Independent Assessment of Software Quality Assurance Program Implementation at the Pacific Northwest National Laboratory

October 2023

Office of Enterprise Assessments
U.S. Department of Energy

Table of Contents

Acronyms

1QP	One Quality Program
BMI	Battelle Memorial Institute
CFR	Code of Federal Regulations
CRAD	Criteria and Review Approach Document
DOE	U.S. Department of Energy
EA	Office of Enterprise Assessments
HDI	How Do I…?
NQAP	Nuclear Quality Assurance Program
OFI	Opportunity for Improvement
OSS	Office of Safety and Security
PEMP	Performance Evaluation Measurement Plan
PNNL	Pacific Northwest National Laboratory
PNSO	Pacific Northwest Site Office
Q5	Quality Grade 5
QAP	Quality Assurance Program
QMPD	Quality Management – Management & Operating Program Description
SQA	Software Quality Assurance
SWQA	Software Quality Assistant

INDEPENDENT ASSESSMENT OF SOFTWARE QUALITY ASSURANCE PROGRAM IMPLEMENTATION AT THE PACIFIC NORTHWEST NATIONAL LABORATORY

Executive Summary

The U.S. Department of Energy (DOE) Office of Enterprise Assessments (EA) conducted an independent assessment of software quality assurance (SQA) program implementation at the Pacific Northwest National Laboratory (PNNL) from March to April 2023. The purpose of this assessment was to evaluate the performance of the Battelle Memorial Institute (BMI) SQA program. This assessment also evaluated the effectiveness of the DOE Office of Science Pacific Northwest Site Office (PNSO) in providing oversight of the SQA program.

EA identified the following strengths, including a best practice:

- BMI identifies a non-nuclear safety software risk level category/grade. This practice enhances the process for implementing controls commensurate with an identified risk. (Best Practice)
- BMI has initiated and is following through with its "One Quality Program" initiative, which will combine its many quality programs into one and bring better alignment across PNNL.
- PNSO and DOE program sponsored oversight have identified, and BMI has self-identified, several SQA issues for which corrective actions are actively being addressed.
- PNSO is using the performance evaluation measurement plan to incentivize successful completion of the "One Quality Program" initiative and the implementation of the NQA-1-2019 standard.

EA also identified several weaknesses, as summarized below:

- BMI has not adequately developed and submitted the complete PNNL quality assurance program (QAP) to PNSO for review and approval.
- BMI does not specify the minimum training and qualification requirements for using all non-safety software.
- PNSO has not formally reviewed elements of the PNNL QAP that apply to implementation of the SQA program and its underlying graded approach.

In summary, BMI has implemented an adequate SQA program at PNNL, and in general, PNSO has conducted adequate oversight. Both safety and non-safety software are managed through processes that provide reasonable assurance of software quality that supports nuclear safety at the laboratory. However, several weaknesses identified by EA during this assessment, and identified by the contractor, DOE program sponsors, and PNSO prior to this assessment, document needed improvements of the SQA program. Allowing these weaknesses to go unresolved and/or unevaluated leaves PNNL vulnerable to unanticipated issues, the risk of which cannot easily be quantified. Until all current corrective actions are completed and the weaknesses identified in this report are addressed, or effective mitigations are put in place, software quality at PNNL will not be optimal.

INDEPENDENT ASSESSMENT OF SOFTWARE QUALITY ASSURANCE PROGRAM IMPLEMENTATION AT THE PACIFIC NORTHWEST NATIONAL LABORATORY

1.0 INTRODUCTION

The U.S. Department of Energy (DOE) Office of Nuclear Engineering and Safety Basis Assessments, within the independent Office of Enterprise Assessments (EA), conducted an assessment of software quality assurance (SQA) program implementation at the Pacific Northwest National Laboratory (PNNL). The purpose of this assessment was to evaluate the SQA program implemented by the primary site contractor, Battelle Memorial Institute (BMI). This assessment also evaluated the effectiveness of the DOE Office of Science Pacific Northwest Site Office (PNSO) in providing oversight of the SQA program.

