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

Mr. Daniel E. Glenn
Manager
Pantex Site Office
U.S. Department of Energy
P.O. Box 30030
Amarillo, Texas 79120

Dear Mr. Glenn:

The staff of the Defense Nuclear Facilities Safety Board (Board) recently performed a review of the authorization basis at the Pantex Plant. As documented in the enclosed report, the Board's staff noted a loss of configuration control of Documented Safety Analyses (DSAs) at Pantex in the last several years, as well as a backlog of hundreds of post-start conditions of approval resulting from reviews of authorization basis documents by the Pantex Site Office. The staff also uncovered issues related to (1) the incomplete treatment of beyond design basis accidents in certain DSAs, (2) the lack of adequate detail for proper implementation of Technical Safety Requirements, and (3) the systematic lack of timeliness in identifying and declaring a Potential Inadequacy of the DSA (PISA) after new information is discovered.

The Board is aware that BWXT-Pantex is addressing several of these issues. BWXT has agreed to improve the treatment of beyond design basis accidents for identified DSAs. BWXT has also stated that adequate detail will be added to Technical Safety Requirements (TSR) through the efforts of the End-State DSA project plan and annual updates to the DSAs. In addition, the Pantex Site Office has requested that BWXT develop a technical basis for dispositioning new information to ensure that PISAs are appropriately identified and declared in a timely manner. The Board's staff will continue to monitor these corrective actions to ensure satisfactory resolution of the above issues and other efforts to improve authorization basis review and TSR implementation at the Pantex Plant.

Sincerely,

A. J. Eggenberger
Chairman

c: Mr. Mark B. Whitaker, Jr.

Enclosure

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

June 19, 2007

MEMORANDUM FOR: J. K. Fortenberry, Technical Director

COPIES: Board Members

FROM: R. Rauch

SUBJECT: Authorization Basis Review at the Pantex Plant

This report documents a review by the staff of the Defense Nuclear Facilities Safety Board (Board) regarding the authorization basis (AB) at the Pantex Plant. Staff members F. Bamdad, R. Layton, C. Martin, R. Rauch, and site representative D. Kupferer participated in discussions with site personnel during the week of April 23–27, 2007. The staff evaluated the review and approval of AB documents by the Pantex Site Office (PXSO); the accident analyses and Technical Safety Requirements (TSRs) for the W76, W78, and W87 Hazard Analysis Reports (HARs); and processes for New Information (NI), Potential Inadequacy of the Documented Safety Analysis (DSA) (PISA), and Unreviewed Safety Questions (USQ).

Background. Title 10 of the Code of Federal Regulations, Part 830 (10 CFR 830), *Nuclear Safety Management* (Rule), required all contractors responsible for hazard category 1, 2, and 3 nuclear facilities to submit a Rule-compliant DSA by April 10, 2003. PXSO issued supplementary direction that DSAs be both submitted and approved by the April 2003 deadline. To comply with the requirements of the Rule and the direction of PXSO, the contractor submitted a series of Safety Analysis Report (SAR) "modules" and various supporting documents—including Fire and Lightning Bases for Interim Operation and an Interim Accident Analysis—that identified and analyzed hazards associated with facility operations, transportation activities, and specific weapon systems, and credited corresponding controls to establish an authorized safety envelope for nuclear operations at Pantex. These documents identified approximately 230 engineered and administrative controls that were functionally classified as either safety-class or safety-significant TSRs or designated in the DSAs as "important to safety." The process for implementing and validating these 230 controls was formally defined in the TSR Integrated Implementation Plan (TSRIIP), which began in October 2003 and was completed in October 2006.

During the execution of the TSRIIP, BWXT began to experience a number of AB-related challenges. As controls from the TSRIIP were implemented, numerous instances were discovered in which either the actual configuration of facility structures, systems, and components (SSCs) or the functional attributes or capabilities of existing SSCs were incorrectly or inappropriately described in the DSA. Delays in implementing approved AB change packages led to a loss of configuration control of the DSA; that is, the master, or "Posted," DSA no longer reflected the currently approved DSA. This discrepant condition existed for months, leading to situations in which the contractor prepared change packages against an outdated DSA

baseline. To address these critical AB issues, BWXT developed an integrated strategy, known as the End-State DSA project plan. That plan has undergone some revisions, but has maintained the same general objectives: to reconstitute configuration control of the DSAs, implement remaining TSRs, and transition to the set of documents that will ultimately compose the End-State DSA.

