DEFENSE NUCLEAR FACILITIES SAFETY BOARD
Washington, DC 20004-2901

January 31, 2025

The Honorable Ingrid Kolb
Acting Secretary of Energy
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

Dear Ms. Kolb:

The Defense Nuclear Facilities Safety Board (Board) has consistently emphasized to the Department of Energy (DOE) the importance of robust quality assurance programs in ensuring the reliability of safety structures, systems, and components (SSC), and safety software at defense nuclear facilities. DOE's approach to quality assurance for safety software was significantly improved by its completion of the implementation plan for Board Recommendation 2002-1, *Quality Assurance for Safety-Related Software*. This plan led to substantial improvements to DOE Order 414.1, *Quality Assurance*, by incorporating essential requirements, best practices, and lessons learned.

Recently, DOE initiated a revision to DOE Order 414.1 and shared proposed drafts with the Board. The Board's staff engaged with DOE's writing team, providing comments on successive drafts of the order. Although DOE has addressed many of the Board's comments, the Board remains concerned about two safety-related issues: 1) the removal of the term safety software and its associated requirements, and 2) the elimination of the mandated use of the American Society of Mechanical Engineers' (ASME) national consensus standard NQA-1, *Quality Assurance Requirements for Nuclear Facility Applications*.

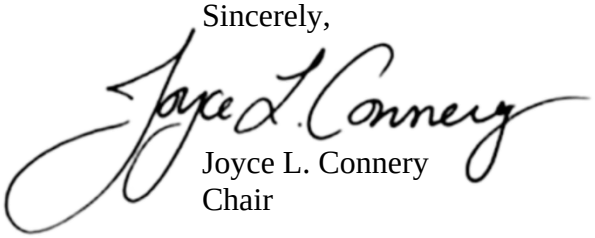
The Board believes that maintaining safety software requirements and the use of NQA-1 are fundamental to DOE's nuclear safety framework. Removing these requirements may lead to reduced reliability of SSCs vital to safety at defense nuclear facilities.

The Board understands the DOE Order 414.1 revision has been approved and issued. However, the Board is concerned that the proposed changes will weaken quality assurance for safety SSCs and safety software vital to defense nuclear facilities. The elimination of established requirements will also increase the oversight burden on field offices, adding unnecessary complexity and safety risk.

The enclosure provides additional details on the Board's review of the draft order, offering insights to assist DOE in enhancing its quality assurance programs. The Board encourages DOE to apply lessons learned since the implementation of Recommendation 2002-1

to strengthen its safety oversight capabilities and ensure continued use of NQA-1 at defense nuclear facilities. The Board will continue to evaluate the use of quality assurance standards at defense nuclear facilities.

Sincerely,



Joyce L. Connery
Chair

Enclosure

c: Ms. Teresa Robbins, Acting Administrator, National Nuclear Security Administration
Ms. Candice Robertson, Senior Advisor, DOE Office of Environmental Management
Mr. Todd Lapointe, Director, DOE Office of Environment, Health, Safety and Security
Mr. Joe Olencz, Director, Office of the Departmental Representative to the Board

ENCLOSURE

Review of Proposed Changes to Department of Energy (DOE) Order 414.1, *Quality Assurance*

Background. In Defense Nuclear Facilities Safety Board (Board) Recommendation 2002-1, *Quality Assurance for Safety-Related Software*, the Board recommended that DOE take prompt actions to improve quality assurance for safety software including proposed changes to the DOE directives system [1]. The DOE implementation plan, in response to Recommendation 2002-1, led to significant improvements in DOE Order 414.1, *Quality Assurance*, to define and identify requirements for safety software. The Board has also continued to encourage DOE to implement an appropriate quality assurance national consensus standard for its defense nuclear facilities. The Board has frequently communicated with DOE on quality assurance issues at defense nuclear facilities [2, 3, 4, 5, 6, 7, 8].

The Board's staff team has been closely following DOE's revision to DOE Order 414.1. In the current draft revision to the quality assurance order, DOE has removed specific safety software requirements and definitions. Additionally, DOE revised the order to remove the mandated use of the American Society of Mechanical Engineers' (ASME) national consensus standard NQA-1, *Quality Assurance Requirements for Nuclear Facility Applications*, for high hazard nuclear facilities, relying rather on the field office managers to ensure the appropriate standard is used for these facilities.

Title 10, Code of Federal Regulations, Part 830 (10 CFR 830), includes two important subparts that provide the pillars for DOE's safety framework for defense nuclear facilities: (1) Subpart A for quality assurance requirements, and (2) Subpart B for safety basis requirements. Subpart B ensures that hazards are identified and analyzed, and hazard controls are established to protect the public and workers at defense nuclear facilities. Hazard controls typically include safety structures, systems, and components (SSC), and may involve use of safety software. Subpart A ensures quality assurance standards are applied so that the selected hazard controls can perform their safety function. Subpart A requires the contractor responsible for a DOE nuclear facility to "Use voluntary consensus standards in [Quality Assurance Program] development and implementation." For defense nuclear facilities, DOE must select appropriate quality assurance consensus standards to provide confidence that safety SSCs, and safety software will reliably perform their safety function.

Discussion. The Board has identified the following safety concerns with DOE's proposed revision to DOE Order 414.1.

Deletion of Safety Software Requirements and Definitions—DOE has removed the term safety software, and associated safety software requirements from the draft order. Instead, the draft order contains quality assurance requirements for all software and requires the development of a graded approach document. However, the draft order does not provide clarity about requirements that would apply for software used in nuclear safety applications. Removal of safety software requirements from the order could lead to less rigor in developing, evaluating, and implementing software important to nuclear safety. If DOE relies on a graded approach to

appropriately categorize and implement software quality assurance without defining or providing guidance for software used in safety applications, the results may not ensure the necessary reliability for nuclear safety applications. Recent and previous staff reviews, as well as DOE's internal reviews, have shown that DOE sites have not been identifying and grading safety software appropriately [2, 7, 8, 9, 10, 11]. Removal of safety software requirements from the order may result in more of these types of grading errors and reduced reliability of software important to safety.