This assessment was performed consistent with *EA Plan for Phase 2 of the Enterprise-wide Independent Assessment of Software Quality Assurance Process Implementation, January 2023*, which describes the second phase of a two-phased, enterprise-wide, targeted assessment of SQA processes. The first phase of this targeted assessment process examined and analyzed the design of SQA programs implemented throughout the DOE enterprise and helped to identify general, complex-wide strengths and weakness. In addition, the first phase helped inform the development of the EA plan to conduct assessments of SQA program implementation. Accordingly, this second phase assessment evaluated SQA program implementation by examining BMI SQA processes. The assessment evaluated a sample of both safety and non-safety software, software that has been assigned varying grading levels, and software that is implemented for a variety of functions (e.g., nuclear and radiological safety analyses, administrative activities).

2.0 METHODOLOGY

The DOE independent oversight program is described in and governed by DOE Order 227.1A, *Independent Oversight Program*, which EA implements through a comprehensive set of internal protocols, operating practices, assessment guides, and process guides. This report uses the terms "best practices, deficiencies, findings, and opportunities for improvement (OFIs)" as defined in the order.

As identified in the assessment plan, this assessment considered requirements related to software, as presented in 10 CFR 830, subpart A, *Quality Assurance Requirements*, and DOE Order 414.1D, *Quality Assurance*, and applicable consensus standards (i.e., NQA-1, *Quality Assurance Requirements for Nuclear Facility Applications*). EA used EA CRAD 30-10, Revision 0, *Software Quality Assurance*, to guide this assessment.

EA examined key documents, such as program plans and descriptions, implementing procedures, software lifecycle management documentation, assessment reports, corrective action plans, and training and qualification records. EA also interviewed key personnel responsible for developing and executing the associated programs and observed meetings and activities that support SQA program implementation. The members of the assessment team, the Quality Review Board, and the management responsible for this assessment are listed in appendix A.

There were no previous findings for follow-up addressed during this assessment.

3.0 RESULTS

3.1 Quality Assurance Program

This portion of the assessment evaluated the contractor's quality assurance program (QAP) for safety and non-safety software.

Safety Software

BMI has established a generally adequate PNNL QAP for safety software, as described in the DOE-approved document *Quality Management – Management & Operating Program Description* (QMPD) (no document number). The PNNL QMPD adequately describes implementation of various versions of the American Society of Mechanical Engineers national consensus standard NQA-1, *Quality Assurance Requirements for Nuclear Facility Applications*, and meets quality requirements in accordance with 10 CFR 830, *Nuclear Safety Management*, subpart A, *Quality Assurance Requirements*, and DOE Order 414.1D, attachment 2, *Quality Assurance Criteria*, and attachment 4, *Safety Software Quality Assurance Requirements for Nuclear Facilities*.

BMI maintains adequate institutional quality assurance implementing procedures through the "How Do I…?" (HDI) web-based management system for work activities governed by the QMPD. In addition to the HDI system, BMI maintains other implementing procedures, which are based on program- or project-specific QAP documents for safety software; address project planning, requirements specifications, design, procurement, verification and validation, and configuration management; and provide for appropriate involvement of the facility design authority, as applicable. In combination with the QMPD, the implementing procedures require the assignment of grading levels to all safety software based on a defined graded approach for applying SQA requirements. In addition to the nuclear safety software risk levels A, B, and C in the QMPD, NQAP-0302, *Software Grading*, appropriately defines a risk level D for non-nuclear safety software. Risk level D software is software that contributes to the control of radiological, biological, chemical, or physical hazards defined by the PNNL integrated safety management system hazard analysis process and does not meet the definitions for risk levels A through C. Identifying this non-nuclear safety software category is cited as a **Best Practice** because it enhances the graded approach process for implementing controls commensurate with specific identified risks.

Use of the DOE Software Central Registry toolbox codes are appropriately subjected to the PNNL SQA processes. Further, BMI employs a cadre of three trained and qualified subject matter experts, using Q-0202-QAL-4, *Certification of Software Quality Practitioner Personnel,* to establish, maintain, and ensure an effective program. Their involvement is appropriately required for PNNL work activities that involve nuclear safety software and non-nuclear safety software.

