Independent Assessment of Software Quality Assurance Program Implementation at the Hanford Site

October 2023

Office of Enterprise Assessments
U.S. Department of Energy

Table of Contents

Acronyms

BNI	Bechtel National, Inc.
CFR	Code of Federal Regulations
CPCCo	Central Plateau Cleanup Company
CRAD	Criteria and Review Approach Document
DOE	U.S. Department of Energy
EA	Office of Enterprise Assessments
HAB	Hanford Accreditation Boundary
HICSAB	Hanford Industrial Control System Accreditation Boundary
HISI	Hanford Information System Inventory
HLAN	Hanford Local Area Network
HMIS	Hanford Mission Integration Solutions, LLC
IHLW	Immobilized High-level Waste
OFI	Opportunity for Improvement
PRRB	Production Readiness Review Board
QAIP	Quality Assurance Implementation Plan
QAP	Quality Assurance Program
QAPD	Quality Assurance Program Description
QAPjP	Quality Assurance Project/Program Plan
QAPP	Quality Assurance Program Plan
QIP	Quality Implementation Plan and Graded Approach
QL	Quality Level
SECB	Systems Engineering Control Board
SQA	Software Quality Assurance
SSME	Software Subject Matter Expert
STSA	Software Technical Support Analyst
WRPS	Washington River Protection Solutions, LLC

INDEPENDENT ASSESSMENT OF SOFTWARE QUALITY ASSURANCE PROGRAM IMPLEMENTATION AT THE HANFORD SITE

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 Hanford Site from March to April 2023. The purpose of this assessment was to evaluate the performance of the Bechtel National, Inc. (BNI), Central Plateau Cleanup Company (CPCCo), Hanford Mission Integration Solutions, LLC (HMIS), and Washington River Protection Solutions, LLC (WRPS) SQA programs. This assessment also evaluated the effectiveness of the Office of Environmental Management's Richland Operations Office and Office of River Protection, collectively referred to as DOE Hanford, in providing oversight of these SQA programs.

EA identified the following strengths, including one best practice:

- BNI identifies a non-nuclear safety software category for facility chemical hazards. This practice enhances the process for implementing controls commensurate with an identified risk. (Best Practice)
- BNI enhances approval status visibility by including the approval reference number on the cover page of DOE-approved quality documents.
- CPCCo and HMIS are coordinating their efforts with DOE Hanford and working on corrective action plans to address several programmatic SQA issues that were self-identified as well as identified through effective field element oversight.
- HMIS hosts review board meetings for SQA-related actions that potentially have sitewide impact.
- WRPS identifies and includes useful standards and guidance in several SQA implementing procedures to support the user in conducting activities and preparing deliverables.
- WRPS includes a summary of the weakness and correlating mitigation statement for each of the DOE safety advisories identified in the safety management plan for software program RadCalc 4.1.

EA also identified several weaknesses, as summarized below:

- HMIS and BNI do not always specify minimum training and qualification requirements for using non-safety software.
- CPCCo did not perform management or independent assessments of SQA activities.
- CPCCo did not implement the requirement to maintain software in all cases, such that damage, loss, and/or deterioration is prevented.
- WRPS does not provide written documentation of the evaluation and review of all non-safety software to support its inclusion in the WRPS software inventory.
- BNI does not always ensure that the plant and project safety software inventories include all minimum elements.

In summary, generally adequate SQA programs have been implemented by BNI, CPCCo, HMIS, and WRPS at the Hanford Site, and oversight conducted by DOE Hanford has been generally effective. Both safety and non-safety software are managed through processes that provide reasonable assurance of software quality, including software that supports nuclear safety. However, several weaknesses identified by EA during this assessment, and identified by the contractors and DOE Hanford prior to this

assessment, document needed improvements to the SQA programs. Allowing these weaknesses to go unresolved and/or unevaluated leaves the Hanford Site vulnerable to unanticipated issues, the risk of which cannot easily be quantified. Until all current corrective actions are complete and the weaknesses identified in this report are addressed, or effective mitigations are put in place, software quality at the Hanford Site will not be optimal.

INDEPENDENT ASSESSMENT OF SOFTWARE QUALITY ASSURANCE PROGRAM IMPLEMENTATION AT THE HANFORD SITE

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 Hanford Site. The purpose of this assessment was to evaluate the performance of the Bechtel National, Inc. (BNI), Central Plateau Cleanup Company (CPCCo), Hanford Mission Integration Solutions, LLC (HMIS), and Washington River Protection Solutions, LLC (WRPS) SQA programs. This assessment also evaluated the effectiveness of the Office of Environmental Management's Richland Operations Office and Office of River Protection, collectively referred to as DOE Hanford, in providing oversight for these SQA programs. EA conducted this assessment remotely between March and April 2023.

This assessment was performed consistent with the *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 examined and analyzed the design of SQA programs implemented throughout the DOE enterprise and helped to identify general, complex-wide strengths and weakness. The first phase also 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 Hanford Site contractor 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.

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 contractor quality assurance programs (QAPs) for safety and non-safety software.