PXSO Review and Approval of Authorization Basis Documents. After evaluating each DSA, PXSO provides a Safety Evaluation Report to the contractor detailing the conditions of approval (COAs) of the DSA. During the staff's review, PXSO presented a list of open pre-start and post-start COAs—as well as open technical review comments (TRCs, the latest terminology for post-start COAs)—and its expectations for closure of these items. At the time of the staff's review, there were 462 open COAs (almost entirely post-start) and 192 open TRCs. The staff reviewed a subset of open COAs and TRCs and found none that, if closed, would reduce the risk accepted by PXSO in any significant way. However, the staff is concerned about the lack of emphasis by both BWXT and PXSO on the closure of post-start COAs and TRCs. In a January 31, 2005, letter to the Department of Energy (DOE), the Board requested that DOE provide the mechanism in place at each site office for verifying the adequacy of actions taken by the contractor to close open COAs. In response to the Board's letter, BWXT stated that post-start COAs would be closed during all annual DSA updates after completion of the TSRIIP. BWXT has now abandoned this effort and is instead developing a longer-term plan for closing the backlog of open COAs and TRCs. In addition, BWXT is counting on the End-State DSA project plan to close a number of COAs and TRCs through AB streamlining and attendant "natural improvements." The staff will continue to track the closure of COAs and TRCs in the coming months.

The staff asked PXSO to discuss its expectations for verifying the implementation of TSRs. During the initial stages of the TSRIIP, PXSO verified the implementation of all TSRs. The Board commended PXSO for this effort in a March 18, 2003, letter to the National Nuclear Security Administration (NNSA). However, PXSO subsequently found this approach to be onerous. PXSO abandoned its original strategy and now verifies the implementation of controls in an ad hoc manner. The staff is concerned about PXSO's change in strategy for verifying TSRs. In light of the implementation issues that BWXT encountered during the TSRIIP, it would be appropriate for PXSO to take a more vigilant approach and explicitly validate all of these controls.

Pantex Accident Analyses and Technical Safety Requirements. The staff reviewed the development and documentation of the Pantex TSRs. Two generic issues were identified: (1) the treatment of beyond design basis accidents in the DSA, and (2) the level of detail in the wording of functional requirements for controls in the TSR document.

Hazard and Accident Analyses—The Pantex DSAs have identified a comprehensive set of operational hazards, external events, and natural phenomena hazards for identification and classification of controls. However, the hazard analyses appear to be deficient in identifying and analyzing beyond design basis accidents as required by DOE directives. BWXT agreed to improve its treatment of beyond design basis accidents.

Technical Safety Requirements—The facility-level controls identified in the hazard and accident analyses are described in detail, including their functional requirements, in Chapters 3 (hazard and accident analysis) and 4 (safety SSCs) of a given DSA. However, the DSA's level of detail for safety-related controls and their functional requirements is not repeated in the Pantex TSR document. The staff found that the TSRs lacked adequate detail for implementation and compliance with DOE expectations as described in DOE Guides 421.1-1, *Implementation Guide for Use in Developing Documented Safety Analyses to Meet Subpart B of 10 CFR 830*, and 423.1-1, *Implementation Guide for Use in Developing Technical Safety Requirements*.

The staff discussed its observations in detail with the BWXT representatives. BWXT has launched an activity to insert the necessary details from Chapter 4 of the DSAs into the TSR document, consistent with the DOE requirements. The inconsistency with the DOE requirements is expected to be corrected gradually through the submittal of AB change packages.

In addition to the lack of adequate detail in the TSRs, the staff is concerned that BWXT, by categorizing certain TSRs as "safety management programs," may be making it difficult to incur a TSR violation for a one-time infraction. For example, Chapter 4 of the Sitewide SAR provides a list of all containers that are qualified to meet the functional requirements for protection of special nuclear material (SNM) from a fire. The Sitewide SAR refers to the Qualified Containers Program in its administrative controls section to ensure that the approved containers are used at the site. The containers are safety-class passive design features and must be identified as such in the Design Feature section of the TSR document. The use of an unapproved container would logically be a TSR violation. Under the umbrella of the Qualified Containers Program, however, the use of an unapproved container would be a safety management program infraction and would not constitute a TSR violation. Safety management programs can result in a TSR violation only if the program is violated repeatedly, thus demonstrating a systematic breakdown.