BMI submitted the QMPD, which describes the PNNL QAP, to PNSO for review and approval in a timely manner; however, the QMPD does not fully address all required quality assurance elements or the graded approach for all work. The QMPD is based on NQA-1-2000 and implemented through the HDI system; however, it only identifies nuclear safety software grading levels. There are other documents not submitted for PNSO approval that identify additional SQA-related implementing procedures to be used in conjunction with the HDI system. For example, BMI did not submit the following documents to PNSO for review:

- NQAP-2012, *Nuclear Quality Assurance Program (NQAP) Manual*, which is based on NQA-1-2012, is for projects requiring more rigor than the QMPD, and identifies a non-nuclear safety software grading level and non-safety software grading levels.
- RPL-PLN-801, *RPL Quality Assurance Program Description (QAPD)*, based on NQA-1-2015, for the 325 Building Radiochemical Processing Laboratory.

- TRIT-Q-MAN-001, *Tritium Technology Program Quality Assurance Manual*, based on NQA-1-2015, for the Tritium Technology Program subject to 10 CFR 50, *Domestic Licensing of Production and Utilization Facilities*, appendix B, *Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants*.

Consequently, PNSO did not review these and other documents that identify and describe important components of the PNNL QAP. Contrary to DOE Order 414.1D, attachment 1, sections 1 and 2, BMI has not submitted the complete PNNL QAP to PNSO for review and approval. (See **Deficiency D-BMI-1**.) Without providing all QAP documents, field element oversight cannot ensure adequate QAP development and implementation.

BMI's use of multiple systems to identify and present QAP implementing procedures introduces unnecessary complexity and opportunities for confusion and error, as previously self-identified. Program-specific QAP documents are required to meet or exceed the HDI system requirements, and differences are required to be reviewed when a change is made to either program to ensure the more conservative requirement is being met. For example, per the document revision history, recent revisions of NQAP-2012 included appropriate clarification regarding which work activities are covered by the NQAP document and which by the HDI system procedures. The One Quality Program (1QP) initiative has been established to bring the PNNL QA programs under one consensus standard, NQA-1-2019, and clarify the QAP structure, which would improve the program.

Similarly, BMI's use of two software inventories, the Software Quality Assistant (SWQA) inventory of active safety software and the TechDirectory inventory of all software, has resulted in conflicting information. (See **OFI-BMI-1**.) For example, the implementation status for the RadCalc 4.1 software did not match between the two inventories. When brought to the attention of BMI, they resolved the conflict. However, contrary to DOE Order 414.1D, attachment 2, section 3.b, software-related errors that do not directly affect the software, such as inventory errors, are not included in, and correct by the PNNL issues tracking and trending processes. (See **Deficiency D-BMI-2**.) Not tracking minor errors inhibits the ability to trend issues and identify potential systemic problems. In addition, RadCalc 4.1 is listed in the software inventory as inactive and is not in use at PNNL. However, BMI has not updated the acquisition documentation to address the known quality issues identified in the DOE safety advisories issued between 2011 and 2015. (See **OFI-BMI-2**.)

BMI has initiated the 1QP initiative to, in part, enhance the connections and consistency between the SQA processes implemented throughout PNNL. BMI states that the purpose of the 1QP is to address a legacy of decentralized quality management, which has led to several quality programs being written and maintained by individual projects or organizations, the adoption of various NQA-1 editions, duplication of processes, and inconsistent approaches to conducting similar work activities. BMI appropriately began familiarity training on the 1QP with the quality engineering staff before implementing changes to processes and procedures. BMI notes that some of its work activities are excluded from the QAP controls. The *1QP Framework for Quality Engineers* [undated] defines Quality Grade 5 (Q5) as items and services that expend resources but have no quality consideration and therefore no QAP requirements. The presentation includes a Q5 example of procurement of office supplies that do not affect the technical adequacy of deliverables and treated as though they are not subject to any controls. However, the PNNL QAP requires that all procurements are subject to some level of control. (See **OFI-BMI-3**.)