3.1.1 Safety Software

3.1.1.1 Hanford Mission Integration Solutions, LLC

HMIS has established an adequate QAP for safety software that meets most requirements of 10 CFR 830, subpart A, *Quality Assurance Requirements*, and DOE Order 414.1D, attachment 2, *Quality Assurance Criteria*, addressing all software, and attachment 4, *Safety Software Quality Assurance Requirements for Nuclear Facilities.* HMIS is undertaking corrective actions for safety software that has known weaknesses documented in the HMIS issues management system. DOE Hanford is providing field element oversight of the HMIS effort to address the condition reports that identified these weaknesses in software quality. The HMIS QAP comprises the Quality Assurance Program Description (QAPD) and Quality Assurance Implementation Plan (QAIP), which are submitted to DOE Hanford for review and approval. The QAIP adequately identifies the primary implementing mechanisms for each section of the QAPD. HMIS has also established adequate implementing procedures for safety software, including project planning, requirements specifications, design, procurement, verification and validation, and configuration management.

HMIS-PRO-QA-259, *Graded Approach*, establishes minimum grading requirements for all procured items, activities, and services, and for all internally performed activities and services; however, the need for updating the software grading requirements is a known weakness cited by DOE in the conditional approval of the QAPD. HMIS-PRO-QA-259 appropriately includes a grading process flowchart and a structure, system, or component grading guide. It also includes a table correlating software grade to quality level (QL)-1, *Safety Class*; QL-2, *Safety Significant*; QL-3, *General Service with additional controls*; and QL-0, *General Service*. However, the use of QL-0 may confuse users as it does not mean that zero controls are applied. (See **OFI-HMIS-1**.)

HMIS has effectively established and maintains the Hanford Information System Inventory (HISI) software and website used at the Hanford Site, except for software controlled by BNI. HMIS-PRO-IS-61311, *Hanford Information System Inventory Procedure*, effectively documents the process to identify, document, control, and maintain the software inventory. HISI summaries for each reviewed software application appropriately include the required safety software inventory fields. The HISI website effectively provides standard and tailored report options for users to access their content. The list of software provided by HMIS was used to select the two software samples for this assessment, and while the list did not include some of the required fields, the HISI documentation for these applications did include the required information. During interviews regarding HISI usage, HMIS personnel recognized the usefulness of a standard safety software inventory list and began internal discussions to develop this capability. (See **OFI-HMIS-2**.)

HMIS effectively uses an independent board to review and approve the software grading level on all HMIS safety and non-safety software applications submitted through HISI. However, while HMIS, CPCCo, Hanford Laboratory Management Integration, and WRPS use the HISI website for controlling software, their individual software grading approaches and workflows for review and approval are unique. HMIS personnel explained that inconsistent grading approaches and workflow routings add complexity to the backend programming of HISI. In addition, these inconsistent approaches can result in

confusion with respect to how sitewide software managed by HMIS is used by individual Hanford Site contractors, and consequently, how it should be graded. (See **OFI-HMIS-3**.) For example, the Sentinel software, which is managed by HMIS for use across the site, was recently re-graded from level D (non-safety) to level B (safety) based on usage requirements for another Hanford Site contractor.

In addition to the HISI website, HMIS effectively manages the Systems Engineering Control Board (SECB) and Production Readiness Review Board (PRRB) for all Hanford Site contractors that access the Hanford Local Area Network (HLAN), Hanford Accreditation Boundary (HAB), and Hanford Industrial Control System Accreditation Boundary (HICSAB). The SECB and PRRB properly focus on ensuring that network security and configuration reliability are effectively managed and maintained following the introduction of new or modified software. Both boards may also review other contractors' application of SQA, as needed, to ensure that testing and records meet requirements.

HMIS adequately controls safety software through implementing procedures and well-trained staff. For example, RadCalc 4.1, which is a software application used across DOE for transportation classifications and calculations to ensure shipment compliance, has a quality defect that has been identified and communicated through several DOE safety advisories. HISI documentation, training records, use logs, and interviews demonstrated that adequate controls are in place for using RadCalc 4.1 to ensure that the software is maintained and used in a manner that produces the intended outcome. HMIS-PRO-IS-309, *Controlled Software Management*, and HMIS-PRO-IS-62263, *Controlled Software Management for Safety Software*, requires the appropriate involvement of the facility design authority, as applicable. Implementing procedures appropriately omit reference to the use of software contained in the DOE Software Central Registry, as HMIS does not use any of the listed software. Additionally, since taking over from the previous contractor in 2021, HMIS has employed three trained and qualified SQA engineers to establish, maintain, and ensure an adequate SQA program. HMIS appropriately defines the Software Design Authority as the software engineer who establishes software engineering requirements, verifies that the design of the software and the end product meet the functional and operational requirements of the owner, and retains ultimate responsibility for the technical baseline. Reviewed management assessments, surveillances, independent assessments, condition reports, and corrective actions demonstrate that identified weaknesses were properly managed through the HMIS issues management system.

3.1.1.2 Central Plateau Cleanup Company

CPCCo has established and maintains a conditionally approved QAP that meets most requirements of 10 CFR 830, subpart A, and DOE Order 414.1D, attachments 2 and 4. CPCC-MP-QA-599, *Quality Assurance Program*, was conditionally approved by DOE Hanford on February 22, 2023. CPCCo is implementing a DOE-approved corrective action plan, CPCC-CR-2021-1228, *Revised Corrective Action Plan for Software Quality Assurance*, to establish a fully adequate QAP for safety software. Resubmittal of an updated QAP is due by September 30, 2023, to address the following expectations from the conditional approval:

- Update the QAP to incorporate all selected consensus standard requirements or add management expectations.
- Remove references to DOE orders in the body of the QAP or provide a rationale as to why the references are included in the QAP.
- Under Criterion 10, *Independent Assessment*, include an explanation addressing the differences between the cited DOE Orders.

