Department of Energy
National Nuclear Security Administration
Washington, DC 20585
February 10, 2011

The Honorable Peter S. Winokur
Chairman
Defense Nuclear Facilities Safety Board
625 Indiana Avenue, N.W., Suite 700
Washington, D.C. 20004

Dear Mr. Chairman:

This is in response to your August 5, 2010, letter including a Staff Issues Report on a review of the Criticality Experiments Facility (CEF) at the Nevada National Security Site. Your letter requested that two reports and briefings be provided to the Board. The National Security Technologies (NSTec), Los Alamos National Laboratory (LANL), and Nevada Site Office (NSO) have evaluated the issues identified by your staff.

The attached report and matrix is being submitted in response to the Board's concerns on CEF. The specific actions, schedule, and responsible organization for each of the issues identified in the staff report are included in the matrix. The responses to the last two issues in the staff report also provide the responses to the second report requested by the Board. Therefore, this attached report is being submitted to fulfill both requested reports. The briefings are scheduled to be provided to the Board during their visit to NSO the week of February 15.

A number of the findings from the CEF Operational Readiness Review (ORR) are directly and indirectly related to the issues identified in the staff report. Since August 1, 2010, NSTec, LANL, and NSO have aggressively been working to develop Corrective Action Plans (CAPs) for the ORR findings and implement the necessary actions to close out the pre-start findings. All pre-start CAPs have been approved and closure of the findings is expected to be completed by the middle of February 2011. All post start CAPs are expected to be approved by the end of February 2011.

The National Nuclear Security Administration is committed to the safe startup and operation of CEF. If you have any questions, please contact me or have your staff contact Dr. Jerry McKamy at (301) 903-7980.

Sincerely,

Donald L. Cook
Deputy Administrator
for Defense Programs

Attachment

cc: w/attachment
T. D'Agostino, NA-1
M. Campagnone, HS-1.1
S. Mellington, NSO

RESPONSE TO DEFENSE NUCLEAR FACILITIES SAFETY BOARD ISSUES CONCERNING DEFICIENCIES IN THE ACCIDENT ANALYSIS, CONTROL SET, AND SAFETY DESIGN AT THE CRITICALITY EXPERIMENTS FACILITY

January 2011

Background

The Defense Nuclear Facilities Safety Board (DNFSB) sent the National Nuclear Security Administration (NNSA) a letter on August 5, 2010 based on a DNFSB staff issue report on review of the Criticality Experiments Facility (CEF). The DNFSB staff evaluated the CEF safety basis and instrumentation and control design. The DNFSB staff review also included observing simulated critical assembly machine operations. The DNFSB identified concerns with the Documented Safety Analysis (DSA) and Inadequate Organizational Support and Technical Capability for Oversight. With respect to the DSA, the DNFSB staff identified three areas of weakness in the safety basis: (1) inadequate accident analysis, (2) inadequate control set, and (3) improper characterization of safety-related controls.

CEF Status and Path Forward

The NNSA Operational Readiness Review (ORR) for CEF was completed on July 29, 2010. The results of the ORR were briefed to the DNFSB on August 12, 2010. A number of the findings from the ORR are directly and indirectly related to the issues identified in the DNFSB staff report. Since August 1, 2010, the Nevada Site Office, National Security Technologies, LLC (NSTec), and Los Alamos National Laboratory (LANL) have aggressively been working to develop corrective action plans (CAPs) for the ORR findings and implement the necessary actions to close out the prestart findings. All prestart CAPs have been approved and closure of the findings is expected to be completed by the middle of February 2011. All post start CAPs are expected to be approved by the end of February 2011. Nevada Site Office is expecting to request authorization to start operations from the Deputy Administrator for Defense Programs by March 15, 2011.

A response and path forward for each of the DNFSB staff issues have been developed by Nevada Site Office, NSTec, and LANL and are provided on the attached matrix. The specific actions, schedule, and responsible organizations are included in the matrix. The following provides a summary response to the DNFSB staff issues.

<u>CEF Documented Safety Analysis</u>

The CEF DSA was developed specifically for CEF operations in the Device Assembly Facility (DAF). The results of hazard/accident analysis presented in the DAF DSA and the TA-18 Basis for Interim Operations were utilized as appropriate in the development of the CEF DSA. As the TA-18 facilities in Los Alamos, New Mexico, and the DAF at the Nevada National Security Site

(NNSS) are two different facilities in two distinctly different locations, the safety basis for CEF operations at both facilities would not be expected to be the same.

Inadequate Accident Analysis – Nevada Site Office and NSTec have determined that enhancements to the CEF DSA are needed to address the specific DNFSB staff issues. NSTec will make the appropriate changes to the DSA and submit to Nevada Site Office for approval. At this time, these changes are not expected to result in any additional controls. Should this change, NSTec will follow the appropriate procedures in accordance with 10 Code of Federal Regulations (CFR) Part 830.

