DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Washington, DC 20004-2901

August 5, 2010

The Honorable Thomas P. D'Agostino
Administrator
National Nuclear Security Administration
U. S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0701

Dear Mr. D'Agostino:

The Defense Nuclear Facilities Safety Board (Board) is concerned about a number of deficiencies in the accident analysis, control set, and safety system design at the Criticality Experiments Facility (CEF) at the Nevada Test Site. The Board is also concerned that inadequate technical expertise has been applied to evaluate and ensure safe operations.

The Board communicated several weaknesses and deficiencies in the CEF safety basis in letters to National Nuclear Security Administration (NNSA) dated March 27, 2006, and September 22, 2006. Your letter of December 7, 2006, stated that the safety issues identified in these two letters from the Board had been resolved. An enclosure to that letter detailed the resolution of those issues. However, recent reviews by members of the Board's staff revealed that, while the specific issues identified in prior Board's letters have been resolved, there remain a number of similar safety issues with the CEF design and safety basis, which fall into the following areas:

- Identification and evaluation of hazards;
- Identification of an adequate set of controls;
- Classification and design of the controls important to safe operation of the facility.

The nature of the issues identified during the staff's most recent review, which are specified in the enclosed report, indicates that the previously identified issues were likely systemic, and their root causes were not adequately addressed. Contributing to this deficiency, it appears that neither NNSA nor National Security Technologies, LLC (NSTec), the management and operating contractor at the facility, conducted sufficiently detailed design reviews of the facility. The enclosed report shows that existing problems may have been compounded by (1) NSTec's lack of in-house technical expertise in specialty subject matter areas crucial to the safety of activities conducted at CEF, and (2) NSTec's heavy reliance on Los Alamos National Laboratory (LANL), the facility user, and its safety process to propose, design, and implement the necessary controls.

While it is important that LANL retain highly qualified specialty technical experts to ensure the safety of its operations, it is equally important that the facility management and operating contractor, NSTec, be able to independently understand, review, and provide safety oversight of those activities. The lack of such specialized technical expertise, combined with weaknesses in the contractor's organizational structure and management processes, may have led to NSTec's failure to identify and resolve important safety issues.

Safe operation of CEF is important to performing national security missions, as well as enhancing safety at other nuclear facilities with commercial or defense-related missions. Both LANL's operational expertise and NSTec's organizational and operational safety capabilities are required to establish and maintain an adequate safety profile for CEF.

Therefore, pursuant to 42 U.S.C. § 2286b(d), the Board requests the following prior to the commencement of remote critical assembly machine operations at CEF, but no later than 90 days from receipt of this letter:

- A briefing and report on NNSA's plan, with schedule and milestones, to address the issues identified in this letter and enclosed report, including any systemic issues.

- A briefing and report that demonstrate the contractor's capability to support startup and safe operations at CEF, including any changes that may be necessary to provide the needed support for design reviews and the conduct of previously characterized experiments.

Additionally, pursuant to 42 U.S.C. § 2286b(d), the Board requests the following prior to the performance of critical experiments *not previously conducted* when CEF was located at Technical Area-18:

- An assessment of the technical expertise needed by the contractor and NNSA to establish and maintain an adequate and effective safety profile for CEF. This assessment should include a discussion on the availability of experienced individuals with specialized technical capabilities who can independently review and oversee the user's activities at CEF.

Sincerely,

Peter S. Winokur, Ph.D.
Chairman

Enclosure

c: Mr. Stephen A. Mellington
Mrs. Mari-Jo Campagnone

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

June 22, 2010

MEMORANDUM FOR: T. J. Dwyer, Technical Director

COPIES: Board Members

FROM: D. Campbell

SUBJECT: Review of the Criticality Experiments Facility, Nevada Test Site

The staff of the Defense Nuclear Facilities Safety Board (Board) identified a number of safety issues at the Criticality Experiments Facility (CEF) through a review of the facility's safety basis and instrumentation and control design. Staff members F. Bamdad, D. Campbell, J. Deplitch, D. Minnema, B. Sharpless, and R. Verhaagen held a series of conference calls with personnel from the Nevada Site Office (NSO) and Los Alamos National Laboratory (LANL) during February and March 2010. The staff's subsequent on-site review consisted of discussions with federal and contractor personnel, including representatives of National Security Technologies, LLC (NSTec), and the observation of simulated critical assembly machine operations. The Board's staff followed up on commitments made by the National Nuclear Security Administration (NNSA) in letters to the Board dated June 2, 2006, and December 7, 2006, and assessed the adequacy of the safety basis changes that have occurred since the approval of Critical Decision-3.