CPCCo has adequately established implementing procedures for safety software. The QAP and implementing procedures require all safety software to be assigned grades based on a defined graded approach for applying SQA requirements. However, a revision of CPCC-MP-QA-54798, *Graded Approach Management Plan*, that addressed DOE comments was approved by DOE Hanford on June 23, 2023, and a corrective action plan is now in place to further develop and revise implementing procedures by July 2023. CPCCo has not yet determined whether a due date will be assigned for applying the revised graded approach to already graded software or whether that software will be allowed to wait until the next software revision. Currently, CPCC-MP-QA-599, section 1.3.4, requires project-specific quality assurance program plans (QAPPs) to be submitted to DOE for concurrence prior to release. However, for project-specific CPCC-QAP7P-OCRWM-001, *Quality Assurance Program Plan for Implementation of the OCRWM Quality Assurance Requirements and Description*, prior concurrence was not obtained. Subsequently, CPCC-QAPP-OCRWM-001 was submitted and conditionally approved by DOE Hanford on October 25, 2022, with resubmittal required by September 30, 2023, to address the following DOE Hanford expectations:

- "Update the QAPP to the Office of Civilian Radioactive Waste Management's (OCRWM) Quality Requirements and Description, rev. 20."
- "Section 3.1, *The Contractor and Quality Assurance Manager*, states 'C&QA Manager is the interpretive authority and has overall responsibility for approving OCRWM QA program requirements.' Since the DOE approval authority approves the quality assurance program as described in DOE Order 414.1D, this statement shall be revised."

The QAP and implementing procedures provide for the appropriate involvement of the facility design authority, as applicable, with respect to software requirement specifications, acquisition, design, development, verification and validation (including inspection and testing), configuration management, and retirement. CPCCo requires software subject matter expert (SSME) training but does not use a qualification card. Thirty-three employees have completed SSME training, and 28 are a "active HISI assigned SSME[s]." Contrary to DOE Order 414.1D, attachment 2, sections 9 and 10.a, CPCCo is not performing management or independent assessments of software quality. (See **Deficiency D-CPCCo-1**.) Not performing assessments may allow unidentified weaknesses to persist without correction.

CPCCo appropriately uses the HISI website to manage software. As a requirement for using the HISI website, CPCCo participates on the HMIS-chaired SECB and PRRB for all the Hanford Site contractors that access the HLAN, HAB, and HICSAB to ensure that network security and configuration reliability are adequately managed and maintained following the introduction of new or modified software. The software inventory list that CPCCo provided, which was used to select software for this assessment, did not include the version identifier or the specific nuclear facilities where each application is used. The HISI documentation for the selected software, however, did include all required information for a safety software inventory.

The CPCCo operational software inventory includes EPIcode, version 9.0.2, and Hotspot, version 3.1.2, which are later versions than those included in the DOE Software Central Registry. Both are graded as non-safety software grading level D. The software management plans to address the software lifecycle activities appropriately include test cases and the acceptance test report as attachments. For the known quality defect in RadCalc 4.1, the HISI documentation provided by CPCCo adequately documents the issue and the CPCCo justification for continued use.

3.1.1.3 Washington River Protection Solutions, LLC

WRPS has established a generally effective QAP for safety software and effectively maintains the DOE-approved QAP consisting of TFC-PLN-02, *Quality Assurance Program Description*, and TFC-PLN-50, *Quality Implementation Plan and Graded Approach* [QIP], that meets the requirements of 10 CFR 830, subpart A, and DOE Order 414.1D, attachments 2 and 4. DOE Hanford quality assurance personnel reviewed and concurred on changes to the QAPD prior to its submittal for review and approval. The QIP identifies the quality implementing procedures and software quality and grading criteria and also lists the DOE-approved Quality Assurance Project/Program Plans (QAPjPs) that take precedence over any QIP requirement. The QAPD, section F 11.0, states that QAPjPs shall be approved by the WRPS Manager of Quality and receive concurrence from the Office of River Protection prior to release. Per DOE Order 414.1D, attachment 2, section 4.a, any documents that specify requirements must be appropriately reviewed and approved. However, although the QAPD specifies that QAPjPs require DOE concurrence, the QIP does not include that requirement. (See **OFI-WRPS-1**.)

WRPS has established adequate implementing procedures for safety software lifecycle activities. The QAP and implementing procedures establish that grading levels (i.e., A, B, or C) are assigned to all safety software based on a defined graded approach for applying SQA requirements and the appropriate involvement of the facility design authority, as applicable. TFC-BSM-IRM-STD-01, *Software Life Cycle Standard*, clearly describes the approach to SQA work activities and associated lifecycle processes to ensure compliance with the QAP. Many implementing procedures provide standards and guidance with respect to conducting activities and preparing deliverables. For example, TFC-ENG-DESIGN-C-32, *Utility Calculation Software Management*, includes review checklists with key points for reviewer consideration, design hints and tips for easy-to-use spreadsheets, and common errors to avoid. Access to checklists, guidance, and tools enhances the implementation process, helping to prevent errors.