Non-Safety Software

BMI has established a generally adequate QAP for non-safety software that meets the requirements of DOE Order 414.1D, attachment 2, through the HDI system and NQAP-2012 implementing procedures. The graded approach that is described in NQAP-2012 identifies two non-safety software levels: E, for non-safety delivered software (i.e., software developed at PNNL as a deliverable for an external client),

and F, for non-safety software used within PNNL. However, as discussed above, the NQAP-2012 implementing procedure was not submitted to PNSO for review and approval. Contrary to DOE Order 414.1D, attachment 1, sections 1.a and 2, BMI did not submit a graded approach for non-safety software in the documentation submitted to PNSO for review and approval. (See **Deficiency D-BMI-1**.) Omitting documentation that completes the description of the software graded approach in the submittal limits PNSO to a partial review.

Quality Assurance Program Conclusions

BMI has established an adequate PNNL QAP for safety software and non-safety software through multiple documents based on various versions of NQA-1. BMI maintains adequate QAP implementing procedures through the web-based HDI system for work activities governed by the QMPD. BMI also enhances its process for implementing controls commensurate with identified risks by identifying a non-nuclear category of safety software. However, BMI has not submitted a complete PNNL QAP or a graded approach for non-safety software to PNSO for review and approval. Additionally, the BMI processes for maintaining implementing procedures and software inventories have duplication that adds unnecessary complexity.

3.2 Software Quality Assurance Program Implementation

This portion of the assessment evaluated BMI implementation of, and adherence to, SQA program procedures for safety software and non-safety software.

Safety Software

For this assessment, EA reviewed SQA program implementation for the following safety software applications:

- Radioactive Materials Tracking
- Utility Calc - NNSA 3 tier evaluation
- MCNP, version 6.1.0
- MCNP, version 6.2
- MCNP, version MCNV6
- MCNP, version 6.0
- RadCalc 69640
- Sentinel
- RadCalc

BMI personnel adequately adhere to applicable SQA requirements in the development and use of nine sampled safety software applications. The software development plans were appropriately approved and distributed and include a roles and responsibilities matrix, which clearly defines project assignments. The requirements specifications adequately address the software function and performance methodology. The software documentation adequately described the overall architecture and workflow based on an SQA-approved process methodology. Software data collection was appropriately gathered, measured, and analyzed per SQA requirements. BMI's documented risk analysis for the reviewed software documentation demonstrates effective mitigation of potential loss of data or functionality. Reviewed documentation showed that testing was performed during each stage of the development workflow and appropriately included peer reviews and audits. The reviewed software application user training documentation demonstrates appropriate training of users aligned with their assigned roles.

Non-Safety Software

For this assessment, EA reviewed SQA program implementation for the following non-safety software applications:

- Primavera
- Microsoft Windows
- Microsoft Excel

BMI has established an adequate QAP for non-safety software with a graded approach to identify non-safety software subject to quality controls in accordance with DOE Order 414.1D, attachment 2. The reviewed risk analysis process demonstrated effective mitigation of potential loss of data or functionality. The reviewed training records generally demonstrated appropriate training and qualification of personnel acquiring, maintaining, using, and assessing non-safety software applications. However, contrary to DOE Order 414.1D, attachment 2, sections 2.a and 2.b, BMI has not specified training requirements for non-safety software applications Microsoft Windows and Microsoft Excel. (See **Deficiency D-BMI-3**.) By not specifying such requirements for personnel training, BMI cannot ensure the proper use of these software applications.

Software Quality Assurance Program Implementation Conclusions

BMI adequately adheres to software quality procedures per the DOE-approved document *Quality Management – Management & Operating Program Description* (QMPD) (no document number) and is generally effective in managing the reviewed safety and non-safety software applications. However, BMI has not specified effective training requirements for personnel in the reviewed non-safety software applications.

3.3 Software Security

This portion of the assessment evaluated BMI processes to ensure the security of safety and non-safety software managed under the implemented SQA program.

BMI adequately ensures the security of safety and non-safety software through its SQA program, in accordance with applicable requirements. *PNNL Secure Software Controls Reference Policy* adequately addresses responsibilities for cybersecurity. BMI uses a defined process, *Cyber Security Management and Operations Program Description*, for appropriate review and approval of software security controls. Reviewed documentation for 12 software applications appropriately addressed access controls, where necessary. As an example of internal review, RadAnalysis-PMP-001, *RadAnalysis Development and Maintenance Project Management Plan*, Revision 3, provides a comprehensive analysis, review, and approval of the RadCalc software application (safety software). RadAnalysis-PMP-001 documents controls meant to effectively address the security of software on computer systems and networks, adequately ensuring that hardware, software, and electronic data is protected from cyber and phishing attacks by using access credentials and anti-phishing controls, as appropriate. Final SQA program approval, which addresses the security of the RadCalc software, is appropriately documented in RadAnalysis-PMP-001.

