DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Washington, DC 20004-2901

March 16, 2015

Mr. David M. Klaus
Deputy Under Secretary for
Management and Performance
Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585

Dear Mr. Klaus:

Recent reviews by the Defense Nuclear Facilities Safety Board's (Board) staff identified deficiencies in the proper oversight, maintenance, and use of the computer program "Radcalc," which is used by over 400 users across the complex and other organizations to determine the appropriate transportation package classification for radioactive materials. These deficiencies could result in vulnerabilities in Radcalc's calculation of decay heat, radioactivity, and/or hydrogen gas generation, which could result in serious consequences for workers and the public in the event of a transportation accident. It is not clear to the Board how the risk associated with the use of Radcalc is being managed.

The issues identified by the staff challenge whether the Radcalc safety calculation results will adequately perform their safety function. The Department of Energy (DOE) Office of Transportation and Packaging has not conducted federal oversight of Radcalc consistent with requirements of Title 10, Code of Federal Regulations, Part 830, Subpart A, *Quality Assurance Requirements*, and DOE Order 414.1D, *Quality Assurance*, for virtually the entire lifespan of the software, even though it categorized Radcalc as safety software. The details of these issues are provided in the enclosed report.

Therefore, pursuant to 42 U.S.C. § 2286b(d), the Board requests a report within 90 days of the issuance of this letter documenting DOE's federal oversight activities and risk assessments (including both processes and the product itself) performed to date associated with Radcalc.

Sincerely,

Jessie H. Roberson
Vice Chairman

Enclosure

c: The Honorable Madelyn Creedon
Mr. Joe Olencz

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Staff Issue Report

December 17, 2014

MEMORANDUM FOR: S. A. Stokes, Technical Director

COPIES: Board Members

FROM: W. S. Horton

SUBJECT: Review of Federal Oversight of Software Quality Assurance for Radcalc

On October 16, 2014, members of the Defense Nuclear Facilities Safety Board's (Board) staff held an on-site review to assess Department of Energy (DOE) Office of Environmental Management (EM) compliance with federal Quality Assurance/Software Quality Assurance (QA/SQA) oversight requirements for the computer program Radcalc.

Radcalc is a custom-developed, web-based computer program used to determine the transportation package classification for radioactive materials, including radioactive waste, based on the isotopic content. (See *RADCALC—An Analytical Tool for Shippers of Radioactive Materials and Waste, Including Transuranic Waste-Transportation and Hydrogen Gas Determinations*—http://energy.gov/sites/prod/files/em/FactsheetRadcalc20100527.pdf.) There are over 400 registered users of Radcalc including radioactive material shippers across the nuclear industry including medical, commercial power, and the defense nuclear complex. EM federal and contractor personnel classified Radcalc as safety software and assigned Safety Classification Level B, the second highest level of rigor in SQA procedures. Typically at this safety classification level, a software failure could result in incorrect analysis of hazardous exposure to workers or the public or compromise the defense in depth of a safety system or component. In the case of Radcalc, an error in the selection of the appropriate waste package, calculation of decay heat, radioactivity, and/or hydrogen gas generation could result in serious consequences for workers and the public in the event of a transportation accident.

Personnel from the DOE Office of Packaging and Transportation (EM-33) manage Radcalc. On October 22, 2014, the staff review team completed discussions with EM-33 personnel. The discussions identified numerous and significant federal oversight deficiencies. The staff team determined that an additional review of Boston Government Services (BGS), the new contractor that manages the software for DOE, was needed to fully assess DOE's oversight of the computer program. Following the October discussions, the Office of Standards and Quality Assurance (EM-43) immediately scheduled a QA review of BGS. The staff review team observed the EM-43 review on November 4, 2014, and conducted a closeout meeting with DOE management covering all issues related to the federal oversight of Radcalc on November 20, 2014.

Background. EM-33 is the technical contracting office for Radcalc and Radtran. It has been responsible for these computer programs since the mid-1990s. Radtran is an additional custom-developed computer program used to analyze consequences and risks of radioactive material transportation. EM federal and contractor personnel also classified Radtran as safety software. The contract structure for the development and management of these computer programs is complicated and has recently changed. Initially, DOE issued a direct contract for the software work to Energy Solutions Federal Services. In the 2007–2008 timeframe, DOE changed the Radcalc contract to Project Enhancement Corporation, which then subcontracted back to Energy Solutions, with further subcontracting to Polestar Applied Technology and Shotz Expressions. For Radtran, EM established an arrangement with Sandia National Laboratories for the development and software management work. In August 2014, a new contractor, BGS, was selected to manage both computer programs.