Further, RadCalc 4.1 is appropriately graded as grading level A safety software. The RadCalc 4.1 Safety Management Plan adequately implements software quality program requirements and includes a summary of the safety weakness and a correlating mitigation statement for each of the seven DOE safety advisories identified for RadCalc 4.1 from 2011 to 2015. The use of this summary helps to ensure that each safety weakness has been addressed, enhancing the effectiveness of the Safety Management Plan.

WRPS effectively controls its software documentation, appropriately uses the HISI website to manage software, and participates on the HMIS-chaired SECB and PRRB for all the Hanford Site contractors that access the HLAN, HAB, and HICSAB to ensure that network security and configuration reliability are effectively managed and maintained following the introduction of new or modified software. WRPS appropriately established a software review board to ensure that software development, implementation, and resulting documentation are compliant. The Plant Installed Change Control Board (PICCB) appropriately provides interpretive authority for software lifecycle activities for plant-installed software, performs verification and validation processes, and ensures that checklist items have been satisfied commensurate with software grading level. The PICCB effectively coordinates with the Project Lead for review and approval of generated software lifecycle deliverables and software change requests. Further, WRPS employs eight trained and qualified SSMEs to establish, maintain, and support an effective program. Training and qualification documentation for four software technical support analysts (STSAs) showed that they had completed their assigned training and STSA qualification cards. The assessment team also verified that two of the STSAs had completed their STSA requalification cards.

The provided WRPS software inventory list, which was used to select software for this assessment, did not include all required elements for a safety software inventory. The HISI documentation for the reviewed safety software did, however, include the required information. The WRPS software inventory includes several toolbox codes from the DOE Software Central Registry, all of which are appropriately

documented in HISI. However, GENII is graded as operational grading level A safety software with no active authorized users and is therefore a candidate for retirement.

3.1.1.4 Bechtel National, Inc.

BNI has established an adequate QAP for safety software and effectively maintains seven DOE-approved quality documents that meet the requirements of 10 CFR 830, subpart A, and DOE Order 414.1D, attachments 2 and 4. BNI divides its work scope between engineering procurement construction (EPC) startup functions and commissioning, maintenance, and operations (C&O) functions, with two of the DOE-approved quality documents applying to both EPC and C&O, two applying only to EPC, and three applying only to C&O. BNI includes the DOE approval reference number on the cover page of the seven documents, a practice that enhances approval status visibility. BNI has also established adequate implementing procedures for safety software, including facility design authority involvement, project planning, requirements specifications, design, procurement, verification and validation, and configuration management. BNI effectively uses standards and guides to assist with implementation.

The QAP and implementing procedures appropriately establish that grading levels are assigned to all safety software based on a defined graded approach for applying SQA requirements with commensurate classification of safety controls. In addition to nuclear safety software grading levels A, B, and C, BNI designates chemical safety system software subject to ISA-84, *Instrumented Systems to Achieve Functional Safety in the Process Industries*, as level CS, raising visibility of a non-nuclear safety risk. Identifying a non-nuclear safety software category for facility chemical hazards is cited as a **Best Practice** because it enhances the process for implementing controls commensurate with an identified risk.

A designation of immobilized high-level waste (IHLW) for waste acceptance-impacting software associated with the IHLW product qualification and disposal requirements is added to the software level, when applicable. BNI effectively maintains six sets of software baselines, which are software inventories that have been approved for use. Four of these baselines have been approved for the Waste Treatment and Immobilization Plant's software and two for project software. Four DOE Software Central Registry toolbox codes are incorporated in one of the project software baselines. BNI appropriately manages the software without relying on the registry status for acceptance. Any software listed in the registry, regardless of the version being acquired, undergoes the same lifecycle work activities as other software prior to approval for use. BNI does not use RadCalc 4.1.

24590-WTP-RPT-OP-11-002, *Approved Plant Administrative Software Baseline Report and Safety Software Inventory*, is controlled and maintained, and includes the required elements for a safety software inventory except for the identification of the nuclear facility where it is used. 24590-WTP-RPT-IT-09-014, *Approved Project Safety Software Inventory*, is controlled and maintained, but does not include the software description, safety software designation, or specific facility where used. These elements are required for the safety software inventory. Contrary to DOE Order 414.1D, attachment 4, section 2.a.(2), BNI does not ensure that safety software inventories include all minimum elements. (See **Deficiency D-BNI-1**.) Not addressing all required SQA inventory requirements can result in missing information that is necessary for management of software.

3.1.2 Non-safety Software

3.1.2.1 Hanford Mission Integration Solutions, LLC

HMIS has established an adequate QAP for non-safety software that meets the requirements of DOE Order 414.1D, attachment 2, with known weaknesses managed through the issues management program. HMIS-PRO-IS-309 assigns grading levels D, E, and F to non-safety software and includes forms for

adequately documenting the non-safety software grading levels D, E, or F as an alternative to the written software management plan required for safety software grading levels A, B, and C. Currently, HMIS defines nine categories of grading level F software that can be exempted from some SQA requirements through use of form A-6007-779, *Software Exemption Form*. This form appropriately specifies the use of HMIS-PRO-SC-335, *Use and Control of Purchasing Card*, when purchasing exempt software. HMIS is working to remove software exemptions in the next revision of the graded approach for DOE Hanford review and approval. Implementing procedures adequately address role-specific SQA training, software engineer qualification, and application-specific user training; the detection and correction of quality-related problems; user instructions and records; design requirements; procurement; verification and validation; and management and independent assessment of non-safety software.

