DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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

September 27, 2004

The Honorable Linton Brooks
Administrator
National Nuclear Security Administration
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0701

Dear Ambassador Brooks:

The Defense Nuclear Facilities Safety Board (Board) recently reviewed an approved safety basis for a nuclear facility located at Sandia National Laboratories, New Mexico (SNL-NM). Based on the Board's review, as detailed in the enclosed report, the approved safety basis does not provide assurance that the operational hazards have been adequately analyzed and controlled.

Many of the inadequacies identified in the safety basis appear to reflect fundamental weaknesses in the implementation of nuclear safety requirements at SNL-NM. The Sandia Site Office (SSO) has taken action to require improvements in SNL-NM's safety basis methodology, but the inadequacies in this safety basis remain. Allowing these inadequacies to go uncorrected permits the startup of a facility without an assurance that all hazards have been adequately addressed. Allowing an inadequate safety basis to go un-corrected also compromises the long-term integrity of the change control system, which relies on adequate safety analyses to serve as a baseline for assessing the impact of future changes.

Because of the fundamental nature of the deficiencies identified in this safety basis, the Board has concerns regarding the other safety bases currently approved for use at SNL-NM. Therefore, pursuant to 42 U.S.C. § 2286b(d), the Board requests a report and briefing within 90 days of receipt of this letter that addresses the following areas:

- The adequacy of safety bases for each currently operating nuclear facility at SNL-NM.

- Actions to be taken to ensure more effective closure of comments from future safety basis review teams.

- Actions to be taken to ensure that adequate draft safety bases are submitted by the SNL-NM contractor in the future.

Sincerely,

John T. Conway
Chairman

c: Mr. Richard Black
Mr. Richard Englehart
Mr. Mark B. Whitaker, Jr.

Enclosure

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

August 12, 2004

MEMORANDUM FOR: J. K. Fortenberry, Technical Director

COPIES: Board Members

FROM: D. Nichols

SUBJECT: Inadequate Documented Safety Analyses at Sandia National Laboratories

This report documents issues identified by members of the staff of the Defense Nuclear Facilities Safety Board (Board) D. Nichols, W. Andrews, F. Bamdad, and D. Kupferer regarding the approved Documented Safety Analysis (DSA) for the Auxiliary Hot Cell Facility (AHCF) at Sandia National Laboratories (SNL), New Mexico. The staff reviewed the DSA and held a series of discussions with SNL and National Nuclear Security Administration's (NNSA) Sandia Site Office (SSO) personnel who were involved in the development, review and approval of the DSA. These discussions were held on August 3–4, 2004, at which time the Board's staff also conducted a walkdown of the facility.

Based on this review, the Board's staff concluded that the DSA does not provide confidence that workers and members of the public are adequately protected from the hazards of the planned operations. In making that determination, the staff identified a number of specific hazards that had been inadequately analyzed and/or inadequately controlled, potentially affecting both worker and public receptors. The methodology used to develop and present the hazard and accident analysis was inconsistent with the approved standard for the development of DSAs. Discussions with site personnel indicated that the underlying weaknesses are not limited to this single DSA, but reflect fundamental problems in the approach used to analyze Technical Area (TA)-V nuclear facilities at SNL.

Background. The AHCF was built to facilitate the sorting, categorization, and repackaging of legacy materials that SNL has categorized as having "no defined use." These materials include radioactive and transuranic waste and fissile isotopes, and may also include mixed waste. Physically, the AHCF is a relatively small collection of structures that are completely contained within the high bay of an existing facility. It includes a shielded hot cell, a permanent shield wall, eight floor silos, and a walk-in fume hood, together with associated cranes, remote manipulators, and video cameras to record operations and facilitate remote-handled operations. A ventilated temporary room may also be constructed as needed behind the shield wall to accommodate items that cannot fit in the hot cell or fume hood. The temporary room is considered part of the AHCF.

No systems, structures, and components are classified as safety-class for the AHCF; the maximum unmitigated exposure to an off-site individual from an accident at the facility is estimated to be 5 rem. The safety analysis identified six safety-significant structures, systems, and components: the hot cell structure, permanent shield wall, silo plugs, hot cell ventilation system, high-efficiency particulate air (HEPA) filters, and trenches in the floor of the high bay. The AHCF was designed to operate as a Hazard Category 3 nuclear facility. It has an approved DSA and has undergone an Operational Readiness Review, but operations have not yet commenced. The Operational Readiness Review identified a number of significant issues, and the final report recommended that an additional, independent verification of readiness be performed prior to startup of the facility. The report also questioned the hazard categorization assigned to the facility, suggesting that it may have been lower than appropriate.