Software Security Conclusions

BMI adequately ensures the security of safety and non-safety software managed under its SQA program. To accomplish this, the program adequately implements comprehensive procedures that flow down applicable security requirements. The software security procedures and documentation are comprehensive and adequately conveyed.

3.4 Federal Oversight

This portion of the assessment evaluated PNSO oversight of the contractor SQA program.

PNSO has established a generally adequate SQA oversight program. PNSO reviewed and approved the QMPD for some PNNL work activities, relying on DOE program sponsor approval and oversight of other activities. Based on a reviewed sample of assessments, PNSO appropriately plans, performs, and documents assessments and follows up on issues and corrective actions in accordance with PNSO-PCDR-02, *PNSO Oversight Program Procedure*. One Office of Science, Office of Safety and Security (OSS) software quality assurance subject matter expert supports PNSO oversight operations and is assigned, adequately trained, and qualified to DOE-STD-1172, *Safety Software Quality Assurance Functional Area Qualification Standard*. PNSO is using the Fiscal Year 2022 Performance Evaluation Measurement Plan (PEMP) notable 6.4.2 and Fiscal Year 2023 PEMP notable 6.4.1 to incentivize successful completion of the 1QP initiative and implementation of the NQA-1-2019 standard. The PNSO QA Lead is also the DOE Enforcement Coordinator for actions pursuant to the contractor self-reported non-compliance NTS-SC-PNSO-BMI-PNNLBOPER-2023-0010565, which is also related to the issues identified during an assessment by the DOE Office of Environmental Management regarding the quality performance of the RadAnalysis software development project to replace RadCalc 4.1. This will help to provide another potential level of assurance in awareness and follow through on corrective actions.

While PNSO has established a generally adequate SQA oversight program, contrary to DOE Order 414.1D, sections 5.c.(2) and 5.c.(7), PNSO has not fully reviewed the PNNL QAP as applicable to implementation of the SQA program. (See **Deficiency D-PNSO-1**.) Without reviewing the complete QAP framework, PNSO cannot ensure the appropriateness of SQA program requirements for all PNNL work activities. Specifically, PNSO did not review SQA program documents that apply to PNNL work activities requiring more rigor than covered in the QMPD, nor did PNSO review the BMI graded approach, as described in NQAP-2012 (see section 3.1 of this report).

PNSO has no staff qualified to the DOE-STD-1172 qualification standard and relies upon OSS support for SQA-specific oversight. In addition, only one individual is qualified to DOE-STD-1150, *Quality Assurance Functional Area Qualification Standard*. (See **OFI-PNSO-1**.)

Assessment A-18-PNSO-PNNL-003, *Functional Area Review, Safety Software Quality Assurance (SSQA) Assessment*, was performed in 2018 and identified several of the weaknesses identified during this assessment. Specifically, assessment A-18-PNSO-PNNL-003 recommended implementation of a single NQA-1 revision by PNNL to reduce overhead and oversight; identified weaknesses with having two software inventories; and identified that there was no indication that NQAP-2012 was reviewed by PNSO as part of the QAP review and approval process. Since the assessment was performed, NQAP-2012 has been revised five times without further review by PNSO. In addition, lack of follow-up for the weakness with having two software inventories resulted in EA identifying the same weakness. (See **OFI-PNSO-2**.)

Federal Oversight Conclusions

PNSO has established a generally adequate SQA oversight program. PNSO reviewed and approved the PNNL QMPD for some PNNL work activities. PNSO appropriately plans, performs, and documents assessments and follows up on issues and corrective actions in accordance with documented procedures. PNSO also appropriately uses the PEMP process to incentivize successful implementation of the laboratory's NQA-1-2019 based 1QP initiative. However, PNSO has not fully reviewed and approved the PNNL graded approach and QAP documentation for work activities requiring more rigor than the QMPD. In addition, PNSO has not identified a need for qualified, expert SQA staff and instead relies on OSS support for SQA oversight. Also, some PNNL SQA program issues persist despite being identified years ago.