3.1.2.2 Central Plateau Cleanup Company

CPCCo has established an adequate QAP for non-safety software that meets the requirements of DOE Order 414.1D, attachment 2, with several corrective actions underway to further enhance the QAP. Implementing procedures CPCC-PRO-EN-40357, *Control System Software*, and CPCC-PRO-IRM-309, *Controlled Software Management*, adequately address the detection and control of quality-related problems, user instructions and records, design requirements, procurement, and verification and validation of safety and non-safety software. Software management plans for individual applications provide specific details for implementation. CPCCo has established a graded approach to address non-safety software through CPCC-MP-QA-54798. While the graded approach process is not used to "grade to zero" (i.e., eliminate requirements), the lowest quality level is QL-0 instead of QL-4. However, the use of 0 as a quality level may confuse users because it does not mean that zero controls are applied. (See **OFI-CPCCo-1**.)

3.1.2.3 Washington River Protection Solutions, LLC

WRPS has established an adequate QAP for non-safety software that meets the requirements of DOE Order 414.1D, attachment 2. Implementing procedures adequately address the detection and prevention of quality-related problems, user instructions and records, design requirements, procurement, verification and validation, and management and independent assessment of non-safety software. WRPS has established a generally effective graded approach to address non-safety software through the QAPD and QIP. While the grading levels are used to select implementing procedures tailored to associated levels of rigor, the lowest quality level is QL-0 instead of QL-4. However, the use of 0 as a quality level may confuse users because it does not mean that zero controls are applied. (See **OFI-WRPS-2**.)

The identified non-safety software grading levels include grading level D for quality affecting software and grading level E for non-quality affecting software. Some of the reviewed implementing procedures include a software grade of N/A, and many WRPS HISI entries are graded N/A. The current graded approach eliminated the N/A grading level and defined grading level E as the minimum grading level for software. Management directive TFC-MD-179, *Interim Plan for Implementing SQA requirements in TFC-PLN-50*, was sent to all software owners and all qualified STSA holders as required reading. This action provides direction and guidance until completion of the effort to transition all software previously graded as N/A to grading level E with all minimum requirements applied.

3.1.2.4 Bechtel National, Inc.

BNI has established an adequate QAP and implementing procedures for non-safety software that meet the requirements of DOE Order 414.1D, attachment 2. BNI has also established an adequate graded approach to address non-safety software using grading levels D/D1, D2, E, and F. The IHLW designation may apply to non-safety software except grading levels E and F. Implementing procedures adequately address

the detection and prevention of quality-related problems, user instructions and records, design requirements, procurement, verification and validation, and management and independent assessment of non-safety software.

3.1.3 Quality Assurance Program Conclusions

HMIS has established a generally adequate QAP for safety and non-safety software and maintains the DOE-approved QAPD and QAIP, which meet most requirements, with known weaknesses documented in the issues management system. The HMIS graded approach establishes minimum grading requirements for procured items, activities, and services, and for internally performed activities and services. HMIS effectively controls and maintains the HISI software and website, and effectively manages the SECB and PRRB. HMIS effectively controls safety and non-safety software through implementing procedures, except for known weaknesses being addressed by HMIS. However, HMIS allows inconsistent grading approaches for the sitewide software that it manages.

CPCCo has established and maintains a generally adequate QAP that meets the requirements for safety and non-safety software, with a DOE-approved corrective action plan underway to implement a completely adequate QAP. In general, CPCCo adequately controls safety and non-safety software through implementing procedures. CPCCo appropriately uses the HISI website for software quality documentation and participates on the HMIS-chaired SECB and PRRB. However, CPCCo is not performing management and independent assessments of software quality.

WRPS has established an adequate QAP for safety software, maintaining a DOE-approved QAP consisting of the QAPD, QIP, and QAPjPs, and has established adequate implementing procedures for safety and non-safety software lifecycle activities. The revised graded approach appropriately eliminated the N/A software grade and effectively established minimum requirements for the lowest grade, grading level E. The RadCalc 4.1 documentation appropriately addressed each of the DOE-issued safety advisories. However, WRPS provides conflicting direction for the approval of SQA-related documentation.

BNI has established an adequate QAP for safety software, maintaining seven DOE-approved documents that meet requirements for safety and non-safety software. The QAP and implementing procedures effectively establish how grading levels are assigned to all safety software based on a defined graded approach for applying SQA requirements with commensurate grading of controls. BNI has also established a non-nuclear safety (i.e., chemical safety) software grading level, which was cited as a best practice. However, BNI's plant and project safety software inventories do not include all required elements.

3.2 Software Quality Assurance Program Implementation

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

3.2.1 Safety Software

3.2.1.1 Hanford Mission Integration Solutions, LLC

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

- RadCalc 4.1
- Radiological Access Control

HMIS personnel adequately adhered to applicable SQA requirements with respect to developing and using the two sampled safety software applications. The software management plans were appropriately approved and distributed and include a roles and responsibilities matrix that clearly defines project assignments. The requirements specifications adequately address the software function and performance methodology, which explain what the software accomplishes and how it does so. The software documentation adequately describes the overall architecture and workflow based on a SQA-approved process model. Software data collection was appropriately gathered, measured, and analyzed per SQA requirements to research problems, answer questions, evaluate outcomes, and forecast trends and probabilities. HMIS'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 software application documentation for use training demonstrates appropriate training of users consistent with their skill levels.

