DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Washington, DC 20004-2901

April 2, 2012

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) has conducted a review of the preliminary design for the Uranium Processing Facility (UPF) at the Y-12 National Security Complex (Y-12). The timing of this review was driven by the development of the Preliminary Safety Design Report (PSDR). The Board is concerned because the PSDR was determined to be inadequate, both by the Board and by the National Nuclear Security Administration (NNSA). An adequate PSDR must be developed soon to support the ongoing final design efforts for UPF.

The Board has determined that safety is not adequately integrated into the design. Multiple significant unaddressed and unresolved issues exist with the PSDR and the development of the underlying safety basis for the facility. The Board is concerned that the UPF project team has not developed the PSDR based on bounding unmitigated analyses of the hazards for the facility and has not established a conservative methodology for determining the consequences of postulated accidents, consistent with DOE Standard 3009, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*. In addition, the UPF project team has not documented a safety strategy that clearly describes how the facility will meet DOE's safety requirements. The enclosure to this letter provides detail on the Board's specific concerns, including those dealing with (1) UPF's confinement strategy following a design basis seismic accident, (2) systems, structures, and components required to avoid an inadvertent criticality during or following a seismic event, (3) the need for thorough evaluation of unmitigated hazard and accident scenarios, (4) the need to identify controls to protect the public against small fires that have the potential for significant offsite toxicological consequences, and (5) the need to use reasonably conservative values to calculate dose consequences for several accident analyses that may require safety class controls.

The Board notes that NNSA decided to tailor the UPF project Critical Decision (CD) structure by combining CD-2 with CD-3. As part of this decision, NNSA initially cancelled the development of the PSDR for UPF. The Board believes that formal development and review of the safety basis and design are necessary to meet the intent of DOE Standard 1189, *Integration of Safety into the Design Process*. NNSA agreed with the need to document the safety basis and reinstated the development of the PSDR late in the preliminary design phase. NNSA completed its review of the PSDR and in a letter dated January 17, 2012, requested resubmission of the

PSDR after the contractor addresses the 110 most significant comments resulting from that review.

Therefore, pursuant to 42 U.S.C. § 2286b(d), the Board requests a report and briefing within 30 days of receipt of this letter describing NNSA's approach for demonstration of the adequate integration of safety in the preliminary design of the UPF. This report should address (1) resolution of issues identified by the Board and NNSA with respect to the safety documentation for UPF, (2) resubmitting and approving the PSDR, and (3) completing the technical independent project review of the integration of safety into the design for UPF as required under DOE Order 413.3, *Program and Project Management for the Acquisition of Capital Assets*.

Sincerely,

Peter S. Winokur, Ph.D.
Chairman

Enclosure

c: Mr. Daniel K. Hoag
Mr. Robert B. Raines
Mr. Harry E. Peters
Mrs. Mari-Jo Campagnone

Enclosure

Summary of Uranium Processing Facility Project and Related Issues

Safety Design Strategy. The Defense Nuclear Facilities Safety Board (Board) reviewed the conceptual design for the Uranium Processing Facility (UPF) at the Y-12 National Security Complex (Y-12) and issued a project letter on August 9, 2007, detailing the results of the review. At that time, the project had a reasonably conservative Safety Design Strategy (SDS) appropriate for a new major nuclear facility. This strategy included the use of safety-significant (SS) passive controls to segregate nuclear materials, reduce accident consequences, and preclude a post-accident nuclear criticality event. The strategy also included SS active systems to provide fire suppression, process safety controls, and primary and secondary confinement of materials. It identified all credited SS controls as being Performance Category 3 (later also designated as Seismic Design Category [SDC]-3) for natural phenomena hazards. While the Board was concerned about the lack of high-level key safety decisions in the SDS document at conceptual design, the proposed control set provided a basis for the Board to determine that the project had a robust safety posture. Now that the project has advanced to preliminary design, the project team has made a number of changes in the safety classification and seismic design of safety-related systems, structures, and components (SSCs) that give rise to concerns. Table 1 provides a summary of the progression of changes in the control set between the conceptual and preliminary design.

Table 1. Changes to the Safety-Related Controls for UPF between Conceptual Design and Preliminary Design

Safety-Related System	Conceptual Design	Preliminary Design
Fire Suppression System, Water supply, Fire Alarms	SS/SDC-3	SS/SDC-3
Criticality Accident Alarm System	SS/SDC-3	SS/SDC-1
Facility Structure	SS/SDC-3	SS/SDC-3
Confinement Ventilation System	SS/SDC-2	Not credited/SDC-1
Emergency Power	SS/SDC-2	No system currently credited
Fire Barriers	SS/SDC-3	Not credited
Process Confinement	SS/SDC-3	Not credited
Explosion Prevention	Not analyzed	SS/SDC-2
Criticality Prevention	Not analyzed/SDC-3	SS based on analyses/SDC-2
Process Shutdown	Not analyzed	SS/SDC-2