Inadequate Control Set – NSTec declared a potential inadequacy in the safety analysis and issued a positive unreviewed safety question determination on the Flat-Top Safe Shutdown System hydraulic pressure boundary. In addition, NSTec instituted a timely order to not allow Flat-top operations to proceed until the issues surrounding the functional classification are resolved. LANL is implementing actions to address this issue. LANL will conduct a review of the design to determine if the project followed the appropriate design standards. Should any discrepancies be identified, these will be presented to Nevada Site Office and a path forward developed. In addition, LANL will re-evaluate the layer of protection analysis and safety integrity level determination and correct any issues that may exist.

Improper Characterization of Safety-Related Controls – LANL has developed an approach to address the specific issue in the DNFSB staff report. The approach will be incorporated into the operating procedures. The CEF ORR also identified a similar issue in a surveillance procedure associated with the human machine interface. This procedure is being modified in accordance with the CAP for the ORR finding.

Inadequate Organizational Support and Technical Capability for Oversight

In 1999, Nevada Site Office established the Real Estate/Operations Permit (REOP) Order. The REOP process was established to effectively coordinate the activities of multiple prime contractors and the National Laboratories and defines the approach to establishing line management responsibility for safety. The REOP process establishes a user-owner relationship, which outlines the general roles and responsibilities of each organization and the requirements for approval of work. Since the establishment of the REOP Order, the Nevada Site Office contractors and the National Laboratories have safely and effectively performed multiple nuclear and high hazard operations under this process. The specific Roles, Responsibilities, Authorities, and Accountabilities for NSTec and LANL at the DAF and CEF are defined within the respective organizations' plans and procedures included in the authorization basis documentation for the respective REOPs.

Nevada Site Office fully understands the concerns with respect to the experiment review process. As a result, the LANL Criticality Experiments Safety Committee will include a representative from NSTec who is fully knowledgeable in the DAF and CEF DSAs and Technical Safety Requirements. In addition, the NSTec Facility Operations Review Committee will include both a representative from the LANL Criticality Experiments Safety Committee and the NSTec representative to the committee.

Nevada Site Office and the CEF ORRs identified issues in the area of conduct of operations. As a result, senior management from both NSTec and LANL have committed to improving and maintaining a high degree of formality while conducting nuclear operations at the NNSS.

Conclusion

The implementation of the actions identified to address the ORR findings and the DNFSB staff issues will ensure that CEF can startup and operate safely. In addition, the lessons learned on CEF are being utilized to improve nuclear operations at the NNSS. Nevada Site Office, NSTec, and LANL are committed to the safe startup and operation of CEF. The following matrix identifies the responsible parties and timelines to complete the specific tasks related to implementing the corrective actions summarized above.

Response to Defense Nuclear Facilities Safety Board (DNFSB) Issues Related to Criticality Experiments Facility (CEF)

DNFSB Issue	Path Forward	Responsible Organization
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 based upon the specific administrative control limit of $1.15 with an additional $0.05 that accounts for core cooling. The unmitigated dose analysis is based upon this administrative control, which is inconsistent with the methodology recommended by the safe harbor of the Nuclear Safety Management rule, Title 10 Code of Federal Regulations, 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	The Specific Administrative Control (SAC) that limits the maximum excess reactivity inserted for burst operations $1.15 in order to prevent subsequent release of airborne radiological material at risk was perceived to be consistent with the safe harbor methodologies of the Nuclear Safety Management rule for establishing initial conditions for the accident analysis. A superprompt burst accident on Godiva involving $1.20 reactivity insertion was deemed to be the bounding reactivity insertion accident. It was understood, by the knowledgeable team preparing the Documented Safety Analysis (DSA) that insertions above $1.15 rapidly decrease in likelihood, ultimately becoming impossible for all practical intent as stray neutron pre-initiation of the sequence at reactivity insertion levels higher than $1.15 becomes inevitable. In particular, the intrinsic neutron density of a plutonium sample in the glory hole, the primary release source of concern, would ensure such pre-initiation. The chosen bounding accident was determined to result in the melting of plutonium and was qualitatively assigned a consequence category "B" range for the public. This consequence for the design basis accident is conservative because the maximum possible consequence of entire Godiva plutonium sample vaporizing for the $1.40 beyond design basis accident would also result in a consequence category "B" range for the public. The postulated dose to the public would be less than 1 rem for this beyond design basis accident and is less than the 25 rem Total Effective Dose Equivalent (TEDE) to the maximally exposed off-site individual (MOI) dictating the application of safety class controls. Moreover, the use of this worst case bounding consequence (i.e., vaporization of entire plutonium sample) ensures that the appropriate defense in depth controls are selected to effectively mitigate the risk of this bounding accident to acceptable levels. Therefore, the DSA preparation team believed the analysis was appropriately bounding and that the unmitigated consequences were	NSTec