Discussion. The Board's staff identified significant inadequacies in the approved DSA, including among others, deficiencies in the analysis of hazards to members of the public, hazards not adequately identified or controlled, and inadequate design requirements. The more significant of these deficiencies are discussed in the paragraphs that follow; however, the inadequacies described here are but a sampling of the problems with the DSA. Additional discussion can be found in the 111 comments made by NNSA's Safety Basis Review Team (SBRT) on the final draft version of the DSA that was submitted for approval to SSO. SNL's responses to most of the SBRT's comments were inadequate to fully resolve the issues raised. Thus, most of those SBRT comments remain valid concerns.

Hazards to Members of the Public—The AHCF is situated just over 3000 m inside the boundary of Kirtland Air Force Base (KAFB) on TA-V, one corner of a parcel of land controlled by SNL. The AHCF DSA, like all of the DSAs for nuclear facilities within TA-V, uses the 3000 m distance to the KAFB boundary to define the radius of a circle that SNL uses as the virtual site boundary for the facility. The dose to the maximally exposed offsite individual (MEOI) for the unmitigated worst-case accident at the facility is estimated to be 5 rem at the edge of this 3000 m circle.

However, the selection of a 3000 m radius to define a virtual site boundary is not consistent with DOE standards, and does not properly protect members of the public who have unfettered access to recreational areas within the 3000 m radius. DOE standards specify that the area within the site boundary must be controlled by DOE and its contractors *without the aid of outside authorities.*[1] A number of facilities that are used by the public are within 3000 m of TA-V. These include horse stables, a riding club (1.6 km from TA-V), and the base golf course

[1] The site boundary is defined in DOE Standard (STD) 3009-94 CN2 as a "well-marked boundary of the property over which the owner and operator can exercise control without the aid of outside authorities. For the purpose of implementing this Standard, the DOE site boundary is a geographic boundary within which public access is controlled and activities are governed by DOE and its contractors, and not by local authorities. A public road traversing a DOE site is considered to be within the DOE site boundary if, when necessary, DOE or the site contractor has the capability to control the road during accident or emergency conditions." The standard defines the public as "all individuals outside the DOE site boundary."

and clubhouse (2 km from TA-V). These facilities and the area between them and TA-V are not controlled by the Department of Energy (DOE) or its contractors; they are controlled by the Department of Defense (DoD). There are no markings within the KAFB boundary to indicate when an individual has entered the 3000 m area around TA-V, and no provisions have been made to exclude personnel from this area. On the contrary, this area contains facilities that invite occupancy by members of the public. The stables, riding club, and golf course are frequently inhabited by military dependents, retirees, and invited guests. These persons fit the technical meaning of "the public" as defined in DOE standards, and some of the military dependents are persons who reside inside the boundaries of KAFB and have unfettered access right up to the boundary of TA-V (less than 200 m from the AHCF). Also within the 3000 m radius are a munitions storage facility (1.9 km), the Manzano Fire Station #3 (2.5 km), and the Manzano offices (2.7 km), all of which are controlled and operated by DoD personnel.

Based on charts included in the SNL's Emergency Planning Hazard Analysis Document, the dose to an individual at 1500 m from the AHCF can be as much as five times that at 3000 m. Thus, the evaluation guidelines are challenged if the MEOI is more correctly identified as the military spouses and children at the horse stables or golf course, indicating the need for safety-class controls.

Hazards not Adequately Identified or Controlled—A brief review of the DSA, together with a walkdown of the facility, revealed a number of specific hazards that had not been addressed or that had been addressed inadequately. Examples include the following:

- The analysis of an accident involving the drop of a container while being hoisted from the high bay into the hot cell underestimated the consequence and adequate controls were not established. The facility uses overhead cranes to transfer material from the high bay into and out of the hot cell, lifting the material about 30 ft. Forklifts are also used to move containerized material within the high bay. The bounding accident associated with a drop of a container in the high bay should have considered the maximum amount of material that can be in a container, with consequent combustion of the drum contents. These assumptions were used for the analysis of a fire in the hot cell, resulting in an unmitigated consequence of 5 rem at the assumed site boundary (3000 m). As a result, a safety-significant HEPA filter and ventilation system were identified for the hot cell. However, no safety significant controls were identified for a drop in the high bay. The high bay has no filtration or confinement capabilities and is kept at a significantly higher pressure than ambient. Thus, any release resulting from the drop and breach of a container would reach the environment essentially unmitigated.