In accordance with Department of Energy (DOE) Standard 1189, *Integration of Safety into the Design Process*, the basis for safety decisions must be clearly articulated and documented to ensure that direction and decisions made regarding safety are explicitly identified and dealt with in the early stages of design. The Board evaluated the above changes using the revised SDS document and Preliminary Safety Design Report (PSDR). As discussed in the next section, the PSDR is inadequate to permit an evaluation of whether these changes to the safety classifications of SSCs are justified. The Board has identified the following concerns with the bases supporting changes in the seismic design category of equipment:

- Downgrading the confinement ventilation system from SDC-2 to SDC-1—this means the confinement ventilation system will not be designed to provide confinement following a seismic event. The SDS document does not identify an alternate system that will be designed to SDC-2 criteria to provide post-seismic confinement. This approach does not meet the DOE Order 420.1, *Facility Safety*, requirement that nuclear facilities with uncontained radioactive material "must have the means to confine the uncontained radioactive material to minimize their potential release in facility effluents during normal operation and during and following accidents."

- Downgrading the criticality prevention controls from SDC-3 to SDC-2—the criticality safety controls that are determined by a criticality safety evaluation to have a failure mechanism that can result in an inadvertent criticality during or following a seismic event will not be designed to reliably survive the seismic event and prevent the criticality. DOE Order 420.1 requires that the seismic design ensure that the safety controls can perform their safety function during a seismic event. DOE Order 420.1 references DOE Guide 420.1-2, *Guide for the Mitigation of Natural Phenomena Hazards for DOE Nuclear Facilities and Nonnuclear Facilities*, as the source for guidance on implementing the seismic requirements. This guide and the associated DOE Standard 1020, *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*, identify that inadvertent criticality is prevented by use of Performance Category 3 (equivalent to SDC-3) design requirements.

- Downgrading the Criticality Accident Alarm System (CAAS) from SDC-3 to SDC-1—this change means the CAAS will not be designed to function during and following a seismic event. The UPF project team's strategy to protect workers from an inadvertent criticality during a seismic event is to have a seismic event evacuation initiated by the seismic detection and response system activating the fire alarms. The use of the fire alarm as a seismic alarm does not adequately protect the facility workers because the appropriate responses for the two potential accident conditions are inherently different. An inadvertent criticality requires a prompt uninterrupted evacuation, while a seismic event or fire alarm typically invokes worker judgment to evacuate in a controlled manner based on the presence of immediate hazards. The project team has not provided a justification for why the potential for an inadvertent criticality during a seismic event is different from normal operations when a CAAS is required.

Babcock & Wilcox Technical Services Y-12, LLC (B&W) transmitted a revised SDS document to the Y-12 Site Office (YSO) on December 15, 2011. In the revised SDS document, B&W attempted to articulate safety goals based on applicable DOE requirements and the key safety decisions. Based on its review of the SDS document, the Board has determined that in some critical areas the revised SDS document provides a summary of the current design rather than a description of the key safety decisions that would guide the design to meet safety expectations (e.g., the confinement strategy).

Preliminary Safety Design Report. Based on application of DOE Standard 1027, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*, the UPF was categorized as a Hazard Category 2 nuclear facility. This categorization is based on the material quantities in the facility and the potential for inadvertent nuclear criticality. This categorization has remained unchanged since the conceptual design was developed. The UPF project team has applied the appropriate codes and standards from DOE Order 420.1 and its associated guides for use in the design and construction.

The Board has completed a detailed review of the PSDR and its supporting documents and has identified significant safety-related concerns. Given the hazards present in the UPF, the Board has determined that the safety controls and their associated safety functions and functional requirements will not provide adequate protection for site workers and the public. Specific examples are discussed below.

The current hazard analyses do not analyze all hazards properly (e.g., did not analyze them or limited the frequency or consequences of the hazard by crediting safety controls). This is not in compliance with the methodology in DOE Standard 3009, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses,* and DOE Standard 1189 for performing unmitigated hazard analysis. Examples include:

- The Saltless Direct Oxide Reduction process has hazards that were not evaluated because of the presence of process controls, an argon environment assumed to prevent metal dust explosions and special containers assumed to prevent pressurization explosions.

- The bounding fire scenarios for UPF are assumed to be limited to a single process area instead of the full facility because fire barriers were credited to prevent their spread.

- Self-protective actions are credited for various accident scenarios. While the PSDR disallowed the use of self-protective actions for some hazards (e.g., explosions), these actions are used for fire scenarios.