Removal of the Mandated Use of NQA-1—The current version of DOE Order 414.1 invokes NQA-1 for "new Hazard Category 1, 2, and 3 nuclear facilities, major modifications, and safety software at these facilities." In the proposed revision, DOE has not invoked a specific quality assurance standard in these cases but has identified NQA-1 as the "preferred" standard. Additionally, the draft order removed the requirement to document an equivalency evaluation when a contractor selects a consensus standard other than NQA-1. Not invoking NQA-1 and ensuring the selected standard provides an equivalent level of quality assurance could lead to the selection of weaker and less prescriptive standards for safety SSCs and safety software, which may adversely affect reliability.

The staff team is concerned that without invoking specific standards that are acceptable, contractors may not select an appropriate standard for nuclear safety applications. Lack of an invoked quality assurance standard for nuclear facilities may undermine the safety framework provided by 10 CFR 830 and lead to reduced reliability of SSCs vital to safety at defense nuclear facilities.

DOE Oversight of Quality Assurance—DOE's proposed changes will also increase the burden on field office personnel to perform oversight of DOE contractors in grading safety software and selecting appropriate quality assurance standards for nuclear applications. Board reviews in this area indicate that DOE field offices may not have an adequate number of subject matter experts to expand their oversight role in this area because several opportunities to appropriately grade safety software have been missed in the field.

As an illustration of the Board concerns with DOE oversight, the Board identified several software quality assurance (SQA) issues at the Lawrence Livermore National Laboratory (LLNL) [9]. In this case, the field office approved a quality assurance plan with exemptions that allowed software to be exempted from SQA requirements. In addition, a federal readiness assessment identified several post-start findings related to SQA at LLNL including the LLNL contractor failing to perform required verification and validation tests and not meeting requirements of applicable SQA consensus standards [10]. In 2016, the Board's staff reviewed the criticality assembly machines at the National Criticality Experiments Research Center and identified a failure to appropriately classify safety software in accordance with DOE Order 414.1D. DOE Office of Enterprise Assessments and National Nuclear Security Administration reports also substantiated several elements of the staff's concerns related to contractors not selecting an appropriate consensus standard and properly grading safety software [9, 10, 13, 14].

Conclusion. DOE should strengthen requirements and provide clear guidance to ensure safety software is properly identified and that appropriate quality assurance measures are

consistently applied. Additionally, DOE should ensure sites use NQA-1 as the quality assurance standard for defense nuclear facilities to ensure that safety SSCs and safety software reliably perform their safety functions. Finally, in light of DOE's proposed changes to DOE Order 414.1 and recurring issues identified by the Board and DOE at various sites, DOE should enhance its oversight of nuclear-related consensus standard and safety software quality assurance at defense nuclear facilities.

References

1. Defense Nuclear Facilities Safety Board Recommendation 2002-1, *Quality Assurance for Safety-Related Software,* September 23, 2002.

2. Defense Nuclear Facilities Safety Board, *Letter from Chair Joyce L Connery to Honorable Jill Hruby, Lawrence Livermore National Laboratory Software Quality Assurance*, January 5, 2024.

3. Defense Nuclear Facilities Safety Board, *Letter from Chair Joyce L Connery to Honorable Jill Hruby, Safety Software Central Registry,* August 24, 2022.

4. Defense Nuclear Facilities Safety Board, *Letter from Chair Bruce Hamilton to Honorable Dan Brouillette, Quality Assurance of Structural Repairs at Pantex Plant,* August 6, 2020.

5. Defense Nuclear Facilities Safety Board, *Letter from Chair Bruce Hamilton to Honorable James Richard Perry, Pantex Special Tooling Program*, October 17, 2018.

6. Defense Nuclear Facilities Safety Board, *Letter from Chair Joyce L Connery to Dr. Monica Regalbuto, Quality Assurance Review of Waste Treatment and Immobilization Plant Project,* April 4, 2016.

7. Defense Nuclear Facilities Safety Board, *Letter from Vice Chair Jessie H. Roberson to Mr. David M. Klaus, DOE's Federal Oversight Activities and Risk Assessments Associated with the Computer Program "Radcalc"*, March 16, 2015.

8. Defense Nuclear Facilities Safety Board, *Letter from Chair Peter S. Winokur to Honorable Donald L. Cook, Quality Assurance and Software Quality Assurance Issues at the Annular Core Research Reactor at Sandia National Laboratories*, April 18, 2012.

9. National Nuclear Security Administration, *Summary Report for the Sandia, Los Alamos, and Lawrence Livermore Safety Software Quality Assurance Weapon Response Code NA-SH-60,* August 2016.

10. National Nuclear Security Administration, *Lawrence Livermore National Laboratory – Pantex (CASTLE-PX) Safety Software Quality Assurance Final Report*, October 24, 2017.

11. Department of Energy, Office of Enterprise Assessments, *Independent Assessment of Software Quality Assurance Program Implementation at the Nevada National Security Sites*, November 2023.

12. Department of Energy, *Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2002-1*, March 13, 2003.

13. National Nuclear Security Administration, *Final Report for the Federal Readiness Assessment Hydrogen Gas System/Metal Conversion Glovebox*, May 18, 2023.

14. Department of Energy, Office of Enterprise Assessments, *Independent Assessment of the Management of Safety Issues at the Lawrence Livermore National Laboratory*, April 2023.