DEFENSE NUCLEAR FACILITIES SAFETY BOARD

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

September 10, 2007

The Honorable Thomas P. D'Agostino
Administrator
National Nuclear Security Administration
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-0104

Dear Mr. D'Agostino:

The Defense Nuclear Facilities Safety Board (Board) has completed a review of nuclear criticality safety (NCS) implementation, conduct of operations, and configuration management in the Plutonium Facility vault at Los Alamos National Laboratory. The enclosed report prepared by the Board's staff provides a detailed discussion of the results of this review. This letter focuses on one of the issues identified during the review that deals with the improper utilization of the laboratory's Materials Accountability and Safeguards System (MASS) software to ensure compliance with criticality safety limits.

The laboratory uses MASS to track material movements and special nuclear material storage throughout the Plutonium Facility, including movements into and out of the vault. MASS often provides the sole source of information about a given item, such as mass and isotopic composition. Despite the laboratory's contention that MASS is merely an operator aid and is not relied upon to determine the safety of material movements, discussion with operators and review of procedures revealed that MASS fulfills critical safety-related functions, such as determining compliance with NCS limits. MASS was initially conceived as a security-related accountability program and accordingly was not designed to perform a criticality safety-related function. As a result, its criticality safety aspects were not subjected to the rigorous quality assurance requirements and configuration management that its current safety-related usage would require.

MASS was developed by the laboratory in the 1970s in a programming language that is difficult to maintain and has not seen a significant software upgrade since its introduction. Consequently, the laboratory has long-standing plans to transition MASS to a modern computing platform and programming language. Even though the need for a MASS update was identified more than 10 years ago, upgrade efforts have been unsuccessful. The laboratory recently revived the effort to modernize and upgrade MASS, but progress is not yet evident. In addition, it is unclear whether the current concept for a new MASS acknowledges its safety-related function and therefore identifies the appropriate software quality assurance and configuration management requirements.

Therefore, pursuant to 42 U.S.C. § 2286b(d), the Board requests a report within 90 days of receipt of this letter outlining the overall strategy and key milestones for the MASS upgrade. Included in this strategy should be:

- Identification of the safety functions that MASS currently performs and upon which management relies, and all new safety functions which will be incorporated into the upgraded system.

- Discussion of the process for incorporating these new requirements into an improved MASS, and how lessons learned from previous upgrade attempts, including the need for strong project leadership, have been captured in the upgrade strategy and milestones.

- Compensatory measures to ensure the safety of material movements before the MASS upgrade has been completed.

- Specific actions the National Nuclear Security Administration will take to ensure the success of the MASS upgrade.

Sincerely,

A. J. Eggenberger
Chairman

c: Mr. Glenn S. Podonsky
Mr. Donald L. Winchell, Jr.
Mr. Mark B. Whitaker, Jr.

Enclosure

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

August 6, 2007

MEMORANDUM FOR: J. Kent Fortenberry

FROM: C. Goff and E. Elliott

SUBJECT: Materials Accountability and Safeguards System Software at Los Alamos National Laboratory

This report documents a review by the staff of the Defense Nuclear Facilities Safety Board (Board) of nuclear criticality safety (NCS) implementation in the Plutonium Facility (PF-4) vault at Los Alamos National Laboratory. The review included a site visit on June 5–7, 2007, as well as a follow-up teleconference held on July 19, 2007. Members of the Board's staff B. Broderick, R. T. Davis, E. Elliott, C. Goff, C. Keilers, M. Moury, and J. Plaue participated in the review.

Materials Accountability and Safeguards System Software. The laboratory tracks material movements and special nuclear material (SNM) storage throughout PF-4 using the software program referred to as the Materials Accountability and Safeguards System (MASS). MASS often provides the sole source of information about a given item, including mass, isotopic composition, material form, and storage location. MASS is also used to generate the material label that is affixed to the outside of each SNM container. Before SNM is physically transferred to a new location in the facility, the transfer must be completed electronically in MASS by the operators. In some cases, the criticality limits for a given location (e.g., glovebox or vault) are loaded into MASS.