4.0 BEST PRACTICES

Best practices are safety-related practices, techniques, processes, or program attributes observed during an assessment that may merit consideration by other DOE and contractor organizations for implementation. The following best practice was identified as part of this assessment:

- BMI identifies a non-nuclear safety software risk level category/grade for facility radiological, biological, chemical, or physical hazards. This practice enhances the process for implementing controls commensurate with an identified risk.

5.0 FINDINGS

No findings were identified during this assessment.

6.0 DEFICIENCIES

Deficiencies are inadequacies in the implementation of an applicable requirement or standard. Deficiencies that did not meet the criteria for findings are listed below, with the expectation from DOE Order 227.1A for site managers to apply their local issues management processes for resolution.

Battelle Memorial Institute

Deficiency D-BMI-1: BMI submitted a PNNL QAP to PNSO for review and approval that does not include a description of all required QAP elements or a graded approach that applies to both safety and non-safety software. (DOE Order 414.1D, att. 1, secs. 1 and 2)

Deficiency D-BMI-2: BMI does include software-related errors not tracked through the software change control process in the institutional quality assurance issues tracking and trending processes. (DOE Order 414.1D, att. 2, sec. 3.b)

Deficiency D-BMI-3: BMI does not specify the minimum training and qualification requirements needed for the use of all non-safety software. (DOE Order 414.1D, att. 2, sec. 2)

Pacific Northwest Site Office

Deficiency D-PNSO-1: PNSO has not formally reviewed and approved all elements of the PNNL QAP as applied to implementation of the SQA program and its underlying graded approach. (DOE Order 414.1D, secs. 5.c.(2) and 5.c.(7))

7.0 OPPORTUNITIES FOR IMPROVEMENT

EA identified the OFIs shown below to assist cognizant managers in improving programs and operations. While OFIs may identify potential solutions to findings and deficiencies identified in assessment reports, they may also address other conditions observed during the assessment process. These OFIs are offered only as recommendations for line management consideration; they do not require formal resolution by management through a corrective action process and are not intended to be prescriptive or mandatory. Rather, they are suggestions that may assist site management in implementing best practices or provide potential solutions to issues identified during the assessment.

Battelle Memorial Institute

OFI-BMI-1: Consider consolidating the SWQA and TechDirectory inventory databases and functions.

OFI-BMI-2: Consider updating acquisitions-related documentation for all software to include documentation of any known quality issues and why continued use of the software is justified.

OFI-BMI-3: Consider revising the 1QP framework presentation and other documentation to appropriately identify the level of quality assurance controls applicable to Q5 level work, items, and services.

Pacific Northwest Site Office

OFI-PNSO-1: Consider having Federal staff qualified to DOE-STD-1172 and increasing the number of staff qualified to DOE-STD-1150.

OFI-PNSO-2: Consider enhancing field element processes for (1) reviewing and approving the PNNL QAP, and (2) SQA program issues management tracking.

Appendix A
Supplemental Information

Dates of Assessment

Offsite Assessment: March – April 2023

Office of Enterprise Assessments (EA) Management

John E. Dupuy, Director, Office of Enterprise Assessments
William F. West, Deputy Director, Office of Enterprise Assessments
Kevin G. Kilp, Director, Office of Environment, Safety and Health Assessments
David A. Young, Deputy Director, Office of Environment, Safety and Health Assessments
Thomas E. Sowinski, Director, Office of Nuclear Safety and Environmental Assessments
Kimberly G. Nelson, Director, Office of Worker Safety and Health Assessments
Jack E. Winston, Director, Office of Emergency Management Assessments
Brent L. Jones, Director, Office of Nuclear Engineering and Safety Basis Assessments

Quality Review Board

William F. West, Advisor
Kevin G. Kilp, Chair
Christopher E. McFearin
Christian M. Palay
Michael A. Kilpatrick

EA Site Lead for PNNL

Eric A. Ruesch

EA Assessment Team

Aleem E. Boatright, Lead
Kathleen M. Mertens
Donna R. H. Riggs
Christopher M. Rozycki
Anthony R. Taylor