The staff also reviewed the design requirements for several safety-related design features to determine whether the controls are designed adequately to meet the safety functional requirements described in the DSA. The staff found that controls were not always implemented in a manner that guaranteed they would meet the requirements specified in the DSA. For example, the Sitewide SAR identifies noncombustible cabinets as safety-class design features that prevent materials stored inside the cabinet from contributing to the combustible loading in the event of a fire. BWXT performed several fire experiments to qualify the cabinets used at the site. These experiments showed that the combustible materials inside the cabinets ignited after the cabinet had been exposed to an external fire for 10 minutes. It was concluded that the cabinets are qualified for use in areas where safety-related fire suppression or deluge systems exist to limit the duration of a fire to less than 10 minutes. However, the TSR contains no mention of the need for noncombustible cabinets to be located in the vicinity of a fire suppression system. BWXT acknowledged this inadequacy in the TSR and agreed to correct it.

In reviewing Pantex safety documents, the staff discovered that a portion of the Pantex DSA could not be analyzed onsite due to security restrictions. A member of the BWXT staff is

planning to travel to Sandia National Laboratories, Albuquerque, in the next several months to update this analysis. The staff will review this topic with the BWXT staff member at that time.

New Information, Potential Inadequacy of the DSA, and Unreviewed Safety Question Processes. BWXT's process for declaring a PISA after discovery of New Information (NI) contains two highly subjective steps. When NI is discovered, it is assigned to a responsible engineer, entered into an NI database for tracking, and an initial determination of the maturity (i.e., either "draft" or "final") of the NI is made (first subjective step). If the NI is considered "final," a PISA is declared, and if sufficient documentation is available, a USQ evaluation is performed. However, if the NI is considered "draft," the need for compensatory measures is determined *before* a PISA is declared (second subjective step). In defense of this final step of the process, BWXT claims that the mere declaration of a PISA is onerous because of the associated reporting requirements and a specification in the site procedure that an evaluation of the safety of the situation must be performed within 10 days of the declaration. BWXT's position is that a PISA is warranted only if the safety of the situation necessitates compensatory measures.

The staff has several concerns regarding BWXT's process for declaring a PISA. Foremost among these is the contractor's threshold for declaring a PISA, given NI. The process and its associated rationale suggest an attitude of "prove it is unsafe" before taking action to resolve potential safety issues. An entry in the NI database that illustrates the staff's concern is discussed below.

In May 2004, a BWXT employee noted that, based on vendor data, it was impossible to tell whether certain facilities could meet the surge suppression requirements stated in the site AB. This discovery was entered into the NI database, and the system engineer began developing a methodology to test the functionality of the surge suppressors in question. These tests were finally performed in December 2005, and it was determined that the surge suppressors did not in fact function as required. A PISA was declared soon thereafter, but this protracted process allowed certain facilities to operate outside the PXSO-approved safety envelope for approximately 20 months.

The staff believes this scenario was a direct result of a flaw in the BWXT PISA process. The process allows the NI database to be used as a holding tank for information that should have resulted in a PISA. By labeling information as "draft," BWXT is able to extend the time frame for evaluation of the safety of the situation beyond that intended by the relevant DOE guidelines and site procedures. As specified by 10 CFR 830.203, *Unreviewed Safety Question Process*, upon discovery of a PISA, a USQ determination must be performed, and the contractor must notify DOE *promptly* of the results. The Pantex standard for implementing this requirement further specifies "hours or days (not weeks or months)" and requires an evaluation of the safety of the situation within 10 days of the declaration of a PISA. In the case of the above surge suppression issue, had a PISA been declared immediately, the relevant guidelines and site procedures would have forced a prompt evaluation of the safety of the situation and a USQ determination.

The staff understands that it is impossible to remove all subjectivity from the PISA process. For every instance similar to the NI related to surge suppression, there are likely others that do not warrant a PISA declaration. The staff notes that the above issue should not be construed as an indictment of the NI database. It provides the contractor a means of ensuring that all NI entries are properly captured and definitively tracked to closure. At this time, however, the NI database is not maintained with a rigor commensurate with the importance of its function. The staff provided this feedback to BWXT personnel, and they agreed to maintain the NI database with additional rigor.