- A drop during a lifting operation in the high bay could be initiated by a seismic event. Although the hot cell was built to Performance Category (PC)-2 requirements, the overhead cranes and supporting high bay structure meet only PC-1 requirements. The DSA did not identify this failure to satisfy the requirement for the cranes and supporting structure to meet PC-2 requirements.

- The hot cell structure and ventilation system perform a safety-significant confinement function. However, the hot cell itself is built only to PC-2 requirements, which do not provide for survivable confinement after a seismic event. The ventilation system is not built to PC-2 requirements. Thus, it does not provide confinement of material released during a fire inside the hot cell that is initiated by a seismic event. The DSA did not identify or address this deficiency.

- The DSA did not address the long-term radiological contamination of the hot cell. For example, the Technical Safety Requirements (TSRs) did not require that the ventilation system be active when the cell is not in operation. However, the hot cell does not provide confinement without active ventilation; an extended shutdown of the ventilation system, which would be allowed by the TSRs, would almost certainly result in contamination of the high bay once the hot cell itself had become contaminated. There was no provision in the DSA or TSRs to address this eventuality, as well as other issues associated with long-term contamination of the hot cell, fume hood, and ventilation system.

- The hazard analysis identified the presence of a natural gas line that passes through the facility. A leak from this line or a rupture during a natural phenomena event could lead to a deflagration within the facility, worker injury or death, and attendant material release up to the maximum amount of material staged outside of the hot cell. However, the DSA did not provide controls for this hazard, such as a seismic shutoff switch or gas sniffers, nor did it analyze the potential for a simple gas line leak (from other than natural phenomena hazards). Natural gas is not needed for AHCF operations, but the DSA did not address the rationale for not removing the gas line from the facility.

- The hazard analysis determined that a forklift or vehicle fire would result in serious worker injury or death, yet identified no safety-significant controls for this scenario as required by DOE directives. Nor did it identify the mechanisms by which the forklift or vehicle might catch fire. To control this hazard, the DSA relied upon maintenance and other administrative programs without specifying what features of those programs would provide the required protection.

- Immediately adjacent to the high bay is a mid-bay that is not managed by the same organization as the AHCF. The mid-bay is used by security forces as a storage facility and has accumulated a significant amount of combustible material. It has a common wall with the AHCF that is not fire rated. The combustible loading within the mid-bay is significant, and, according to a fire protection subject matter expert, the sprinkler system is not capable of fully extinguishing a fire in the mid-bay, given the combustible loading. This hazard was not addressed in the DSA or underlying analyses.

- As noted in the SBRT's comments, the fire protection analysis for the facility identified a number of significant fire protection issues that did not appear to have been adequately resolved in the DSA.

- Aircraft crashes were not thoroughly analyzed, even though the facility is located within the take-off and landing pattern approximately 5 miles from the jointly operated Kirtland Air Force Base and Albuquerque airport. Given their proximity to each other, multiple TA-V nuclear facilities could be affected by a single aircraft crash. TA-V is also located on a direct vector associated with one of the runways.

- Operational hazards were not comprehensively addressed in the DSA. The DSA relied on future hazard analysis of specific operations (called campaign plans) to identify the hazards and their associated controls. For example, hydrogen deflagration of a waste drum in the facility was not identified in the DSA as a potential event. The DSA relied upon future campaign plans to identify this hazard and its associated safety controls; significantly, the DSA did not require that individual campaign plans be approved by NNSA. The relegation of facility hazard analysis to future plans that do not require DOE approval is inconsistent with DOE-STD-3009-94 CN2. It should be noted that a similar hazard at other nuclear facilities has led to the identification of safety-significant controls for worker protection.

