DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Washington, DC 20004-2901

December 13, 2011

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 staff of the Defense Nuclear Facilities Safety Board (Board) recently completed a review of the design, functionality, and maintenance of selected safety systems at Lawrence Livermore National Laboratory (LLNL). The results of this review, detailed in the enclosure to this letter, indicate (1) the defined safety functions of certain systems could not be reliably implemented during normal and abnormal operating conditions and (2) the boundaries of safety systems were inappropriately defined.

The Board notes that the Livermore Site Office has initiated an extent-of-condition review based on the issues identified in the enclosed report. However, two issues are of particular concern to the Board:

- The credited confinement boundary in the Plutonium Facility's glovebox system includes (1) wooden enclosures of housekeeping high-efficiency particulate air filters and (2) plastic tubing, which cannot be relied upon to fulfill the system's safety function.

- The Plutonium Facility's Fire Detection and Alarm System cannot fulfill its safety function because it can be defeated by a non-safety system.

Therefore, pursuant to 42 U.S.C. § 2286b(d), the Board requests a report and briefing within 60 days of receipt of this letter describing specific actions the National Nuclear Security Administration (NNSA) has taken or plans to take to ensure the glovebox system and Fire Detection and Alarm System can perform their safety functions. The Board also requests a

report within 1 year of receipt of this letter describing any actions NNSA has taken to resolve the other issues noted in the enclosed report.

Sincerely,

Peter S. Winokur, Ph.D.
Chairman

Enclosure

c: Ms. Alice C. Williams
Mrs. Mari-Jo Campagnone

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

September 2, 2011

MEMORANDUM FOR: T. J. Dwyer, Technical Director

COPIES: Board Members

FROM: C. Roscetti

SUBJECT: Review of the Design, Functionality, and Maintenance of Safety Systems at Lawrence Livermore National Laboratory

This report documents a review of the design, functionality, and maintenance of safety systems at Lawrence Livermore National Laboratory (LLNL). This review was conducted by members of the staff of the Defense Nuclear Facilities Safety Board (Board) J. Anderson, E. Gibson, J. Plaue, C. Roscetti, and C. Shuffler during June 14–16, 2011. The Board's staff concluded not all the safety systems the staff reviewed could reliably fulfill their specified safety-significant functions as defined in the Plutonium Facility Documented Safety Analysis (DSA).

Gloveboxes. The Plutonium Facility DSA classifies as safety-significant gloveboxes whose safety function is to protect workers by confining hazardous and radioactive materials. The glovebox system is comprised of multiple components including the glovebox, attached accessories (e.g., vacuum pumps, atmospheric monitors/controllers, analytical equipment), the housekeeping high-efficiency particulate air (HEPA) filters and associated encasements, and the exhaust ducting up to the differential pressure regulator in the exhaust header.

Many of the gloveboxes in the Plutonium Facility include wooden-enclosed housekeeping HEPA filters and plastic tubing in the glovebox exhaust path. The wooden casing and plastic tubing are credited as safety-significant confinement barriers. These aged glovebox components represent a vulnerability in the confinement boundary of gloveboxes because they were not designed, analyzed, or tested to meet the housing or ventilation ducting containment requirements of nuclear codes. In addition, Department of Energy (DOE) Handbook 1169-2003, *Nuclear Air Cleaning Handbook*, warns against using enclosed filters. These components may therefore not be capable of fulfilling their safety function during all normal and abnormal conditions.

LLNL applies no time restrictions on housekeeping HEPA filter service life, which includes the wooden encasement. The Board's staff observed that many filters and encasements are approaching 30 years of age. LLNL has no formal plans to replace these filters and encasements with nuclear-grade housings and filters and maintains that operating experience and regular surveillances, including annual visual inspection and periodic radiation surveys, verify

their confinement capability. Routine visual inspections and radiation surveys do not ensure the ability of the wooden encasements or plastic tubing to maintain a safety-significant confinement boundary. The staff notes that recent glovebox installations at LLNL and other nuclear facilities, such as the Plutonium Facility at Los Alamos National Laboratory, utilize a more robust, nuclear-grade housing and replaceable filter along with a flexible metal bellows connection to exhaust ducting.

The Board's staff also determined the safety function and performance criterion for gloveboxes stated in the Plutonium Facility DSA does not capture and protect all functional requirements implied and credited in the hazard analysis. For example, the glovebox is credited in the hazard analysis to support an inert gas atmosphere for prevention of pyrophoric material reactions and to protect facility workers against shrapnel hazards generated during glovebox operations (i.e., events 46b and 12 in Table 3-8 of the Plutonium Facility DSA). However, the Plutonium Facility DSA does not capture these requirements in the description of the safety function, nor does it identify any functional requirements or performance criteria for protecting them.