DNFSB Issue	Path Forward	Responsible Organization
	conservative because of the use of consequences associated with the full vaporization of plutonium and the understood physical limitations of achieving maximum excess reactivity in excess of $1.15. The maximum excess reactivity inserted for burst operations $1.15 is chosen as the design basis accident because it has been shown by analysis that this maximum excess reactivity corresponds to the onset of Plutonium melting. The accident analysis for this design basis accident resulted in the predicted dose consequence to the MOI as a TEDE of .02 rem. This predicted dose consequence would normally correspond to a public risk consequence category designation of "C" that represents radioactive material dispersal with potential for doses <0.1 rem. However, the process hazards analysis for this design basis accident conservatively assumed an unmitigated public risk consequence category designation of "B" that represents radioactive material dispersal with potential for doses between 0.1 and 25 rem. A Beyond Design Basis (BDB) event was done for a postulated accident involving an excess reactivity insertion of $1.40 on the Godiva critical assembly. Godiva is administratively controlled to have a maximum excess reactivity loading of $1.40 and a maximum reactivity insertion of $1.15 above delayed critical. As indicated in DOE-STD-3009, the Nuclear Safety Management Rule requires consideration of the need for analysis of accidents, which may be beyond the design basis of the facility to provide a perspective of the residual risk associated with the operation of the facility. As shown in supporting analyses, at a $1.40 insertion all of a Godiva plutonium sample and a small fraction of the Godiva highly enriched uranium core could vaporize. The postulated dose to the public would be less than 1 rem and continue to correspond to a public risk consequence category designation of "B" with the entire plutonium sample vaporizing.	

DNFSB Issue	Path Forward	Responsible Organization
	As indicated above, the design basis and beyond design basis accidents selected for Godiva excess reactivity excursions represent the range of fuel consequences from melting to vaporizing. The public consequences used in control selection for this range of phenomena associated fuel condition remains the same as a public risk consequence category designation of "B." Thus, a design basis accident perceived to be more bounding would have no impact on the unmitigated bounding consequence used in the process hazards of analysis used to determine the preventive and mitigative controls to attain acceptable risk. However, to provide enhanced clarity the design basis accident will be revised to provide the bounding release (i.e., vaporization of entire Plutonium sample) that could occur regardless of reactivity insertion. This revision will eliminate the Godiva excess reactivity insertion limit of $1.15 for burst operations as an initial condition. Instead, this limit will be applied as a control, as appropriate, in mitigating an excess reactivity accident to protect the Critical Assembly Machine (CAM) from this level of unplanned reactivity excursion. These changes will be pursued in accordance with the established action plan to address an Operational Readiness Review (ORR) finding, since this conservatism was already applied in the process hazards analysis evaluating this accident. **Submit DSA changes to Nevada Site Office – June 1, 2011**	

Uncontrolled reactivity analysis for Comet, Planet, and Flat-Top. Similar to 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 to show that this limit is bounding, however, is not sufficient. 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 concern.	Similar to the discussion on Godiva, the maximum excess reactivity limit for the other machines was considered as an initial condition and preserved as a Limiting Condition for Operation (LCO). The bounding consequence analysis for the maximum excessive reactivity excursion design basis accident for these CAMs used the Flat-Top maximum excessive reactivity limit of \$0.50 for experiments using the plutonium core. The limit was chosen because plutonium bounds the consequences of Comet and Planet (separate analysis in Appendix B of the DSA shows melting does not occur for these CAMs). A conservative analysis presented in the DSA indicates that ~ 40 percent of the plutonium may melt following an unmitigated \$0.50 reactivity insertion. The computer codes supporting this analysis used the prompt-jump approximation to estimate onset of melting even though actual experiments performed in 1978 and documented, the recorded temperature from a repeated step-reactivity insertion of \$0.80 with plutonium, was less than 30°C. Like Godiva, the application of the design basis accident to the process hazards analysis was done conservatively by using a public consequence category of "B" vice the actual consequences calculated for the postulated design basis accident. This public consequence category also corresponds to the beyond design basis event of a \$0.80 that represents full melting of the plutonium. Since the higher consequence category is applied as, the unmitigated consequence to the process hazards analysis, it results in the same identified controls to attain acceptable risk levels. The calculated predicted dose of the design basis accident, consequence to the MOI as a TEDE, was calculated as .02 rem that corresponds to a public risk consequence category designation of "C." This consequence was calculated with conservatisms, such as a damage ratio and leak path factor of unity. However, the Flat-Top process hazards analysis for this design basis accident conservatively assumed an unmitigated public risk consequence category designation of "B" as the starting point for control selection to reach acceptable	NSTec