Inadequate Design Requirements—The AHCF is the result of a modification to the Temporary Hot Cell, a temporary facility that was built inside of the high bay of Building 6597 in 1996. The modifications included the addition of a permanent shield wall, floor silos, a new hot cell roof, a fume hood, an upgraded ventilation system (that included HEPA filtration), upgraded cranes, and the installation of video cameras. However, important design requirements do not appear to have been met, either in the original construction of the Temporary Hot Cell or in its modification to become the AHCF. These requirements are found in both DOE Order 420.1, *Facility Safety*, which was introduced in 1995 and incorporated into the SNL-NM contract in 1998, and its predecessor, DOE Order 6430.1A, *General Design Criteria*. DOE Order 420.1 is referenced in the AHCF DSA as the basis for its facility safety requirements.

- The design of new facilities or major modifications is required to be based on the confinement of hazards. In a letter to DOE dated July 8, 1999, the Board emphasized that such confinement systems for Hazard Category 2 and 3 nuclear facilities should be classified as safety-class or safety-significant, commensurate with the hazards. The external structure of the AHCF (the high bay of Building 6597) is not capable of confining the hazards and is not identified as a safety-related design feature. Several events could occur inside the AHCF but outside the hot cell, that is, within the high bay. The high bay ventilation system keeps the facility above atmospheric pressure and does not have a HEPA filtration capability. Accidental releases of radioactive materials in the high bay would be discharged directly to the environment.

- Facility structures are required to provide appropriate protection from expected natural phenomena events. The exterior walls of Building 6597 are designed to PC-1 design requirements for natural phenomena hazards, even though the AHCF contained within Building 6597 is a Hazard Category 3 nuclear facility in which accidents could result in significant consequences to workers. A seismic event could result in the total collapse of Building 6597, destruction of the hot cell by the falling crane, and rupture of the natural gas pipe in the facility. Such an event is shown in the DSA to result in significant radiological consequences to the collocated workers and a dose of about 5 rem at 3000 m from the facility. Although the hot cell and the permanent shield wall are identified as safety-significant design features and designed to meet PC-2 seismic requirements, their integrity cannot be assured if the crane (supported by PC-1 walls) collapses on these structures in a seismic event. Site personnel stated that their procedures (instead of a TSR-level administrative control) require the overhead crane to be parked away from the hot cell. However, during its walkdown of the facility, the Board's staff observed that the crane was parked where it could fall onto the hot cell during a building collapse.

Other Inadequacies—The Board's staff identified the following additional inadequacies in the DSA:

- The TSR bases and derivations were ambiguous as to what they actually required. For example, the TSRs included a Limiting Condition for Operation (LCO) that restricted material quantities within the facility to levels below the Hazard Category 2 thresholds. If those limits were exceeded, one action required the development and implementation of an approved recovery plan prior to resumption of operations. The action statement did not define who was to approve the recovery plan, which would by definition involve the temporary operation of this Hazard Category 3 facility with Hazard Category 2 quantities of material. In discussions with the Board's staff, SSO personnel indicated that their intent was for SSO to approve the recovery plan. SNL personnel, on the other hand, indicated that their understanding was that the shipping and receiving facility managers were the intended approval authorities.

- Similarly, there was confusion about the TSR requiring the development of specific campaign plans for each type of item to be processed at the AHCF. A required feature of these plans was that they "address the potential for criticality." This is an important requirement, as the facility's Hazard Category 3 classification depends upon the nature of the process precluding the potential for criticality, and because SSO approval of these plans is not required. When asked what "addressing the potential" for criticality meant, SSO personnel stated it meant that each plan must include a criticality safety analysis demonstrating that criticality was precluded without reliance upon double-contingency controls. SNL safety basis personnel, on

the other hand, were divided as to what the statement meant. Some agreed with SSO personnel, while others argued that the statement meant only that the potential for criticality had to be discussed in the campaign plan.

- The threshold material quantity values for facility hazard categorization identified in *Hazard Categorization and Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports* (DOE-STD-1027-92) were incorrectly applied, resulting in the inappropriate categorization of the facility. Two errors were made. First, Hazard Category 3 facilities are those with no potential for significant off-site accident consequences, and with only the potential for limited on-site accident consequences, interpreted by the standard as a worker dose of less than 1 rem at 100 m. Although the AHCF accident analysis used material quantity values from DOE-STD-1027-92 that were consistent with the upper thresholds of a Hazard Category 3 facility, the calculated consequence of 5 rem at 3000 m. should have indicated that the assumptions used in the development of the threshold material quantity values did not apply at the AHCF. According to Section 3.1.2 of DOE-STD-1027-92, final hazard categorization must be consistent with the ground rules on which the threshold tables were based. This was not the case for the AHCF.

