this SAC was to ensure that the exhaust duct would remain intact to prevent the potential release of contamination during accident scenarios. However, it was noted that neither the TSR nor the implementing procedures for conducting the inspection contained the guidance and level of detail necessary to ensure that the intended acceptance criteria demonstrating the integrity of the duct would be met. Further, during a walkdown of the system, the staff observed that significant portions of the duct could not be inspected because of its routing through confined spaces, contaminated areas, and high overhead areas. As a result, the staff questioned the overall effectiveness of a visual inspection in accomplishing the objectives of this SAC.

- The staff noted that a number of the SACs contained a requirement for various levels of independent verification or second checking. While the expectations for most of these requirements were generally clear, there was a lack of specificity with respect to the definition of "qualified observers" for some of the SACs. In particular, a number of steps associated with H-Canyon crane operations specified that a qualified observer should observe and sign off on the required step. However, discussions with operations personnel yielded conflicting information as to the qualifications and responsibilities of a qualified observer.

- Similar to the situation at Pantex, the staff observed that programs, plans, or schedules did not exist for assessing or reviewing the adequacy of SACs on a periodic basis. This observation applied to DOE oversight activities as well as the contractor's own self-assessment program. When the staff raised this issue, the contractor agreed to develop an approach for periodically assessing the effectiveness of SACs.

- At the time of the staff's review, the SAC analysis had not been completed for the Tritium Extraction Facility; rather, SACs are being incorporated into the fiscal year

annual update of the 2007 Documented Safety Analysis. As a result, full implementation of the Recommendation was incomplete at SRS.

Y-12 National Security Complex

- The SACs for Building 9212 had not been implemented as of the staff's review. Consequently, implementation of the Recommendation was incomplete at Y-12.

- Contrary to the guidance in Section 3.2.1 of DOE Standard 1186, none of the SACs that had been implemented required independent verification by a second qualified operator, even though these controls in many cases constituted the single credited safety control for the hazard of concern. Examples of this weakness included SACs associated with hazardous material inventories, combustible material loading controls, and calibration of equipment important to safety.

- The TSR and implementing procedure for at least one SAC contained an insufficient level of detail for the operator to adequately satisfy the intent of the control. In this example, the SAC required the operator to verify that the combustible loading for a specific location remained within the limits prescribed by the fire hazards analysis. However, the implementing procedure and TSR did not specify these limits. Further, the fire hazards analysis referenced by the SAC did not specify the combustible loading limits in sufficient detail to allow the operator to implement the required surveillance effectively. The operators were unaware of the specific details necessary to ensure that the combustible loading in the affected area would remain below acceptable limits. As a result of the staff raising this issue, the contractor initiated a site-wide review of SACs to determine whether sufficient specificity was embodied in the implementing procedures.

- The contractor developed a unique category of SACs for non-nuclear applications, which are not described in DOE Standard 1186 or elsewhere in the DOE directives system. The staff determined it was possible that confusion could occur in the treatment of these SACs relative to those designated for nuclear applications.

- The contractor had not adequately considered the safety classification of a critical system necessary to support one of the SACs as outlined in DOE Standard 1186, Section 3.3. In this instance, the SAC was to maintain the oxygen level in a glovebox at less than 2 percent to avoid an explosion. This SAC depended on the indication and alarm from an oxygen monitor for an operator to take the appropriate safety-related actions in response to an abnormal condition. However, this indication and alarm system did not have a safety pedigree. Further, when questioned by the staff about the response to an alarm, the operator did not refer to the alarm response procedure and indicated that he would take action inconsistent with that outlined in the procedure. Further review revealed that the calibration activities for the indication and the alarm system lacked the discipline and rigor

typically associated with safety-related systems. In particular, the system lacked a formal setpoint analysis, verification of a fail-safe circuit and alarm design, and independent verification of calibration adequacy. As a result of the staff raising this issue, the contractor committed to reevaluating the safety pedigree of the alarm instrumentation. Further, DOE indicated that portions of the indication system and alarm would be upgraded to safety-significant.

Summary. Although considerable progress had been made toward addressing the issues outlined in Recommendation 2002-3, the staff's review found that significant and apparently systemic weaknesses existed in the implementation of Recommendation 2002-3 across the defense nuclear complex. While each of the facilities reviewed had developed a systematic process for the development of safety bases that addressed the guidance and requirements defined in DOE Standard 3009 and DOE Standard 1186 for SACs, the Board's staff observed numerous weaknesses in the Recommendation's implementation suggesting additional efforts would be necessary to fully realize the benefits envisioned by the Board. These included weaknesses in developing programs to ensure the long-term effectiveness of SACs, providing the specificity and level of detail necessary to accomplish the desired safety objectives of SACs, ensuring that critical support systems for SACs are appropriately classified, specifying the need for independent or concurrent verification, and inappropriately crediting safety management programs in lieu of SACs or engineered controls. Further, the Board's staff observed that a number of major defense nuclear facilities had not yet fully implemented the Recommendation.

In response to the staff's observations and findings, a number of corrective actions have been taken at the facilities that were reviewed to address many of the identified deficiencies. The staff is concerned that DOE and contractor audits and self-assessments had not identified the deficiencies observed by the Board's staff.

Commitment 4.7 of the Implementation Plan indicated that DOE would evaluate the overall success of the effectiveness of the implementation of the Recommendation. In its letter of January 4, 2007, DOE informed the Board that all of the commitments in the Implementation Plan had been completed and proposed that the Recommendation be closed. The staff's observations show that DOE's review was not effective in identifying the weaknesses, deficiencies, and incompleteness of the Recommendation's implementation, and that additional effort and attention in this area is warranted before the Recommendation can be closed.