Summary. The Board's staff noted that the CEF hazard and accident analysis, considering both facility and experiment conditions, is incomplete, and thus the derived control set may be inadequate. In certain instances, the safety system designs fail to meet the requirements specified in the Documented Safety Analysis (DSA). The severity assessment for some postulated accident scenarios is not based on unmitigated analysis and therefore is not conservative. Organizational support for and oversight of the experiment review process by the management and operating contractor, NSTec, are not adequately robust or technically based. Contributing to this deficiency, NSTec appears to lack the requisite technical capabilities to effectively review and oversee the design and operation of this facility. The Board's staff is also concerned that these issues were not identified by NNSA.

Background. The Technical Area (TA)-18 Mission Relocation project moved four critical assembly machines from the TA-18 facility at LANL to the Device Assembly Facility (DAF) at the Nevada Test Site (NTS). A mission of the facility is to conduct experiments on critical assemblies with fissile material in support of criticality safety, accident simulation and analysis, and weapons and reactor design. The project is scheduled for the federal operational readiness review in July 2010 and Critical Decision-4 approval in September 2010.

The contractor operational readiness review (CORR) was conducted in December 2009 per DOE Order 425.1C, *Start Up and Restart of Nuclear Facilities*. The CORR team noted deficiencies in the areas of safety basis implementation, criticality safety, engineering change control, and maintenance and determined that the project was not ready for startup. However, despite the fact that the CORR resulted in some improvements to procedures, safety management programs, system design descriptions, and other documentation, the Board's staff identified additional issues with the safety basis, as documented in this report. Notably, these issues were similar to those specified in a letter from the Board to the NNSA dated March 27, 2006, and indicate that while NNSA resolved these issues, it appears that inadequate resolution of the underlying root causes led to the additional findings.

Documented Safety Analysis. The *Device Assembly Facility Documented Safety Analysis Addendum for Criticality Experiments Facility Operations* contains significant weaknesses and is not reasonably bounding for criticality experiment operations. Three primary areas of weakness in the safety basis are (1) the accident analysis is inadequate, (2) the derived control set may be inadequate, and (3) all controls that perform safety functions are not properly characterized.

Inadequate Accident Analysis—The Board's staff identified the following examples of unanalyzed conditions and existing errors in the CEF accident analysis. Many of these examples were specifically considered in the TA-18 safety basis. The CEF safety basis, however, provides no justification for eliminating some potential conditions from consideration or for modifying the previous analysis, despite the appropriately conservative precedent set by past operations.

- **Unmitigated Dose Analysis for Godiva**—The design basis event for the accident analysis of the Godiva critical assembly machine is a $1.20 insertion of reactivity above delayed critical. This amount of reactivity is based on the specific administrative control limit of $1.15, with an additional $0.05 that accounts for core cooling. The unmitigated dose analysis is based on this administrative control, which is inconsistent with the methodology recommended by the safe harbor of the Nuclear Safety Management Rule, 10 Code of Federal Regulations (CFR) Part 830. This accident is not bounding, as failure of this administrative control could result in credible reactivity insertions up to or possibly exceeding $1.40.

- **Uncontrolled Reactivity Analysis for Comet, Planet, and Flat-top**—As with Godiva, the accident analyses for Comet, Planet, and Flat-top are based on reactivity limits that are administratively controlled. In each machine, the limit is $0.80 ($0.50 for the plutonium core on Flat-top). The analysis performed to show that this limit is bounding, however, is insufficient. The actual reactivity available to the assembly is not specified in the absence of the administrative control. Controls such as shutdown margin and reactivity insertion rates, for example, had been incorporated at the TA-18 facility to address this issue.

- **Inadequately Established Experimental Envelope**—The safety analysis fails to fully establish the operating envelope for potential future experiments at CEF. The TA-18 safety basis analyzed and controlled a number of conditions that have been omitted at CEF without justification. Analyses and controls at other criticality experiment facilities with capabilities similar to those of CEF—the Sandia Pulsed Reactor, for example—have not been considered. Specifically, the CEF safety analysis does not evaluate controls for experiments involving liquids and stored energy sources. Nor does it consider the reactivity effects of reflecting and moderating materials external to the critical assembly machines or the effects of experiment misalignment and undetected movement during operation. Neutron source requirements have not been established during startup for all configurations. Furthermore, in each of these cases, it is unclear how the lessons learned from past criticality accidents have been incorporated into the control set at CEF.