Reliance on MASS for Safety—According to laboratory management, MASS is regarded as an operator aid that provides information for criticality control purposes, but is not relied upon to perform a criticality safety function. This belief is consistent with the description of MASS in the administrative procedure that governs NCS implementation in PF-4 (TA55-AP-522) which states that MASS is "a useful administrative tool to assist nuclear material handlers in managing fissile material inventories within approved limits." The NCS group also informed the Board's staff that operators use MASS only to obtain data; compliance with NCS limits is to be determined by hand calculation while referencing the approved values contained in the NCS posting and associated Criticality Safety Limit Approval (CSLA).

The assertion that MASS is only an operator aid is not consistent with the laboratory's implementing procedures. In some situations, MASS automatically provides both NCS limit information and performs the calculation to verify compliance with the limits. In TA55-AP-522—the procedure that describes MASS as an "administrative tool"—there are procedural steps detailing the movement of items into a glovebox that state, "Before physically moving the fissile material, perform the MASS transaction to check that the amount and form of the material being

transferred is within the criticality safety limit for the destination glovebox." Hand calculations are not mentioned in the procedure or the associated training. Additionally, a Technical Area-55 Notice (TA55-Notice-011) sent to all employees on October 31, 2006, instructs operators to execute the electronic transfer in MASS before physically moving the material into the location, with the express purpose of preventing an overmass condition. The notice uses the following lessons-learned statement to explain the new requirement: "The practice was to physically move items, then enter the information into MASS. This means that computer material accountability checks were not performed until the item was in the new location. This permitted human error, which can result in exceedance of criticality safety limits." In both the procedure and the notice, the laboratory is instructing operators to use MASS to comply with NCS limits.

After speaking with vault operators, it was clear to the Board's staff that MASS was also being relied upon in the vault for compliance with criticality safety limits. For example, some vault storage locations have NCS limits that are based on the total mass and allow multiple SNM containers. MASS keeps a running total of the mass in each storage location, and will output a warning message that informs the operators if an NCS limit will be exceeded when they electronically process an SNM transfer. According to the vault operator procedure (NMT4-WI-101) if MASS generates a warning that a criticality limit will be exceeded, the operators are instructed to consult the CSLA to check the NCS limit, *after* MASS has alerted them. The operators also consult a handwritten Vault Availability Book (the Blue Book), which is used primarily to ensure that the item will physically fit into the storage location. The Blue Book also provides a form to indicate the location's running mass total, which could serve as a second check of the total mass; however, it does not contain the NCS limits. In this case, MASS is relied upon to prevent an "overmass" condition, which means that MASS is performing a safety function exceeding that of an "operator aid."

Safety Software Requirements—MASS was originally developed in the 1970s as a security-related accountability program, and thus it lacks the configuration management control and software quality assurance pedigree of a safety-related system. Department of Energy Order 414.1C, *Quality Assurance*, requires that software performing safety functions meet certain requirements, including appropriate configuration management of key data, verification and validation of software operation, and documentation. Currently, MASS does not meet many of these requirements. As an example, changes to NCS limit data in MASS that should require configuration management control are handled informally via email and are not verified or audited by the NCS group.

Planned Improvements—As mentioned previously, MASS was developed more than 20 years ago, and was written in a programming language that is difficult to maintain; it has not undergone a software upgrade since its inception. The original author of the code, now retired, is the only person capable of editing the source code and is still relied upon to make improvements and correct problems, which included three instances of system inoperability during the past year.

Because of the age of the code and the limited ability to update it, the laboratory began efforts to transition MASS to a modern computing platform and programming language more than 10 years ago; however, these efforts were unsuccessful. A March 2006 report by the laboratory's Audits and Assessments office found that the MASS upgrade project lacked "full management support, project leadership, defined scope, prepared schedule and budget, and quality assurance plan for a successful functional and timely implementation." This finding was repeated from two previous assessments, one performed in July 2004 and the other in March 2002.

Recently, the laboratory revived the effort to modernize and upgrade MASS. In particular, laboratory management formally: (1) consolidated responsibility for the system, which historically has been a significant hindrance to progress and (2) committed to providing the necessary resources for the upgrade. During the teleconference with the Board's staff on July 19, 2007, the laboratory further indicated that early planning had begun for a renewed effort that is expected to be mature in early fall 2007. No project manager had been assigned to the project, and substantive planning incorporating lessons learned from previous upgrade attempts was not evident. It was unclear whether the concept for a new MASS acknowledges its safety-related function and therefore identifies the appropriate software quality assurance and configuration management requirements. The effort to upgrade and modernize MASS would appear to be an excellent opportunity to implement these requirements formally. A representative from the Los Alamos Site Office (LASO) expressed the expectation that the managerial rigor of the MASS update effort would be commensurate with that of other major design and construction projects, but did not explicitly acknowledge MASS as safety-related software.