The staff review team requested documents related to federal oversight and SQA for both computer programs. The staff review team received and reviewed the Radcalc SQA documents and compared them to the requirements of Title 10, Code of Federal Regulations, Part 830 (10 CFR 830) Subpart A, *Quality Assurance Requirements*; DOE Order 414.1D, *Quality Assurance*; and ASME NQA-1-2008, *Quality Assurance Requirements for Nuclear Facility Applications* (NQA-1). Because this software work is contracted by DOE-EM, the staff review team specifically assessed the methodology DOE-EM used to comply with the federal oversight responsibilities normally performed by the Field Element Manager/Site Manager.

Observations. The staff team's review shows that EM-33 personnel failed to comply with federal QA/SQA oversight requirements of DOE Order 226.1B, *Implementation of DOE Oversight Policy*. Further, DOE could not provide any evidence of federal oversight of these computer programs during the software's lifetime. The staff review team determined there were multiple safety issues associated directly with the federal oversight of Radcalc and four additional safety issues that could affect other safety software.

The following issues are examples of where DOE failed to ensure that the contractors managing Radcalc met the requirements of 10 CFR 830, DOE Order 414.1D, and ASME NQA-1-2008. These issues demonstrate that DOE failed to perform adequate federal oversight in accordance with the requirements of DOE Order 226.1B:

- The contractors failed to submit a Quality Assurance Plan (QAP) and safety software grading levels to DOE-EM personnel for review and approval. Thus, DOE-EM personnel did not oversee the contractors' QA/SQA program. Inadequate DOE oversight persisted for virtually the entire lifespan of the software.

- There is no evidence that the contractors reviewed computer program characteristics, software process implementation, and other quality-related information to identify software, services, and processes needing improvement.

- The contractors failed to establish and implement processes to ensure that approved suppliers continue to provide acceptable items and services. For example, DOE-EM

could not verify that all users of Radcalc are using the latest version of the computer program.

- The past contractors' approach to retire earlier versions of Radcalc did not ensure routine use was prevented and conflicted with the contractors' established procedures and practice.

- The DOE-EM personnel and EM contractors failed to adequately maintain Radcalc configuration management. During the October 22, 2014, review, DOE-EM personnel could not identify who was responsible for, and the location of, the source code for Radcalc version 4.1 (the latest version) or Radtran for over a year during the procurement activities to select a new contractor.

- The contractors' problem reporting and corrective action processes failed to promptly identify and correct conditions adverse to quality as soon as practicable. Further, in the case of a significant condition adverse to quality, the cause was not determined and there is no evidence that corrective actions were taken to preclude recurrence. The non-sequential and apparently random numbering of Problem Reports and Change Requests (PR/CR) indicates a loss of configuration management, as well as uncertainty in the correction of defects of the software and potentially unapproved and untested changes to the software. Multiple PR/CRs identified in 2009, 2010, and 2011 remain uncorrected. The staff review team noted the EM contractor classified PR/CR 78, identified in 2011, as a major problem. PR/CR 78 identified a significant error in the calculation algorithm for determining total and partial pressure of hydrogen, oxygen, and helium. The error in the algorithm remains uncorrected. A DOE software advisory notified users of the computer program to perform handwritten calculations to confirm computer program results for gas generation. DOE published another Radcalc Software Advisory on April 14, 2014, concerning Fissile Material Exceptions and International Shipments. The staff review team could not identify a PR/CR associated with this advisory. DOE-EM did not conduct surveillances of the contractors or the users to verify implementation of corrective actions including PR/CR 78.

- DOE-EM personnel failed to flow down the applicable QA/SQA requirements and responsibilities throughout all levels of the organization. Specific examples include: the contracting/subcontracting efforts omitted specific QA/SQA requirement documents (i.e., *EM Quality Assurance Program (QAP) EM-QA-001*, Rev. 0 and subsequently Rev. 1) and failed to specifically identify applicable portions of QA consensus standards in EM's standard contracting language to ensure software procurements include QA requirements. Further, only after EM personnel became aware of the staff review team's interest in these computer programs did they perform a QA assessment of BGS and direct the DOE-EM Consolidated Business Center to amend the August 2014 contract with BGS to include EM's standard contract language for QA. This could indicate a larger, potentially systemic, problem in the matrix organization of DOE-EM where the lack of interaction between project

managers, SQA experts, and contracting officials may result in some contracts not containing, and contractors not implementing, necessary requirements.

- DOE-EM failed to perform any audits, management assessments, or independent assessments involving Radcalc over the entire contracting lifespan of the software. Further, there is no evidence of any independent assessments—either by any DOE organization (e.g., Office of the Chief of Nuclear Safety), nor any organization outside DOE.