The accident analyses do not adequately identify and analyze representative and bounding accidents. DOE Standard 3009 states, "The range of accident scenarios analyzed in a DSA [Documented Safety Analyses] should be such that a complete set of bounding conditions to define the envelope of accident conditions to which the operation could be subjected are evaluated and documented." DOE Standard 1189 states that the preliminary design hazard and

accident analyses include "updating the analysis of the DBAs [Design Basis Accidents] analyzed in conceptual design to confirm the selection of facility-level hazard controls and their functional classifications" as part of iteratively developing a DSA meeting the methodology of DOE Standard 3009.

- Both small and large area fires are identified as having a significant offsite toxicological consequence. The accident analyses assumed the large area fire bounded small fires; this required the identification of SS controls. The large fire control selected was a fire suppression system, which has the safety function to prevent small fires from becoming large fires. However, small fires with the potential for significant offsite consequences are not prevented or mitigated by this control. This is because small fires may not provide sufficient heat to activate the fire suppression system or may be located in gloveboxes where the suppression system will not provide coverage. Yet the small fires are not analyzed. The analyses for fires need to be evaluated for representative and bounding fires to ensure the public is adequately protected.

- The post-seismic fire bounding analysis used a methodology that was not technically valid. The UPF project team has withdrawn the analysis but has not developed a replacement.

- The UPF project criticality accident scenario is not reasonably conservative. The UPF facility will process the same types of materials that are currently being processed in other facilities at Y-12. However, the criticality analysis supporting existing operations uses fission yields for criticality accidents at least a factor of 2 higher than are used in the analysis for UPF. For the existing operations, SS engineered controls are necessary to protect collocated workers. SS engineered controls have not been identified for UPF.

- 10 CFR Part 830, *Nuclear Safety Management*, requires the evaluation of beyond DBA, i.e., accidents with more severe conditions or equipment failures than are estimated for the corresponding bounding accidents. The one beyond DBA currently analyzed for UPF is not adequate, as it does not consider plant conditions, such as explosions, that could increase the dispersal of materials and dose consequences.

The UPF project team also has used non-conservative input parameters in their radiological dose consequence analysis. The dry deposition velocity calculation was performed in a manner not compliant with DOE Safety Bulletin 2011-02. The UPF project team has since revised the dry deposition velocity calculation to be compliant with the safety bulletin; however, this calculation uses non-conservative parameters. The dose consequence analysis also uses a potentially non-conservative minimum wind speed threshold value. The use of reasonably conservative values for these parameters would increase the dose consequences sufficiently to require the National Nuclear Security Administration (NNSA) to consider whether safety class controls are needed to protect the public.

Project Management. Following Critical Decision (CD)-1, NNSA tailored the project's CD structure to combine CD-2 and CD-3. NNSA also eliminated the development of the PSDR. While the Board did not object to NNSA's combination of critical decisions for project management purposes, the Board was concerned that NNSA planned to defer the preparation of crucial safety documentation and performance of safety-related reviews until the completion of the final design.

As early as April 2010, the Board discussed with YSO and B&W the need to conduct a preliminary design review to meet the intent of DOE Standard 1189. As a result of these discussions, B&W developed a roadmap for the integration of safety into the UPF design. In December 2010, B&W declared its readiness for the preliminary design review. YSO's review determined that the control set and integration of safety in design were not adequate. Subsequently, YSO directed B&W to develop a corrective action plan for addressing this inadequacy and prepare a PSDR (to support future preliminary design review efforts). B&W completed the PSDR in August 2011. Due to the significant findings identified in the subsequent NNSA and Board reviews, YSO directed B&W to revise both the SDS document and PSDR and resubmit them for review.

Preliminary Design. As mentioned previously, the Board does not believe the safety controls identified in the PSDR are adequate or that appropriate safety functions and functional requirements have been identified. At the present time, the Board does not have sufficient information to complete its review of the adequacy of integration of safety into the UPF preliminary design. The following discussion provides an overview of each area of the UPF design.

Geotechnical Design—The site is adequately characterized consisting of layers of residual soils, weathered shale, and unweathered shale. The project team has decided to leave some weathered shale in place because of cost considerations. While it is typical to remove all weathered shale, the structure can be adequately designed with some weathered shale left in place. The Board does not currently have any safety concerns with the geotechnical design.

Structural Engineering Design—The UPF process area structure is designed to meet conservative SDC-3 limit state D requirements. The shear wall building is well configured to resist design loads and seismic load paths are well developed. The Board's staff has reached consensus with the project team on structural modeling approaches and determined that the structure is sufficiently robust to address most of the issues raised in the Board's letter of March 15, 2010. Modeling assumptions were developed to simplify the analysis of the process area structure. These assumptions are reasonable and do not affect the fidelity of the completed analyses. However, they will need to be addressed before completion of the design of the process area structure. B&W has not developed an adequate summary of the remaining work scope to complete the final design. This summary is needed to provide a systematic plan with sufficient detail to assure the effective completion of the design effort that will resolve the remaining concerns identified in the Board's letter. Another letter from the Board raised technical and quality assurance issues associated with the computer program SASSI (a System for the Analysis of Soil-Structure Interaction), which is in use at multiple projects across the

defense nuclear complex, including UPF. The Board and NNSA have not yet agreed on a resolution approach to address all of the issues identified in this letter.

