Department of Energy
Washington, DC 20585

July 22, 2013

Dr. Penrose C. Albright
President and Laboratory Director
Lawrence Livermore National Security, LLC
Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, California 94550

NEL-2013-03

Dear Dr. Albright:

The Office of Health, Safety and Security's Office of Enforcement and Oversight has evaluated the facts and circumstances surrounding programmatic deficiencies identified in the Lawrence Livermore National Security, LLC (LLNS) software quality assurance (SQA) program. LLNS reported these deficiencies on January 16, 2013, in Noncompliance Tracking System (NTS) report NTS--LSO-LLNL-LLNL-2013-0001, *LLNL Software Quality Assurance Program Does Not Meet DOE O 414.1D Standards and Procedures Requirements*.

On December 13, 2011, the Defense Nuclear Facilities Safety Board (DNFSB) issued a letter to the National Nuclear Security Administration (NNSA) documenting the DNFSB's review of the design, functionality, and maintenance of selected safety systems at Lawrence Livermore National Laboratory (LLNL). This review identified, in part, that the "site-wide evacuation voice/alarm (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." In addition, the DNFSB noted that, although the Hydrogen Gas Control System (HGCS) programmable logic controller (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."

As part of a safety system review required by the Livermore Field Office Master Assessment Schedule, the Department of Energy's (DOE) Livermore Field Office (NA-00-LL) enlisted a SQA subject-matter-expert to conduct an assessment of LLNS's SQA practices for the Fire Detection and Alarm System (FDAS) software and the PLC for the HGCS, including flowdown of institutional SQA program requirements. The assessment report documented 19 findings, 3 observations, and 6 recommendations, and was formally provided to LLNS on November 19, 2012. The assessment identified that "[m]ost of the findings were associated with the LLNS's inability to demonstrate how the set of IEEE [Institute of Electrical and Electronics Engineers] Standards are to be utilized or are equivalent to ASME [American Society of Mechanical Engineers] NQA-1 [Nuclear Quality Assurance - 1]

requirements and the LLNS ISQAP's [institutional SQA program] safety software grading methodology that was used to grade the two applications that were assessed. Some findings were based on the lack of procedures that are needed to define, document, and manage the SQA lifecycle documentation for the two applications [HGCS and FDAS] as required by ASME NQA-1 and the set of IEEE Standards that LLNS has selected as their consensus standard."

In response to this assessment, LLNS performed a causal analysis using the System-Problem-Cause methodology and identified two root causes and four other causal factors. In its first root cause, LLNS identified that "[a]t the programmatic (i.e., ISQAP) level, lack of formality in the interactions between LLNL [LLNS] and LSO [NA-00-LL] and the lack of rigor in the impact analysis resulted in inadequate or missing records of evidence that the ISQAP was reviewed against all DOE O 414.1D requirements. This allowed for misinterpretations on the part of LLNL [LLNS] regarding DOE O 414.1D requirements." In its second root cause, LLNS identified that "[a]t the implementation level, the ISQAP documentation lacks sufficient detail to accurately convey what is expected of LLNL [LLNS] organizations when implementing the ISQAP, particularly for those organizations lacking SQA expertise of their own and for lower risk applications."

Based on a review of this documentation, the Office of Enforcement and Oversight identified potential noncompliances with 10 C.F.R. Part 830, *Nuclear Safety Management*. These include: (1) failure to identify, control, and correct items, services, and processes that do not meet established requirements; (2) failure to prepare and maintain records; and (3) failure to perform work consistent with technical standards, administrative controls, and other hazard controls adopted to meet regulatory or contractual requirements, using approved instructions, procedures, or other appropriate means.

The planned LLNS corrective actions in response to findings presented in the NA-00-LL assessment appear appropriate. Of particular note are the actions to revise the ISQAP and to re-evaluate the grading level methodology and grading levels for all LLNS safety software in light of the report findings. In addition, LLNS's completed operability checks of nuclear facility safety systems having imbedded software applications, and the operability checks did not identify any immediate concerns with safety system software functionality. The corrective action plan was approved by NA-00-LL with the condition that specific interim milestone deliverables be submitted by LLNS prior to the submission of the revised ISQAP and that additional corrective actions for the implementation phase of the revised ISQAP be provided to NA-00-LL.

The Office of Enforcement and Oversight considers SQA to be vital in ensuring that embedded software in safety systems, structures, and component will perform reliably as designed. While no immediate safety consequences resulted from these programmatic deficiencies in the LLNS ISQAP, the potential for adverse consequences to LLNS's operations remains a concern until significant

improvements are made to the ISQAP. Therefore, the Office of Enforcement and Oversight, in conjunction with NNSA, will continue to closely monitor SQA implementation at the laboratory.

No response to this letter is required. If you have questions, please contact me at (301) 903-2178, or your staff may contact Mr. Steven Simonson, Deputy Director for Enforcement, Office of Enforcement and Oversight, at (301) 903-7707.

Sincerely,

John S. Boulden III
Director
Office of Enforcement and Oversight
Office of Health, Safety and Security

cc: Kimberly Davis-Lebak, NA-00-LL
Peter Rodrik, NA-00-LL
Thomas Gioconda, LLNS
Connie De Grange, LLNS
David Jonas, DNFSB