- DOE-EM personnel directly responsible for oversight of safety SQA activities are not qualified in accordance with DOE Standard 1172-2003, *Safety Software Quality Assurance Functional Area Qualification Standard.* This could indicate another larger, potentially systemic, problem in the matrix organization of DOE-EM where the lack of interaction between project managers, SQA experts, and contracting officials may result in unqualified personnel performing federal oversight, insufficient numbers of qualified personnel to perform the required amount of federal oversight, or both.

- There is no evidence that the designated DOE approval authority approved the contractors' selection and use of a consensus standard to acquire, develop, and implement the safety software QA program.

- The results of the staff-observed EM QA Assessment on November 4, 2014, show that the current Radcalc contractor, BGS, does not have a compliant NQA-1 program because the contractor's QA/SQA procedures are immature and insufficient.

The staff team's review identified four other observations that contributed to the above issues and may affect other safety software within DOE:

- There is an apparent lack of a systematic, structured, and documented approach to determine the number of qualified QA/SQA personnel needed to perform the federal oversight functions and comply with DOE's established QA/SQA oversight requirements. Based on this review and the observation of the EM QA review, the staff review team believes there are not enough qualified personnel performing SQA oversight at both DOE Headquarters and Field Offices. This weakness likely contributes to inadequate review of contractor QAPs, as well as the inability to ensure that SQA requirements flow down to all contractors and subcontractors.

- There is an apparent lack of a systematic, structured, and documented approach to determine which organization within DOE is responsible to perform QA audits of contractor organizations. During the review, different organizations within DOE stated that they thought another organization was responsible for performing Radcalc contractor QA audits. DOE procedures do not clearly delineate which organization is responsible for QA/SQA audits and assessments. That organization would also be responsible to train and qualify those DOE personnel to applicable DOE standards.

- DOE lacks policies and procedures to resolve and clarify the difference between the ownership of a work product, in this case software, and the government's rights to use the work product. The staff review team believes that the uncertainties of ownership and government rights associated with Radcalc are likely large contributors to the inadequate federal oversight of the software work.

- Members of the Board's staff also submitted an information request to DOE-EM for SQA documentation regarding Radtran. On December 3, 2014, the staff review team received a response from EM-33 personnel that they could not find a specific SQA Plan for Radtran, nor had they ever reviewed Radtran for compliance with SQA requirements since taking ownership of the computer program in 2011. Thus, it has similar federal oversight concerns as Radcalc. The Board's staff review team's issues and observations associated with Radcalc in this review and the lack of information concerning the SQA compliance of Radtran suggest that other computer programs managed by other organizations within DOE Headquarters may have similar SQA deficiencies.

Conclusions. The results of this review show a lack of federal oversight of the Radcalc safety software work. The failures in problem reporting and corrective action, inadequate flow down of SQA requirements to the lowest subcontractor, failure to maintain software configuration change control and retire previous software versions, and failure to conduct assessments of the computer program challenge the reasonable assurance of the reliability of Radcalc's results. Because the contracts with the previous contractors have expired, and the available documentation provides an incomplete picture of the past SQA program, this review was unable to assess the compliance and effectiveness of the previous contractors' QA/SQA programs. However, on November 4, 2014, the staff review team shadowed an EM certification assessment of the new contractor, BGS, which currently maintains the Radcalc source code. The EM assessment team and the staff review team identified that BGS does not have an NQA-1 compliant program. The staff review team is closely following the completion of the assessment report process to ensure DOE takes adequate corrective actions for any identified deficiencies in the report. Together, these numerous identified and unaddressed SQA deficiencies indicate compliance and implementation insufficiencies in the QA/SQA programs for BGS and the previous contractors.

In addition, this review identified potentially significant systemic concerns that could affect other safety software. These are: inadequate QA/SQA requirement specification in DOE contracts and the lack of policy identifying the DOE organizations in charge of performing QA assessments to ensure compliance; unqualified and/or inadequate numbers of qualified federal personnel to oversee contract work; absence of policy and procedures to resolve ownership and government rights for quality-related software; and additional instances of inadequate oversight of computer work within DOE (e.g., Radtran).

The staff team's review of the oversight of Radcalc prompted the DOE Office of Standards and Quality Assurance (EM-43) to review the new contract and contractor's QA/SQA program implementation associated with these EM-33 computer programs. During the closeout

meeting conducted on November 20, 2014, DOE-EM personnel acknowledged the staff review team's analysis of the inadequacy of SQA oversight.