Additionally, the performance criterion in the Plutonium Facility DSA does not ensure the glovebox system can meet its functional requirements. DOE Standard 3009-94 Change Notice 3, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, states, "Performance criteria characterize the specific operational responses and capabilities necessary to meet functional requirements." The performance criterion for gloveboxes specifies only that gloveboxes must be capable of facilitating a negative pressure differential with respect to the room. Being capable of facilitating a negative differential pressure is non-specific, not measurable, and cannot reliably ensure that an inert gas atmosphere, shrapnel protection, and hazardous material confinement are maintained. As a result, a degraded glovebox (e.g., a broken window or non-leak tight encased housekeeping HEPA filter) could meet the performance criterion for gloveboxes yet be incapable of fulfilling the safety function. Improvements to the safety function, functional requirements and performance criteria are necessary to provide reasonable assurance that the glovebox system can meet the safety requirements in the Plutonium Facility DSA.

Fire Detection and Alarm System (FDAS). The Plutonium Facility DSA designates the FDAS as a safety-significant system whose function is to detect fires and alert personnel. When a fire in the Plutonium Facility is detected, the FDAS alerts personnel through the audio warning and building paging (AW/P) system. However, the FDAS cannot fulfill its safety function at all times because the AW/P system interfaces with a non-safety system, the site-wide evacuation voice/alarm (EVA) system. The site-wide EVA system can prevent the AW/P system's alert message from being heard in the Plutonium Facility. Thus, the FDAS cannot fulfill its safety function during all normal and abnormal conditions.

The FDAS does not provide immediate, local annunciation of a potential fire condition, which would be the most direct method of alerting the worker to take appropriate action. Instead, the FDAS generates a facility-wide message that gives workers no detail on what actions to take, but merely instructs them to stand by for further information. The Facility Safety Plan (FSP) also contains no instruction to workers to check their immediate areas following receipt of

the facility-wide message and reiterates that workers are to stand by for further information. The facility-wide message or actions required by the FSP require more detail to ensure the protection of workers in the Plutonium Facility. Additionally, further information is provided to workers after the fire department's response to a fire condition. It is clear that as part of the FDAS safety function to alert personnel, the fire department must be alerted. However, the fire department response and ability to provide further instructions to workers as required by the facility-wide alert message and FSP is not captured in the FDAS functional requirements or performance criteria.

Because the EVA system can override the FDAS safety function, LLNL implemented a software restriction in the Alameda County Dispatch Center that limits the time for which the EVA system can override the FDAS to 2–3 minutes. The 2–3 minute software restriction and associated documentation fail to meet software quality assurance (SQA) requirements and have no technical basis. Irrespective of its role and interface with the safety-significant FDAS, the EVA system clearly meets requirements for consideration of SQA for its life safety function in all other facilities at the laboratory, but has neither been screened for nor undergone SQA review.

LLNL credits indications at the fire alarm panel in the Control Room as a supplement to the facility-wide message, but the Control Room is not continuously manned. The repeater panel in the Operations Office, which is continuously manned, is not included in the credited, safety-significant portion of the FDAS. Furthermore, the FDAS cannot be relied upon to notify the fire department because the FDAS includes non-credited leased communication lines and unqualified software and other systems in the Alameda County Dispatch Center.

Additionally, the Fire Hazards Analysis (FHA) in 2002, 2006, and 2009 determined that the Plutonium Facility building paging system (AW/P system) does not meet NFPA 72, *National Fire Alarm and Signaling Code*, requirements for an emergency system. The 2009 FHA states, "The EVA panels were upgraded with units that are UL [Underwriters Laboratories] listed for emergency use but the [AW/P system] speakers and wiring were not, resulting in circuits that are not supervised to show trouble conditions such as open, shorts or grounds." The implications of this vulnerability are that the FDAS would not be able to perform its safety function if the system experienced shorts or grounds in the wiring.

Livermore Site Office (LSO) Assessments. Based on this review and issues identified by the Board's staff, LSO is performing an extent-of-condition review of the selected safety systems. The staff is encouraged by this action. However, the staff reviewed various assessments of safety systems performed by LSO personnel during the past 2 years, and found that these assessments were insufficiently detailed to identify issues similar to those discussed in this report. When LSO personnel did identify potential issues, the issues were not given appropriate attention or follow-up and subsequently not brought to the attention of LLNL personnel for appropriate corrective action.

During this review the Board's staff identified additional deficiencies associated with the safety significant systems in the Plutonium Facility, which are outlined in Appendix A of this report.

Appendix A

The following system deficiencies were also identified by the Board's staff during its review of the design, functionality, and maintenance of safety systems at LLNL during June 14–16, 2011.

Gloveboxes.

- Some leak test requirements for new glovebox installations specified in the LLNL *Nuclear Materials Technology Program Glovebox Manual* are inconsistent with the latest industry technical standard for nuclear glovebox fabrication and design, American Glovebox Society (AGS) Standard G006-2005, *Standard of Practice for the Design and Fabrication of Nuclear-Application Gloveboxes*.

- The Plutonium Facility's FHA provides no justification for excluding an automatic fire suppression and inerting system from the design of a recent glovebox installation (Work Station 2111). DOE Standard 1066-99, *Fire Protection Design Criteria*, states, "An automatic fire suppression or inerting system is required in all new gloveboxes unless an FHA [Fire Hazards Analysis] concludes that such a system is not warranted...."