Observations on Vault Operations. The following observations made by the Board's staff have been informally communicated to the laboratory for its use.

NCS Involvement in Operational Changes—The staff was briefed on findings from an internal assessment by the PF-4 Deputy Facilities Operations Director. This assessment identified that the NCS group was not always involved when an operation underwent a change. This lack of NCS involvement in the change process has resulted in ongoing operations that are not in compliance with NCS postings. The NCS group is required by ISD 130-1.0, *Nuclear Criticality Safety Program Manual*, to evaluate new or revised operations involving significant quantities of fissionable material. However, this requirement is weakly implemented at the present time, a situation that the improved Unreviewed Safety Question process should rectify by requiring NCS concurrence on proposed changes to fissile material operations. In the interim, the NCS group issued a letter stating that NCS approval is needed for any changes to fissionable material operations.

Adequacy of Vault Operator Staffing—Vault operations require two trained vault operators. Currently, there are only two trained vault operators, with a third in training who is approximately 1 year away from full qualification. Because of the limited number of qualified personnel, the vault is typically accessible to users only during the morning and must close if one of the two vault operators is absent from work. Overall, the laboratory has not developed

adequate staffing plans to safely support the expected increase in programmatic mission, as well as ongoing nuclear material stabilization and repackaging activities, including actions to implement the Board's Recommendations 94-1, *Improved Schedule for Remediation in the Defense Nuclear Facilities Complex*, and 2000-1, *Prioritization for Stabilizing Nuclear Materials*.

Priority of NCS Reevaluation for the Vault—Based on earlier walkdowns conducted as part of the NCS Program Improvement Plan (PIP), vault operations were categorized as a medium-risk activity, and NCS evaluations governing the vault were deemed to have only "administrative deficiencies." The Board's staff examined the vault documentation, which consists of a number of convoluted NCS evaluations that rely heavily on expert judgement. In some cases, the evaluations contradict one another. In at least one case, controls identified as necessary in the evaluations (i.e., use of neutron-absorbing material) are not being implemented appropriately. These deficiencies in the NCS evaluations for the vault are unlikely to be addressed in the near term, because the NCS group is currently focused on evaluating and documenting other operations deemed to be of higher risk during NCS PIP walkdowns. Additionally, bringing the vault NCS evaluations into compliance with DOE Standard 3007, *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Nonreactor Nuclear Facilities*, will require substantial staff resources. According to the current schedule, the vault evaluations will not be rewritten until the third quarter of fiscal year 2009. The Board's staff believes the existing vault evaluations contain technical deficiencies and that their rewriting should be accorded higher priority, especially given the large number of vault movements and the fact that the vault is nearing capacity.

Weaknesses in the Conduct of Operations—The staff observed a movement of SNM into the vault. Overall, the vault staff and material handlers appeared to be highly knowledgeable; however, the Board's staff did observe weaknesses in the conduct of operations. For example, the vault operators informed the staff that the local copy of the procedure that governs the use of MASS was 2 years out of date and did not accurately reflect some of their current practices. While an updated procedure was available in the facility's document control system, it was not being utilized. The Board's staff emphasized the need for the correct version of the procedure to be present in the workspace. Subsequently, the local (and out-of-date) copy of the procedure was replaced.

Status of Federal NCS Oversight. Currently, LASO has one individual performing NCS oversight, with augmentation and monitoring provided by personnel from the National Nuclear Security Administration (NNSA) Service Center. The LASO engineer has limited NCS experience and has completed about one-third of the required training to qualify under the appropriate technical qualification standard (DOE Standard 1173, *Criticality Safety Functional Area Qualification Standard*); this individual's full qualification is anticipated late this year. The Board's staff is concerned about the objectivity of the oversight being performed, because NNSA is relying on the laboratory NCS group to provide mentoring and NCS instruction to the qualifying LASO engineer. NNSA should require that NCS oversight personnel in training spend time at sites other than their own to obtain a broader perspective on NCS program implementation.