	risk through the application of defense in depth controls. Also, the DSA presents a Flat-Top BDB event for a $0.80 reactivity insertion for experiments using plutonium that results in a dose to the public that would be less than 1 rem with full melting. This limiting consequence results in also a risk consequence category designation of "B" and hence does not alter the control selection to attain the desired mitigated risk. Consistent with the resolution approach for the excess reactivity limit for Godiva, the design basis accident for the other CAMs will be revised to provide the bounding release (e.g., full melting of Plutonium sample) that could occur regardless of reactivity insertion. This revision will eliminate as an initial condition and instead applies this limit as a control, as appropriate, in mitigating an excess reactivity accident to protect the CAMs from this level of unplanned reactivity excursion. These changes will be pursued in accordance with the established action plan to address an ORR finding, since this conservatism was already applied in the process hazards analysis evaluating this design basis accident. **Submit DSA changes to Nevada Site Office – June 1, 2011**	
Inadequately established experimental envelope. The safety analysis does not fully establish the operating envelope for potential future experiments at CEF. The TA-18 safety basis analyzed and controlled a number of conditions, which have been omitted at CEF without justification. Analysis and controls at other criticality experiment facilities with similar capabilities to CEF, the Sandia Pulsed Reactor for example, have not been considered. Specifically, the CEF safety analysis does not evaluate controls for experiments containing liquids and stored energy sources. Nor does it consider the reactivity effects of reflecting and moderating materials external to the critical assembly machines	The approved DSA that has been prepared to the DOE-STD-3009 safe harbor methodology provides a process description or scope of work, and completes hazard identification and evaluation along with required accident analyses to identify the spectrum for defense in depth controls to effectively mitigate the risk to the public, workers, and environment to allow work to be performed safely and appropriately authorized by the approval authority. DSA Section 3.3.2.1.7 discusses relevant operating experience addressed by the due diligence consideration of: (1) Occurrence Reporting Processing System reports, (2) the 1998 TA-18 Stand Down, (3) TA-18 Unreviewed Safety Question (USQ) data base, and (4) Criticality Accidents at Los Alamos National Laboratory (LANL) and World-Wide. The analyzed forms of the experimental materials are based on the as-described processes within the DSA. Changes to the CEF procedures, facilities, and other special	NSTec/LANL

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	tests to accommodate new experiments will be evaluated through the approved USQ process, with revisions to the hazards/accident analysis and supporting controls, as appropriate. All experiments will be conducted in accordance with an approved experiment plan, which has been evaluated by the Criticality Experiments Safety Committee, the Facility Operations Review Committee (FORC), and the approved USQ process. The process hazards analysis does provide an evaluation supporting control selection for moderator, reflector, misalignment, and incorrect material loading types of events, and derives controls to address these types of initiators to accidents. The use of neutron sources are provided as part of approach to criticality considerations with supporting controls of when sources are used to support safely controlled evolutions.	
Effects of fuel cracking. The documented safety analysis ruled out fuel cracking as an operational concern on the Godiva critical assembly machine, despite the fact that fuel cracking 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 any further technical justification in the accident analysis and is inappropriately eliminated from consideration for control or inspection.	The indicated quote is completed in Section 2.5.4.7, Thermal, and Nuclear Characteristics of Godiva in the DSA with the following sentences "…In the initial stages, this cracking is difficult to identify, and the prompt-burst assemblies at both laboratories may be operating with some cracking in the fuel plates. Cracks were found to have decreased the overall reactivity of the assembly. Therefore, it is concluded that the cracks do not present an operational or safety issue." The complete citation in summary indicates that cracks have not caused operational difficulties and they have been found to decrease the overall reactivity of the assembly rather than present an increased reactivity concern. However, the reference to cracking raises other potential concerns if new information from the present operating experience is found (e.g., through operational events) that indicates cracking has become significantly further degraded with resulting effects that have not been experienced to date (e.g., Safety Shutdown Mechanism obstruction caused by cracking). Godiva design and operations are compliant to American National Standards Institute/American Nuclear Society (ANSI/ANS) ANSI/ANS-14.1-2004, *Operation of Fast Pulse Reactors*. Requirements from this standard include provisions for at least two independent safety devices (such as safety block and control elements) that shall be capable of shutting down the reactor under the most	NSTec

	reactive experimental arrangement to be modified and requirements for the reproducibility of experimental data. The safety function of the SCRAM Safety System (SSS) and Safety Shutdown Mechanism (SSM) to SCRAM the critical assembly (rapidly move the critical assembly to a subcritical level) when indicated to do so by the state of the sensors or by a loss of power, demonstrates that Section 5.2 of ANSI/ANS-14.1-2004 is met. The associated daily and annual surveillance tests for these independent systems involve movement of the safety block and control rods that provide associated confidence relative to unobstructed movement of the safety devices. The reproducibility requirement ensures that measured core conditions match expected core conditions as part of deliberate standard based critical operations. It is anticipated that reduced reactivity caused by fuel cracking would be identified by these activities. Attachment A, Section A.1.5 of DOE G 424.1-1A, "Implementation Guide for Use in Addressing Unreviewed Safety Question Requirements," indicates "certain accidents or malfunctions are not treated in the nuclear facility's existing safety analyses because their effects are bounded by similar events with the same control set that are analyzed." The surveillance testing of the SSS and SSM required by Technical Safety Requirement (TSR) Surveillance Requirement (SR) 4.8.2 upon startup of a CAM, that involves the physical movement of the safety block and control rods, provide assurance and associated controls to identify issues with obstructed movement, even though these controls were not derived for that specific purpose. If an operational event is discovered by this testing that identifies an issue with movement, a Potential Inadequacy in the Documented Safety Analysis (PISA) would be declared, compensatory measures defined to assure safety and an USQ determination initiated. As an enhancement to the DSA, the hazard identification and evaluation will be expanded to include fuel cracking concerns causing potential	