3.2.1.2 Central Plateau Cleanup Company

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

- Power Tools for Windows Version 7.0
- Survey Simple
- Environmental Restoration Disposal Facility (ERDF) Leachate Instrumentation and Control System

CPCCo personnel generally adhered to applicable SQA requirements with respect to developing and using three sampled safety software applications. The software management plans were appropriately approved and distributed and include a roles and responsibilities matrix that clearly defines project assignments. The requirements specifications adequately address the software function and performance methodology, which explain what the software accomplishes and how it does so. The software documentation adequately describes the overall architecture and workflow based on a SQA-approved process model. Software data collection is appropriately gathered, measured, and analyzed per SQA requirements to research problems, answer questions, evaluate outcomes, and forecast trends and probabilities. CPCCo'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 software application documentation for user training demonstrates appropriate training of users specific to their level of skill.

Although the reviewed sample of safety software applications demonstrated that the CPCCo's SQA program meets most applicable requirements, EA observed two instances where a SQA procedure was not fully implemented. For two reviewed software applications, Power Tools for Windows Version 7.0 and the ERDF Leachate Instrumentation and Control System, there was no evidence provided that procedure CPCC-PRO-IRM-309 was used to define the requirements for maintenance of data and application integrity. Contrary to DOE Order 414.1D, attachment 2, section 5.c, CPCCo did not implement the requirement to maintain software, such that damage, loss, and/or deterioration is prevented. (See **Deficiency D-CPCCo-2**.) Without implementing this requirement, CPCCo cannot ensure consistency in controlling the quality of software. A corrective action plan that has not yet been approved was drafted by CPCCo to address these issues.

3.2.1.3 Washington River Protection Solutions, LLC

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

- Unit Liter Dose Calculation Spreadsheet
- MicroShield
- Hydraulic Analyzer of Sprinkler Systems

WRPS personnel adequately adhered to applicable SQA requirements with respect to developing and using the three sampled safety software applications. The software management plans were appropriately approved and distributed, and include a roles and responsibilities matrix that clearly defines project assignments. The requirements specifications adequately address the software function and performance methodology, which explain what the software accomplishes and how it does so. The software documentation adequately describes the overall architecture and workflow based on a SQA-approved process model. Software data collection is appropriately gathered, measured, and analyzed per SQA requirements to research problems, answer questions, evaluate outcomes, and forecast trends and probabilities. WRPS's documented risk analysis for the reviewed software documentation demonstrates effective mitigation of potential loss of data or functionality. Reviewed documentation shows that testing was performed during each stage of the development workflow, and appropriately included peer reviews and audits. The software application documentation for user training demonstrates appropriate training of users consistent with their roles.

3.2.1.4 Bechtel National, Inc.

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

- ASPEN Process Performance Simulation (APPS)
- BSIMQKE
- ATTILA

BNI personnel adequately adhered to applicable SQA requirements with respect to developing and using the three sampled safety software applications. The software management plans were appropriately approved and distributed, and include a roles and responsibilities matrix that clearly defines project assignments. The requirements specifications adequately address the software function and performance methodology, which explain what the software accomplishes and how it does so. The software documentation adequately describes the overall architecture and workflow based on a SQA-approved process model. Software data collection is appropriately gathered, measured, and analyzed per SQA requirements to research problems, answer questions, evaluate outcomes, and forecast trends and probabilities. BNI's documented risk analysis for the reviewed software documentation demonstrates effective mitigation of potential loss of data or functionality. Reviewed documentation shows that testing was performed during each stage of the development workflow, and appropriately included peer reviews and audits. The reviewed software application documentation for user training demonstrates appropriate training of users consistent with their skill levels.

3.2.2 Non-safety Software

3.2.2.1 Hanford Mission Integration Solutions, LLC

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

- Dragos Passive ICS Threat Detection
- Access Control Entry System
- SENTRY
- Tokay Software Backflow Prevention Management
- Microsoft Windows
- Microsoft Excel

HMIS has established a generally 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 training records generally demonstrate appropriate training and qualification of personnel who acquire, maintain, use, and assess non-safety software applications. Review of HNF-27376, *Software Management Plan*, section 2.2.3, for the Access Control Entry System software application, demonstrated that procedures adequately address the detection and prevention of quality-related problems, user instructions and records, design requirements, procurement, verification and validation, and management and independent assessment of non-safety software. However, contrary to DOE Order 414.1D, attachment 2, sections 2.a and 2.b, HMIS has not specified training requirements for non-safety software applications Microsoft Windows, Microsoft Excel, and Tokay Software Backflow Prevention Management. (See **Deficiency D-HMIS-1**.) By not specifying such requirements for personnel training, the proper use of these software applications cannot be ensured. Prior to this assessment, HMIS developed a corrective action plan to address the inappropriate exemptions of software from certain DOE Order 414.1D, attachment 2, criteria; however, the planned corrective actions do not explicitly identify the need for all order criteria to be met.