Glovebox Exhaust System (GBES).

- The hazard table in the Plutonium Facility DSA credits the GBES to protect workers from a radiological release caused by a glovebox explosion (event 47b). One functional requirement for the GBES is to maintain gloveboxes at a negative pressure relative to the room. LLNL personnel could not explain how the system meets this functional requirement during postulated explosion events. The GBES is the only credited control that protects workers in the immediate vicinity of a glovebox explosion for several accident initiators, such as water leaking into a process furnace, leakage from a methane or acetylene torch, and ion exchange resin reactions.

- DOE Handbook 1169-2003, AGS standards, and the LLNL *Nuclear Materials Technology Program Glovebox Manual* specify that glovebox exhaust systems must be capable of maintaining 125 +/- 25 feet per minute (fpm) of inward airflow through an open glovebox gloveport to prevent the spread of contamination in the event of a glove breach. LLNL does not evaluate whether gloveboxes can meet the 125 fpm safety requirement at the GBES's most limiting condition (i.e., lowest allowable GBES header pressure in the Technical Safety Requirements (TSR)).

- The Plutonium Facility DSA does not include the GBES exhaust stack within the safety-significant boundary of the system, although the exhaust flow path through the stack is required for the GBES to perform its safety function.

- The Plutonium Facility DSA requires that GBES exhaust header pressure be maintained between -3.0 and -7.0 inches of water gauge; however, the set point that initiates startup of a backup exhaust fan is -1.5 inches of water gauge.

Hydrogen Gas Control System (HGCS).

- The system boundaries for the HGCS are inadequately defined, and failure of non-safety components could preclude the system from fulfilling its safety-significant function during normal and abnormal operations. Specifically, the non-safety hydrogen sample pump and the flow meters need to be operable for the HGCS to perform its safety function and fulfill its performance criteria. These flow meters provide an indication of flow to a safety-significant programmable logic controller (PLC) for the HGCS. Although the PLC is safety-significant and the embedded software has been through SQA, the system's documentation is not clear regarding the safety classification of the PLC or whether the embedded software on the PLC has been through SQA.

- The vacuum pump that serves the programmatic Hydride/Dehydride/Casting (HYDEC) equipment interfaces with atmospheres containing significant quantities of hydrogen. It is not clear to the Board's staff that the appropriate design requirements for this service were identified and implemented for the existing vacuum pump.

Hydrogen Gas Isolation System.

- Operating Procedure-Programmatic (OPP-B332-001), *Operating procedure for HYDEC process in the Metal Conversion Glovebox*, steps 6.13.1 and 6.13.2, implements the specific administrative control (SAC) to isolate the hydrogen gas cylinder to the radioactive materials area (RMA) when hydrogen is not being used in the RMA. However, this procedure does not indicate these steps fulfill a TSR-level control. Operational Safety Plan (OSP) 332.194, *Metal Conversion Glovebox*, implements the same TSR-level control, but OSP 332.194 is a plan, not a continuous-use procedure. OSP 332.194 implements the TSR control that only a single hydrogen gas cylinder shall be connected to the hydrogen gas manifold at a time, but it is also not a continuous-use procedure. It is therefore not clear to the staff how operators are made aware that their actions implement SACs.

- Based on system specifications and conservative assumptions (i.e., maximum bottle pressure), the Board's staff determined that a sheared hydrogen gas supply tube in the glovebox could overpressurize the glovebox with hydrogen. As a result, the staff believes the excess flow shutoff valves and/or pressure regulator serve important safety functions (i.e., to prevent overpressurization), and it would be appropriate to credit at least one of these components. However, this overpressurization hazard and the related safety function are not identified in the Plutonium Facility DSA, and none of these components are credited.

Equipment Important to Safety (EITS).

- At LLNL, EITS systems are subject to more rigorous configuration management and quality assurance requirements compared with other defense-in-depth systems. Although LLNL does not credit EITS for protection of workers or the public, these systems are recognized as important contributors to safety. The documentation for configuration management of EITS systems is a system data sheet rather than a typical system design description, and the EITS configuration item owner maintains the system data sheet. LLNL's implementation and use of system data sheets is immature. For example, the training and expectations for configuration item owners are not well defined or consistent. Neither the data sheet for the Tritium Facility's fire suppression system nor that for the Hardened Engineering Test Building's ventilation system listed procedures related to system operation or maintenance. The procedures section of these data sheets only included drawings, the respective facility DSA, the more general FSP, and nonspecific emergency management division policy and procedures.

- If EITS systems are going to be recognized in a DSA as meeting certain requirements, these systems should be assessed against the stated requirements, functions, and configuration. There have been at least four discrepant as-found conditions regarding EITS systems in the past 2 years, which suggests this is not the case.

- For LLNL to benefit from the EITS designation and corresponding system data sheets, increased training for configuration item owners and clearer, written expectations concerning the structure and utilization of system data sheets are warranted. Similarly, expectations need to be defined for the site office's oversight of EITS systems.