	obstructions to safety block and control rod travel as part of planned changes to address ORR findings. **Submit DSA changes to Nevada Site Office – June 1, 2011**	
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 $1.00 is incredible." This is not technically supported. Several criticality accidents, most notably two at LANL in 1945 and 1946, have occurred where a plutonium system was assembled to a prompt supercritical state. Both of the LANL accidents resulted in worker deaths. The CEF accident analysis rules out the consideration for controls in these particular types of accidents without justification. This is also inconsistent with the TA-18 safety basis, which accounted for these types of accidents for critical assembly machines capable of loading plutonium.	The quote as provided in the Section 3.3.2.4, Hazard Evaluation section of the DSA for Reactivity-Insertion Accidents indicates that since "…plutonium has an intrinsic neutron source from spontaneous fission of ^{240}Pu that generates on the order of 10^4 neutrons/s-kg, mechanical assembly of a system with excess reactivity in excess of $1.00 is incredible." Although this statement based on the intrinsic nature of plutonium radionuclide neutron sources can be scrutinized based on past experience, the impact of this statement on the completed CEF hazards and accident analysis is negligible. This is because the CEF safety analyses for reactivity insertion does consider plutonium as a fuel type and the unmitigated frequency estimates for scenarios analyzed for reactivity insertions are independent of fuel type (human errors leading to reactivity insertion that are not discriminated by fuel type). Also, the bounding consequences for bounding CAM reactivity insertion accidents are conservatively based on plutonium because of the inherently higher dispersion consequence of this material opposed to other nuclear materials. Thus, both the frequencies and consequences supporting the process hazards analysis are not impacted by this statement. Therefore, the defense in depth controls identified to mitigate the risk of these scenarios to acceptable levels is unchanged by the statement. As an enhancement to the DSA, this statement will be deleted since plutonium reactivity accidents of this magnitude are part of the hazard and accident analysis. **Submit DSA changes to Nevada Site Office – June 1, 2011**	NSTec

Ground acceleration from High Explosive Violent Reaction. 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 high explosive violent reaction in an adjacent cell is not supported.	The CEF DSA currently provides an Inhabited Building Distance Level of protection to CEF workers based on DoD 6055.9 to overpressure of 1.2 psi. This is more conservative than the Class II level of protection provided to DAF workers and is an Explosive Safety consideration for determining the proximity of non-explosive activities near explosive operations to ensure no impact on adjacent facilities/activities. Acceptor mode level of explosives safety protection is afforded to CEF workers at this higher standard for the explosive operations that may be occurring elsewhere in DAF. Consistent with the established key elements of the Explosive Safety Management Program of the DAF TSRs, acceptor mode protection is provided by a combination of Design Features (DFs), LCOs, and SACs. For the DAF DSA Addendum for CEF operations and associated TSRs, acceptor mode protection is implemented through the LCOs for Special Door Interlocks (i.e., LCO 3.2.1 and LCO 3.2.2), and DFs for the Building Structures (DF 6.2.1 for blast design) and Special Doors (DF 6.2.3). SACs that comprise the DAF DSA and TSRs ensure at least one Special Door is closed in CEF buildings during High Explosive (HE) operations occurring in DAF buildings, and at least two Special Doors are closed in CEF buildings during DAF HE corridor movements, where applicable, or material is placed in an approved container with personnel evacuated where donor mode cannot be assured. These controls preserve the desired level of protection to CEF workers from a consequence perspective in a manner compliant with the application of standards based approach for collocated workers not associated with explosive operations. Further, the application of these controls reduce the uncontrolled frequency of an explosion from 2.75 E-3 (frequency ID bin "II"; $10^{-2} - 10^{-4}$ per year) in Cells and Bays (frequency is less in the corridor) to a controlled frequency that is beyond extremely unlikely (frequency ID bin of "IV," $< 10^{-6}$ per year) high explosive configurations. Currently, the CEF DSA indicates in the functional requirement for the Seismic Anchoring of Critical Assemblies engineered control that the capability of the critical assemblies to maintain stability and	NSTec

	position during a seismic event bounds explosive operations occurring in DAF (Table 4-13). This text will be deleted from the DSA and the Beyond Design Basis Accident (BDBA) section of the CEF DSA (Section 3.4.3) will be expanded to include a discussion of a BDBA for the impact of a nearby explosion occurring in DAF on CEF activities. Currently, Section 3.4.3 of the CEF DSA includes BDBAs for Godiva toppling and a greater than a performance Criterion 3 earthquake. These existing BDBAs provide an understanding of the residual risk associated with the operation of CEF consistent with a nearby explosion in DAF. This enhancement to the CEF DSA will be completed in accordance with the established action plan to address an ORR finding. **Submit DSA changes to Nevada Site Office – June 1, 2011**	
Flat-Top hydraulic safety system boundary. The Flat-Top critical assembly machine employs a safety significant SCRAM Shutdown System (SSS) to move the machine to its least reactive state when a SCRAM is necessary, including a loss of power. The SSS functions by applying high pressure hydraulics to two moveable 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 safety significant for this function; however, there are many components within this hydraulic pressure boundary that 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	The DNFSB trip report asserts that the boundary analysis that was used to designate which components of the Flat-Top hydraulic pressure boundary should be safety significant is in error and that there are certain valves, gages and pressure switches which are currently categorized as general service should in fact be safety significant. NSTec has declared a PISA for this issue, issued a positive USQ Determination, and instituted a timely order to not allow Flat-Top operations to proceed until the issues surrounding the functional classification are resolved. A hold point in the CEF Startup Plan has also been imposed to require resolution of this issue prior to loading fuel on Flat-Top. An Evaluation of Safety of the Situation will be performed prior to removing the established compensatory measures based on the results of the functional classification review. The following actions are being pursued to resolve functional classification boundary concerns. 1. Review the codes and standards that were used to define the overall process for performing the boundary analysis initially and verify (or not) the adequacy of the process used. **(Action Completed)** 2. Review the Failure Modes and Effects Analysis and the Flat-Top boundary analysis. **(Complete action – April 29, 2011)**	LANL