3.2.2.2 Central Plateau Cleanup Company

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

- Field Logging and Electronic Data Gathering
- SCADA/PLC software
- MathCAD Prime 3.1
- Microsoft Windows
- Microsoft Excel

CPCCo has established a generally 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 training records for the sampled software applications demonstrate appropriate training and qualification of personnel who acquire, maintain, use, and assess non-safety software applications. HNF-66718, *Field Logging and Electronic Data Gathering (FLEDG) Software Management Plan*, section 6.6, demonstrated adequate user instructions, design requirements, procurement, validation, and management of non-safety software, as well as effective mitigation of the potential loss of data or functionality.

3.2.2.3 Washington River Protection Solutions, LLC

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

- TOPSim
- TOPSim Automator

- Autopano Giga 3.0
- Microsoft Windows
- Microsoft Excel

WRPS has established an effective 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 training records for the four sampled software applications demonstrated appropriate training and qualification of personnel who acquire, maintain, use, and assess non-safety software applications. WRPS RPP-PLAN-61812, *Software Manag*[*e*]*ment Plan for Grade D Custom Developed Planning Support Software*, section 3, for the application TOPSim, demonstrated adequate user instructions, design requirements, procurement, validation, and management of non-safety software. Additionally, RPP-PLAN-61812, section 4, adequately documented the risk analysis and effective mitigation of potential loss of data or functionality. However, contrary to DOE Order 414.1D, attachment 2, section 4, WRPS did not document the SECB process or the results of its review of the Autopano Giga 3.0 software. (See **Deficiency D-WRPS-1**.) Without written documentation of completed SQA processes, no record exists to inform users of outcomes related to the initial evaluation of software and facilitate its ongoing maintenance.

3.2.2.4 Bechtel National, Inc.

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

- CHAMPS/Computerized Maintenance Management System (CMMS)
- Process calculations App 2
- IHLW – ProCalV5 Instrument Calibration Management System (ICMS)
- Sentinel
- Labview 7 Express
- Microsoft Windows
- Microsoft Excel

BNI has established a generally effective 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 training records demonstrated appropriate training and qualification of personnel who acquire, maintain, use, and assess non-safety software applications, with two exceptions. Procedure 24590-WTP-PSRA-PENG-19-0003_003, *Process Calculations App 2*, adequately addresses procedures for detection and prevention of quality-related problems, user instructions and records, design requirements, procurement, verification and validation, and management and independent assessment of non-safety software. However, contrary to DOE Order 414.1D, attachment 2, sections 2.a and 2.b, BNI has not specified training requirements for non-safety software applications Microsoft Windows and Microsoft Excel. (See **Deficiency D-BNI-2**.) When such requirements are not specified for personnel training, the proper use of these software applications cannot be ensured.

3.2.3 Software Quality Assurance Program Implementation Conclusions

In general, HMIS, CPCCo, WRPS, and BNI adequately adhere to software quality procedures that have been implemented in accordance with DOE Order 414.1D, attachments 2 and 4, and are generally effective in managing safety and non-safety software applications. However, HMIS, BNI, and CPCCo have not implemented all required criteria for some of the reviewed non-safety software applications. In addition, for one reviewed software application, WRPS did not produce documentation to demonstrate that all established SQA processes had been completed.

3.3 Software Security

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

3.3.1 Hanford Mission Integration Solutions, LLC

HMIS adequately ensures the security of safety and non-safety software through its SQA program, in accordance with applicable requirements. HMIS-PRO-IS-47277, *Systems Engineering Control Board*, adequately addresses responsibilities for cybersecurity. The SECB uses a defined process (IM-PRO-CS-62614, *Cyber Security for SECB Software Engineering Control Board Procedure*) for appropriate review and approval of software security controls. Reviewed documentation for eight software applications appropriately addresses access controls, where necessary. As an example of internal review, HNF-66673, *Administrative Document Processing and Approval*, provides comprehensive analysis and review and approval of the non-safety software application, Dragos Passive ICS Threat Detection. HNF-66673 documents controls meant to effectively address the security of software on computer systems and networks, adequately ensuring that hardware, software, and electronic data are protected, including through the use of access credentials and anti-phishing controls, as appropriate. Final approval of the Dragos software is appropriately documented in ESP-SECB-347833, *Systems Engineering Control Board Request*.

3.3.2 Central Plateau Cleanup Company

CPCCo adequately ensures the security of safety and non-safety software through its SQA program, in accordance with applicable requirements. The HMIS procedure HMIS-PRO-IS-47277 adequately addresses responsibilities for cybersecurity of CPCCo software. The SECB uses a defined process (IM-PRO-CS-62614) for appropriate review and approval of software security controls. Reviewed documentation for eight software applications appropriately addressed access controls, where necessary. As an example of internal review, HNF-66718 provides comprehensive analysis and review and approval of the Field Logging and Electronic Data Gathering software application (non-safety software). HNF-66718 documents controls meant to effectively address the security of software on computer systems and networks, adequately ensuring that hardware, software, and electronic data are protected, including through the use of access credentials and anti-phishing controls, as appropriate. Final approval of the Field Logging and Electronic Data Gathering software application is appropriately documented in HMIS-PRO-IS-16677, *Production Readiness Review Board*.

3.3.3 Washington River Protection Solutions, LLC

WRPS adequately ensures the security of safety and non-safety software through its SQA program, in accordance with applicable requirements. HMIS-PRO-IS-47277 adequately addresses responsibilities for cybersecurity of WRPS software. The SECB uses a defined process (IM-PRO-CS-62614) for appropriate review and approval of software security controls. Reviewed documentation for eight software applications appropriately addressed access controls, where necessary. As an example of internal review, RPP-PLAN-61812 provides comprehensive analysis and review and approval of the TOPSim software application (non-safety software). RPP-PLAN-61812 documents controls meant to effectively address the security of software on computer systems and networks, adequately ensuring that hardware, software, and electronic data are protected, including through the use of access credentials and anti-phishing controls, as appropriate. Final approval of the TOPSim software is appropriately documented in RPP-PLAN-61812.