- **Effects of Fuel Cracking**—The DSA ruled out fuel cracking as an operational issue for the Godiva critical assembly machine, even though fuel cracking had previously occurred on Godiva during prompt-critical operations with temperature rises of 450°C. The statement that "experiences at both LANL and Sandia National Laboratories have shown that, at least initially, these cracks do not pose operational difficulties" is not supported by further technical justification in the accident analysis, and these cracks were inappropriately eliminated from consideration for control or inspection.

- **Reactivity Insertions Greater Than $1.00 for Plutonium Systems**—The CEF DSA states that "mechanical assembly of a [plutonium] system with excess reactivity in excess of $1 is incredible." This statement is not technically supported. Several criticality accidents, most notably two at LANL in 1945 and 1946, have occurred when a plutonium system was assembled to a prompt supercritical state. Both of these LANL accidents resulted in worker deaths. The CEF accident analysis rules out consideration of controls for these types of accidents without justification, a position that is inconsistent with the TA-18 safety basis, which accounted for these types of accidents for critical assembly machines capable of loading plutonium.

- **Ground Acceleration from High Explosive Violent Reaction (HEVR)**—While the critical assembly machines are seismically anchored to meet Performance Category-3 seismic requirements, the justification that this design feature will also protect the critical assembly machines from a HEVR in an adjacent cell is not supported.

Inadequate Control Set—The Board's staff identified the following deficiencies in the existing control set by reviewing a sample of the system design documentation. The presence of such errors indicates that a more detailed design review may be prudent to evaluate similar vulnerabilities in the remaining safety systems.

- **Flat-top Hydraulic Safety System Boundary**—The Flat-top critical assembly machine employs a safety-significant safety shutdown mechanism to move the machine to its least reactive state when a scram is necessary, including a loss of power. The safety shutdown mechanism functions by applying high-pressure hydraulics to two movable rams that position two reflecting quarter spheres (safety blocks) away from the critical assembly. A total loss of hydraulic pressure would prevent the movement of these safety blocks. The system uses redundant hydraulic accumulators that are classified as safety-significant for this function; however, many components within this hydraulic pressure boundary are not safety-significant.

  These non-safety components include check valves, pressure switches, pressure gages, hydraulic valve modules, and system piping. The failure of any of these components to maintain pressure within the boundary would prevent the machine from moving to its least reactive state when necessary, thus defeating the safety function. Additionally, failure of two of these non-safety components, in many different combinations, could prevent the safety blocks from being moved at all. Thus, the safety-significant boundary analysis did not identify all potential failure modes that could degrade the safety function. As a result, the boundary has not been properly controlled.

- **Design of Safety Instrumented Systems**—The LANL *Engineering Standards Manual* (ISD 341-2) specifies the safety instrumented system design requirements for the CEF project. The manual expands on the requirements contained in American National Standards Institute (ANSI)/International Society of Automation (ISA)-84.01-1996, *Application of Safety Instrumented Systems for the Process Industries*, which is the selected national consensus standard for use in designing and operating safety instrumented systems at CEF. Of note, this standard underwent significant revision in 2004 and was reissued as ANSI/ISA-84.00.01-2004 to reflect technological advances and changes in consensus. The system design for CEF does not incorporate these changes. Additionally, as specified below, there are several instances in which the current design fails to meet the requirements of any of these design standards.

  The scram safety system employs three safety-significant instrumented systems to implement the controls required by the DSA. These safety-significant instrumented systems consist of redundant sensors (nuclear instruments, door interlocks, and manual scram buttons) and programmable logic controllers for each cell. Each machine has its own redundant safety shutdown mechanism. The DSA credits the three safety-significant instrumented systems as independent protection layers, each of which provides a specific safety function. Thus each protection layer has been assigned a risk reduction factor and safety integrity level, which indicates the required system reliability. The Board's staff noted that the protection layers all share the same final elements and as such are not independent. This observation is significant

in that the Layer of Protection Analysis calculation credits these systems for their independence.

One safety instrumented function credited in several accident scenarios requires an operator to interpret the audible count rate from safety-significant startup and audible neutron counters and press the manual scram button to shut the system down if the count rate is abnormal. There are several problems with this design approach:

- ANSI/ISA-84.01-1996 states that it does not cover systems for which operator action is the sole means of returning the process to a safe state. Although the LANL *Engineering Standards Manual* does address this application, it does not specify how to credit operator action and is unclear which standard should be used for such a design.

- Operators are modeled as completely independent and the DSA credits the probability of failure on demand of 1E-2 for certain accident scenarios. This is inconsistent with industry standards.