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. This reveals that 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.	3. Using one and two above, re-affirm (or not) the adequacy of the existing design as it is described in the approved CEF DSA. **(Complete action – April 29, 2011)** 4. If the adequacy of the existing design is re-affirmed, brief Nevada Site Office and await any further direction. **(This action is contingent on Item 3 results)** 5. If the existing design is determined to be inadequate, then initiate an activity to upgrade the affected Flat-Top hydraulic components. **(This action is contingent on Item 3 results. If the design is inadequate, a schedule to upgrade the hydraulic boundary will be developed by May 13, 2011)**	
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 amplifies the requirements provided in ANSI/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, there are several instances where the current design does not meet the requirements of any of these design standards	The report observations and comments assert that there are "several instances" where the current design does not meet the requirements of the LANL *Engineering Standards Manual* (ISD 341-2) and ANSI/ISA-84.01-1996. The observations and comments also assert that ANSI/ISA-84.01 went through a substantial upgrade in 2004 and that the CEF design did not incorporate these changes. Our path forward for addressing this comment is as follows. 1. Research the project commitments with regard to the applicable standards. At present, we know that ISD 341-2 and ANSI/ISA-84.01-2004 did not exist during the design phase of the project. Clearly, ANSI/ISA-84.01-1996 did exist during the design phase of the project. **(Complete action – April 29, 2011)** 2. Re-affirm (or not) that the project followed the appropriate set of standards during the design phase. **(Complete action – April 29, 2011)** 3. If it is concluded that the project did not follow the appropriate set of standards, then initiate discussions with Nevada Site Office with regard to evaluating the adequacy of the design process as it was used. **(This action is contingent on Item 2 results. If the appropriate set of standards was not followed, a schedule to evaluate the adequacy of the design process will be developed by May 27, 2011)**	LANL

The CEF project employs safety significant instrumented systems to achieve the controls required by the documented safety analysis. Three independent protection layers, which form the machine SCRAM systems, have been assigned a required risk reduction factor and safety integrity level, which indicate the desired system reliability. These protection layers are assigned as safety instrumented functions that work in concert to ensure the controls specified in the DSA are achieved. The Board's staff noted that the protection layers all share the same final elements and as such are not independent. This is significant in that the Layer of Protection Analysis calculation credits these systems for their independence.	The report observations and comments assert that the three layers of protection that form the machine SCRAM systems all share the same final element and are therefore not independent. This assertion is significant because the Layer of Protection Analysis (LOPA) credits these systems for their independence. In a follow-on teleconference with the Board staff, it was stated that the issue may not be a common final element issue, but rather the issue may be with CEF-ENG-CAL-0465, LOPA Analysis for Safety Integrity Level (SIL) Determination of the SCRAM System; Hazard ID REA-20. Our path forward for addressing this comment is as follows. 1. Analyze the CEF Layer of Protection Analysis and determine if the protection layers are independent or not. **(Complete action – April 29, 2011)** 2. If there is an issue with respect to independence, revise the analysis to address this issue. **(Complete action – May 31, 2011)** 3. Evaluate any modifications to the LOPA with respect to impact on the required SIL and CEF SIL calculation. **(Complete action – June 17, 2011)** 4. Provide report to Nevada Site Office with results of LOPA actions and any impact to the CEF SIS design. **(Complete action – June 30, 2011)**	LANL
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 shutdown the system if the count rate is abnormal. There are several problems with the design approach.	The manual SCRAM is credited as a dual action/control with the audible startup counters for three Godiva reactivity insertion accidents and one Flat-Top reactivity insertion accident. Two of the Godiva reactivity accident scenarios pertain to postulated accidents in local operations where safety block/control rods are inserted, while control rod/safety block checks are being performed. The other two postulated scenarios for Godiva and Flat-Top involve leaving a worker in the building during the transition from the pre-operational state to remote operations. In all of these scenarios, the manual SCRAM and audible startup counters are credited along with other controls for providing a one bin frequency reduction.	NSTec