  The second error was that the threshold fissile material quantity values that were selected from DOE-STD-1027-92 were only applicable for facilities in which the potential for criticality using those values was precluded by segmentation or the nature of the process. This was not the case for the AHCF, which relies upon administrative double-contingency controls to assure sub-criticality.

  DOE frequently grades its oversight and regulatory efforts based upon facility categorization, which in turn is expected to reflect the degree of hazard associated with a facility. Given the potential for significant non-localized accident consequences and the potential for criticality, Hazard Category 2 status was warranted for the AHCF.

- It is not possible, based upon the DSA, to determine the specific functional requirements and performance criteria that enable a control to prevent and/or mitigate a particular hazard scenario. Likewise, for a given accident scenario, the DSA did not clearly describe which controls were credited to perform specific preventive and/or mitigative safety functions. Instead, the discussion of controls in the accident analysis referred the reader to a simple listing of safety-significant controls, provided in a previous section. This list did not detail the specific functions provided by the controls or indicate their roles in interrupting particular accident sequences or providing mitigation. Consequently, it is impossible to verify that specific controls would accomplish their intended safety function. These deficiencies may be the result of the hazard and accident analysis approach that was followed. In general, the development of the hazard analysis did not implement the concept of an unmitigated hazard or accident scenario as described in DOE-STD-

3009-94 CN2. Instead, accident scenarios were discussed in general terms with little regard for the details of accident initiation and progression. It is difficult to identify the opportunities to interrupt specific accident sequences, and from those opportunities to derive the necessary characteristics of effective controls, when the accident sequences are not well defined.

After an independent review of the DSA and discussions with site personnel, the Board's staff concluded that this DSA does not meet the requirements and expectations set forth by the Department of Energy (DOE) in its *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, DOE Standard (STD) 3009-94 CN2, or in any other safe harbor standard approved for compliance with the Nuclear Safety Management Rule (Title 10, U.S. Code of Federal Regulations, Part 830 [10 CFR 830]). According to site personnel, the initial version of the DSA for the AHCF submitted for review resulted in more than 200 comments by the SBRT. The final version was reportedly a marked improvement, but still resulted in 111 comments by the SBRT, many of which reflected fundamental issues that had previously been identified but not adequately addressed. The SBRT was reportedly facing similar difficulties with other TA-V DSAs. As part of its performance evaluation process, SSO had graded SNL in the safety basis area with its lowest rating—red—in both of the last 2 years' performance appraisals, again underscoring the broad nature of the difficulties the site is facing in this area.

To address the improvements that SSO recognized were still needed in this DSA, SSO imposed conditions of approval that required actions by the Operational Readiness Review team to verify the effectiveness of certain controls. SSO is relying on anticipated upgrades to the analysis in the next annual update of the DSA, due in December 2004, to provide a more comprehensive hazard analysis. To address the broader concerns regarding safety basis inadequacies at TA-V facilities, SNL agreed to take steps to strengthen its central safety basis office, and to require approval by a central safety basis authority prior to the submission of a DSA to SSO.

However, the approved DSA for the AHCF remains deficient, and significant hazards have still not been adequately addressed. The incomplete hazard and accident analysis in the DSA will not allow the development of effective Unreviewed Safety Question determinations for future changes. Most significantly, the operation of the facility should not be permitted without an assurance that all hazards have been adequately analyzed and controlled; this DSA does not provide that assurance.

Conclusion. The DSA for the AHCF does not appear to be consistent with the safe harbor methodologies of the Nuclear Safety Management Rule, and does not provide an adequate assurance that the operational hazards have been identified through a comprehensive hazard and accident analysis. It would be advisable for NNSA to retract its determination that this DSA is compliant with the requirements of 10 CFR 830, and rescind its approval of the DSA until a version that meets the requirements of the rule is submitted. Similar actions ought to be taken for any other DSAs at SNL that have not complied with approved safe-harbor standards.