- Operators are provided with audible indications and required to take credited action; the time interval for this action is much longer than the onset of a hazardous condition.

- Nuclear instrument set points, system response times, and operator response times have not been determined, as required by ANSI-ISA-84.01-1996.

- The design documentation does not specify all design inputs, as required by the LANL *Engineering Standards Manual.*

Therefore, due to the deficiencies in the safety instrumented system design, the resultant controls for several reactivity insertion accidents cannot be shown to perform their specified safety function as required by the DSA.

Improper Characterization of Safety-Related Controls—Operators determine the point of delayed criticality and the system excess reactivity for critical assembly machines by performing calculations during the conduct of experiments. System excess reactivity is administratively controlled as a technical safety requirement (TSR). The operators use human-machine interfaces to conduct the experiments remotely, and these interfaces provide data, such as control rod position and neutron population, that directly support the execution of the related TSRs. While excess reactivity limits are credited to mitigate the severity of each postulated reactivity insertion accident, the human-machine interface consoles are not designated as safety-significant. This is inconsistent with the safety function performed by these systems, and evaluation is required to ensure that the credited excess reactivity limits can be implemented as designed.

Inadequate Organizational Support and Technical Capability for Oversight. CEF operations require the implementation of a "user-owner" relationship. NSTec is the facility owner and is responsible for defining, implementing, and enforcing the facility safety envelope. LANL is the facility user and is responsible for operating the critical assembly machines and executing each experiment within the safety envelope established by NSTec. NSTec reviews and approves all experiment plans and system design changes through the change control and unreviewed safety question determination processes.

The NSTec nuclear safety organization's technical duties are performed and supported exclusively by Omicron Safety and Risk Technologies, Inc. The NSTec Facility Operations Review Committee (FORC) reviews each proposed experiment plan and recommends approval to DAF management. The FORC review is the only TSR-level control credited in the experiment review process. According to NSTec, however, the function of the FORC is to ensure that LANL has followed its internal review process. Neither Omicron nor the FORC employs technical experts with experience in the field of criticality experiments.

LANL's internal experiment review process requires that the Criticality Experiments Safety Committee conduct an independent and objective safety review of each proposed experiment plan. This committee makes recommendations to LANL line management regarding all experiments and system design changes, and conducts annual appraisals of criticality experiment operations at NTS. Although NSTec relies on the LANL review process, it is not a credited TSR-level control.

While it is important to the operational safety of the facility that the user, LANL, retain highly qualified specialty technical experts for its operations, it is also essential that the facility management and operating contractor, NSTec, be able to understand, review, and provide safety oversight of those activities. NSTec needs to have the organizational and technical capability to establish and implement the facility safety envelope independently of the recommendations of LANL line management.

During this review, the Board's staff also observed a number of simulated operations on the Godiva and Flat-top machines and noted several deficiencies in the area of conduct of operations and instrumentation. During simulated material movement, the operators violated a criticality safety requirement while transferring the Flat-top core into the cell. In addition, instrumentation problems precluded satisfactory completion of a simulated operation on Godiva. In each case, the management and operating contractor representatives involved in the simulated operation lacked familiarity with the criticality experiments and failed to provide adequate oversight of the operation.

Conclusion. The responsibility for safe operation of CEF lies with the facility manager, under oversight by NNSA. NSTec, however, is completely reliant upon the design and experiment reviews conducted by LANL, the facility user. The Board's staff identified multiple issues adversely impacting the safety basis that NSTec and LANL should have been identified previously. NSTec has not demonstrated that its nuclear safety organization possesses the necessary skill set to review, analyze, and oversee the complex operations that will occur at CEF.

In similar situations in which highly experienced technical support is needed to conduct new operational activities, safety organizations have formed independent oversight committees to supplement the contractor's safety organization. Examples include the Nuclear Explosive Safety Study Group at the Pantex Plant and the Advisory Committee on Reactor Safeguards at the Nuclear Regulatory Commission. The Board's staff believes that the lack of such expertise at NSTec, compounded by the complexity of highly technical issues that may arise during the performance of future criticality experiments at CEF, warrant consideration of an oversight committee that is both supportive of the contractor and independent of the LANL oversight process. This committee needs to possess technical expertise in criticality experiments and an in-depth knowledge of the physics of critical assemblies and potential upset conditions for the machines. It would be able to evaluate whether existing safety controls are adequate and make appropriate recommendations to NNSA or NSTec to ensure that safe operations commence and continue for the life of the facility.