	While the audible neutron counter is part of a credited safety significant system, an appropriate control regarding the operator response is not well linked to the instrument indication. Further review of this concern indicates that a time-sensitive SAC was not written for the required operator response based on an understanding that operator training and expertise on ANS-1 ensured appropriate operator response to abnormal audible startup counter readings. Established human reliability analysis methodologies allow for human response actions to prevent or mitigate an accident sequence. Taking into account the two-person rule, it is reasonable to expect one of the operators to initiate manual SCRAM. Unlike a handstacking scenario where the criticality may have already occurred, for the local operation based scenarios there may be adequate time to interrupt the accident progression with the operator initiated manual SCRAM. However, the use of this credited control will be reexamined as part of the established action plan to address an ORR finding, to develop a control with the necessary timing to achieve the level of expected mitigation, or to remove the control with the presentation of an alternate strategy for attaining the desired risk mitigation for these defined accident scenarios. TSR implementation procedures will be revised to reflect the time sensitivity for completing the required actions. This enhancement to the CEF DSA will be completed in accordance with the established action plan to address an ORR finding. Note: The CEF DSA uses the human error probabilities in NUREG/CR-1278, adjusted for DAF experience, and judgment on the typical number of activities per operation per year for significant human actions. A reduction factor of 0.1 is assigned to these types of actions based on this standard. The practice of using NUREG/CR-1278 for the assignment of human error has been a common practice in both the commercial nuclear industry and the Department of Energy; however, the defensibility of this reduction factor will be reexamined recognizing the time sensitivity of completing the required actions.	

	Submit DSA changes to Nevada Site Office – June 1, 2011	
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 TSR. The operators use human machine interfaces to remotely conduct the experiments and these interfaces provide data, including control rod position and neutron population, for example, that directly supports 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 requires evaluation to ensure that the credited excess reactivity limits can be implemented as designed.	The DNFSB trip report asserts that the human machine interface consoles should be safety significant as they are used to collect and display data that is used to execute daily and annual TSR surveillances related to excess reactivity. Our path forward for addressing this comment is as follows. We have agreed to use a combination of Startup Instrumentation and Log-N instrumentation to address this issue. The following describes the approach that will be used. Period measurements will be made using the Startup Instrumentation in concert with the Labview based Startup/Channel Program. This measurement will be confirmed by a period measurement using the Log-N Instrumentation. Period measurements using the Log-Ns will proceed as follows: 1. Establish a stable period in accordance with the applicable SOP. 2. Using a calibrated stopwatch and the Log-N meter, measure the doubling time. a. Measure the time it takes for the Log-N indicated power to increase by a factor of 2. b. The reactor period is calculated via the following relation: $\tau = \frac{T}{\ln 2}$ Where τ is the reactor period and T is the doubling time. Given the period, reactivity is easily determined from the In-Hour Equation with parameters appropriate for the assembly. The Startup Instrumentation consists of ML-2 (SS-SSC) equipment from the detector to the local counters. The cabling from the experiment building to the control room is general service. The Instrumentation and LabView based Startup Channel Program are also	LANL

	general service. This lack of pedigree commensurate with the safety significance of the measured parameter (excess reactivity) has come into question. The measured parameter is the rate of change of assembly power, which may be measured from the neutron leakage. Thus, this is a difference measurement. One can envision only a finite set of system failures: 1. The system reads high. 2. The system reads low. 3. The system reads nothing. 4. The system reads intermittently. The consequences of these failures do not compromise the quality of the measured parameter. Failure 1 results in a difference between two readings that are both biased high. The resultant slope is the same as with no failure. Failure 2 results in a difference between two readings that are both biased low. The resultant slope is the same as with no failure. Failure 3 results in no measurement. Failure 4 results in a nonlinear reading from which a measurement cannot be made. Therefore, excess reactivity measurements may be made with the Startup Instrumentation in support of TSR SRs. These measurements will be confirmed by a measurement on the Log-Ns as described above. The implementation of this alternative period measurement will require the procurement of a calibrated stopwatch, the modification of procedures, and operator training/dry-runs. **(A schedule for these actions will be developed by March 31, 2011)**	

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 to define, implement, and enforce the facility safety envelope. LANL is the facility user and is responsible to operate the critical assembly machines and execute 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 technical duties are performed and supported exclusively by Omicron Safety and Risk Technologies, Inc. The NSTec FORC reviews and recommends approval of each proposed experiment plan to DAF management. The FORC review is the only TSR-level control credited in the experiment review process. However, according to NSTec, the function of the FORC is to ensure that LANL has followed its internal review process. Neither Omicron nor the FORC employ technical experts who have experience in the field of criticality experiments. The LANL internal experiment review process requires the Criticality Experiments Safety Committee to 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	In 1999, Nevada Site Office established the Real Estate/Operations Permit (REOP) Order (currently NSO O 412.X1E). The objective of this order is to ensure that work performed on the Nevada National Security Site (NNSS) or offsite, under the control of Nevada Site Office, is well defined; has well defined geographical boundaries; has identified the hazards; has established and implemented controls to mitigate those hazards; is properly authorized; and is effectively managed. The REOP process was established to effectively manage Nevada Site Office assets and operations and defines the review and approval of all work and the approach to establishing line management responsibility for safety. To effectively coordinate the activities of multiple prime contractors and the National Laboratories, the REOP process establishes a user-owner relationship (Primary and Secondary REOP Holder), which outlines the general roles and responsibilities of each organization and the requirements for approval of work. Since the establishment of the REOP Order, the Nevada Site Office contractors and the National Laboratories have safely and effectively performed multiple nuclear and high hazard operations under this process. The specific Roles, Responsibilities, Authorities, and Accountabilities for NSTec and LANL at the DAF and CEF are defined within the respective organizations' plans and procedures included in the authorization basis documentation for the respective Primary and Secondary REOPs. Both NSTec and LANL are executing the CEF activities in accordance with the REOP process. The Nevada Site Office federal staff is responsible for performing oversight of both organizations. Nevada Site Office fully understands the concerns with respect to the experiment review process. We have reviewed the current process and concur that not only does the NSTec FORC not possess the expertise related to the operation of the critical assembly machines but the LANL Criticality Experiments Safety Committee does not possess the expertise with respect to the DAF and CEF DSA and TSRs. As a result, NSTec	NSTec/LANL