Confinement Design—The Board has determined that the confinement design (e.g., active confinement ventilation, process SSCs) does not meet the requirements of DOE Order 420.1 to provide confinement following a seismic event due to the downgrading of the SDC.

During normal operations, primary confinement of hazardous materials is maintained by process equipment and glovebox systems. This design approach represents a substantial improvement in operational safety relative to current Y-12 facilities, where some operations are unconfined or in fume hoods.

Fire Protection Design—The fire protection system is classified as a SS system. The safety functions identified for this system are: (1) prevention of small or localized fires from becoming large process area wide fires, and (2) prevention of inadvertent spraying of water on reactive materials. The system is to be designed in accordance with the national and international fire protection codes. The system is supported by a SS seismically qualified water supply system that services both UPF and the Highly Enriched Uranium Materials Facility. The design of the water supply eliminates reliability concerns with the current site water supply.

The Board has identified that the current list of functional requirements for this system is incomplete. For example, the project team did not consider functional requirements to address: (1) the potential for high offsite toxicological consequences from a localized fire (the existing design may not be capable of mitigating this hazard) and (2) the spraying of water on reactive materials following a seismic event (the gloveboxes containing reactive materials are not designed to survive a seismic event, any area fires that activate the fire suppression system can wet the reactive materials. This will cause explosions and potentially cause small fires to become a design basis fire).

Emergency Power Design—The UPF project team has determined that the safety-related emergency power requirements do not require the use of generators. Electric power for the safety-related systems, such as the CAAS and the fire alarm system, will be provided by an uninterruptible power supply or backup batteries as part of each system's design. The fire water supply system is powered by SS diesel-powered pumps. The Board currently has no concerns with this strategy.

Instrumentation and Control—The UPF project team has stated its intent to implement Institute of Electrical and Electronics Engineers (IEEE) Standard IEEE-379, *IEEE Standard Application of the Single-Failure Criteria to Nuclear Power Generating Stations*, and IEEE-384, *IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits*, as design criteria for the reliability of SS controls used to prevent explosions. Other industry standards (e.g., National Fire Protection Association, American Nuclear Society) may be used in lieu of the IEEE design requirements to design controls for accident scenarios to which they are directly applicable. This approach is acceptable for the design of SS safety instrumented systems and is consistent with the requirements of DOE Order 420.1. While discussed at a high level in the SDS, this approach has not yet been formally detailed in the *Control System Philosophy for the*

Y-12 Uranium Processing Facility, and thus has not yet been implemented for the design of SS safety instrumented systems.

Process Engineering and Process Safety—The hazards from the chemical inventory in UPF will be substantially reduced due to the use of new technologies when compared to the chemical forms and quantities that are used in the existing Y-12 facilities. The design also incorporates a strategy to use confinement for processes with unconfined hazardous materials. This design approach improves worker safety relative to current operations. The UPF SDS is to prevent explosions that pose a significant threat to worker safety or would damage facilities with appropriate SS controls. The UPF SDS also requires automated shutdown of processes should a DBA occur. While the Board continues to evaluate the adequacy of the safety analysis, the overall SDS for process controls appears adequate.

The technology readiness for most processes at the preliminary design stage is mature or represents minor modifications of existing processes. The development of agile machining and chip management is not at the expected technology readiness level for this stage of design but a technology maturation plan is in place. Technical problems have been experienced with the hot operational testing of the production microwave caster unit in an existing Y-12 facility. These technical problems are being investigated for resolution and for lessons learned to apply to the UPF microwave caster. The project team has risk mitigation plans in place for all identified technology maturation problems.

Criticality—As described previously, the Board has identified issues associated with the seismic design of the CAAS and controls whose failure has been determined to potentially result in an inadvertent criticality during or following a seismic event, and the determination of the bounding criticality accident.

The project team has invoked the requirement from 10 CFR Part 830 to ensure that operations with fissionable material remain subcritical under all normal and credible abnormal conditions. When possible, the project team has selected mass controls to prevent criticality. The processes often also require geometry controls to prevent criticality.

Federal Oversight. YSO continues to be understaffed and the Board believes that additional resources are required for adequate oversight of the UPF project. The YSO staffing analysis identifies the following engineering staffing needs: one project engineering and design, one nuclear safety engineering, one criticality safety engineering, and two quality assurance personnel. Several of these functions are currently being performed by YSO personnel that are also responsible for project management. This dual responsibility for both project management and engineering results in a reduced capability for federal oversight.