appraisals of criticality experiment operations at NNSS. Although NSTec relies upon the LANL review process, it is not a credited TSR-level control.	and LANL are implementing the following modifications to the experiment plan review process. The LANL Criticality Experiments Safety Committee will include a representative from NSTec who is fully knowledgeable in the DAF and CEF DSAs and TSRs. In addition, the NSTec FORC will include both a representative from the LANL Criticality Experiments Safety Committee and the NSTec representative to the committee. This has been fully documented in the appropriate company documents (i.e., committee charters, experiment plan procedures, facility procedures). The assignment will be by formal letter from the associated organization. This will enhance the review process by adding the relevant facility safety basis expertise to the Criticality Experiments Safety Committee and the criticality experiments expertise to the FORC. In addition, the inclusion of both individuals on both committees better integrates the two committees. A further enhancement would be to make both of these individuals available to the USQ analyst as resources to be utilized during the USQ review. NSTec responsibilities for reactor safety oversight will be defined in a policy statement based on NSTec's role as the Primary REOP holder with the defined responsibility for safety coordination of user projects conducted at DAF. The policy will institute participation in the Criticality Experiments Safety Committee and FORC as described above, and establish the expertise and oversight needs to achieve effective safety coordination of critical experiments. Also, as part of an action plan to address an ORR finding, the SAC 5.9.17 will be reexamined to ensure necessary qualification requirements of the committees responsible for reviewing CEF Experiment Plans have been appropriately flowed-down into the SAC. TSR implementation procedures and processes will be modified, as appropriate, to address these qualification expectations. This enhancement to the CEF DSA will be completed in accordance with the established action plan to address an ORR finding.	

	NSTec - Revise DAF procedures for FORC – Completed **LANL - Revise Criticality Experiments Safety Review Committee charter – Completed** **NSTec – Issue policy statement on role as primary REOP holder – June 1, 2011** **NSTec - Submit DSA changes to Nevada Site Office – June 1, 2011**	
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 facility owner representatives involved in the simulated operation were detached and did not provide adequate oversight of the operation. It appears as though the lack of familiarity with criticality experiments extends to the operational level in the NSTec organization.	The following additional information is provided with respect to the deficiencies that were noted during dry run training evolutions. The activity observed by the staff was not a formal demonstration for a readiness review. It was a dry run training evolution. Deficiencies and opportunities for improvement are anticipated and expected outcomes of dry run training evolutions. The issue associated with the material movement and criticality safety requirement for Flat-Top was identified by the Nevada Site Office federal staff and discussed with LANL following the dry run. With respect to the instrumentation problems during the simulated operation of Godiva, the LANL Crew Chief clearly identified the problem and immediately declared to the entire audience in the control room that he could not proceed and had to cease the operation. In response to a question from the staff, he then discussed the follow on actions he would take with respect to the lockout of the fire suppression system. These steps involved notification to the DAF Operations Manager and implementation of the LCO. The Crew Chief's actions and follow on discussion were fully in accordance with the established procedures and authorization basis. The CEF operational readiness reviews identified issues in the area of conduct of operations. As a result, senior management from both NSTec and LANL have committed to improving and maintaining a high degree of formality, while conducting nuclear operations at the NNSS. NSTec has developed and is implementing the Formality of Operations Improvement Project (FOIP). The scope of the FOIP encompasses the following:	NSTec/LANL

	• Ensure documented compliance with nuclear safety requirements. • Formally define the Safety Management Programs and their owners. • Improve issues management process to ensure it provides an effective system of identifying and correcting causes. • Establish a consistent, high degree of management attention and formality when conducting nuclear operations. • Evaluate functional, organizational, and mission needs; assign necessary human capital with nuclear experience to achieve and sustain safe and compliant nuclear operations. LANL is implementing the following improvements, which are documented in the corrective action plans for the ORR prestart findings: • Develop and implement a procedure enhancement process. • Utilize an independent Senior Supervisory Watch for all CEF operations. • Establish and communicate management expectations for conduct of operations. • Ensure performance through periodic independent and management assessments.	