3.3.4 Bechtel National, Inc.

BNI adequately ensures the security of safety and non-safety software through its SQA program, in accordance with applicable requirements. HMIS-PRO-IS-47277 adequately addresses responsibilities for cybersecurity of BNI software. The SECB uses a defined process (IM-PRO-CS-62614) for appropriate review and approval of software security controls. Reviewed documentation for 10 software applications appropriately addressed access controls, where necessary. As an example of internal review, 24590-WTP-GPP-RAIT-SQ-1001, *r12 Project (EPCC) and Plant Administrative Software Life Cycle Management Plan*, provides comprehensive analysis and review and approval of the Process Calculations App 2 software (non-safety software). 24590-WTP-GPP-RAIT-SQ-1001 documents controls meant to effectively address the security of software on computer systems and networks, adequately ensuring that hardware, software, and electronic data are protected, including through the use of access credentials and anti-phishing controls, as appropriate. Final approval of the Process Calculations App 2 software is appropriately documented in 24590-WTP-GPP-RAIT-SQ-1001.

3.3.5 Software Security Conclusions

HMIS, CPCCo, WRPS, and BNI adequately ensure the security of safety and non-safety software managed under their respective SQA programs. Each program adequately implements comprehensive procedures that flow down applicable requirements.

3.4 Federal Oversight

This portion of the assessment evaluated DOE Hanford's oversight of contractor SQA programs.

Overall, DOE Hanford has implemented effective processes to provide oversight for the HMIS, CPCCo, WRPS, and BNI SQA programs. Two SQA subject matter experts have been assigned, adequately trained, and qualified to DOE-STD-1172, *Safety Software Quality Assurance Functional Area Qualification Standard*. Further, DOE Hanford appropriately plans, performs, and documents assessments in accordance with DOE-PRO-PAI-50085, *Integrated Oversight*, and DOE-PRO-50571, *Perform Quality Assurance Program Audit/Surveillance and Operational Awareness*, and effectively follows up on issues and corrective actions in accordance with DOE-PRO-PAI-50086, *Integrated Issues Management*.

- EA's review of five software assessments performed by DOE Hanford over the past 24 months show adequate oversight of HMIS software activities, resulting in substantial changes to the HMIS SQA program and included one effectiveness review of HMIS corrective actions.
- DOE Hanford assessment DOE-ASMT-2021-0324, *Quality Assurance Program Audit of CPCCo's Implementation of NQA-1 Requirements 1, 2, 5, 6, 15, 16, S/CI and Software Quality Assurance*, resulted in one condition adverse to software quality and one significant condition adverse to software quality and DOE Hanford is monitoring corrective actions by CPCCo.
- EA's review of four software assessments performed over the past 24 months show adequate DOE Hanford oversight of WRPS software activities and documentation of results.
- EA's review of five software assessments performed over the past 24 months show adequate DOE Hanford oversight of BNI software activities and documentation of results.

Reviewed documentation demonstrates effective DOE Hanford oversight of SQA programs, including approval of contractor corrective action plans, and extensions, when warranted.

3.4.1 Federal Oversight Conclusions

DOE Hanford has established an effective SQA oversight program. DOE Hanford appropriately plans, performs, and documents assessments in accordance with documented procedures. Assessment results are adequately documented, and work to complete corrective actions is being overseen with requested extensions approved when necessary. Two adequately trained and qualified SQA subject matter experts are assigned responsibility for oversight of the Hanford Site contractors.

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:

- BNI uses a non-nuclear safety software category to clearly identify facility chemical hazards. This practice enhances the process for implementing controls commensurate with 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.

Hanford Mission Integration Solutions, LLC

Deficiency D-HMIS-1: HMIS does not always specify the minimum training and qualification requirements for using non-safety software. (DOE Order 414.1D, att. 2, sec. 2)

Central Plateau Cleanup Company

Deficiency D-CPCCo-1: CPCCo is not performing management or independent assessments of SQA activities. (DOE Order 414.1D, att. 2, secs. 9 and 10.a)

Deficiency D-CPCCo-2: CPCCo did not implement the requirement to maintain software in all cases, such that damage, loss, and/or deterioration is prevented. (DOE Order 414.1D, att. 2, sec. 5.c)

Washington River Protection Solutions, LLC

Deficiency D-WRPS-1: WRPS does not provide written documentation of the evaluation and review of all non-safety software to support its inclusion in the WRPS software inventory. (DOE Order 414.1D, att. 2, sec. 4)

Bechtel National, Inc.

Deficiency D-BNI-1: BNI does not ensure that the plant and project safety software inventories include all minimum elements. (DOE Order 414.1D, att. 4, sec. 2.a.(2))

Deficiency D-BNI-2: BNI does not always specify the minimum training and qualification requirements for using non-safety software. (DOE Order 414.1D, att. 2, sec. 2)

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.

Hanford Mission Integration Solutions, LLC

OFI-HMIS-1: Consider using the designation of quality level QL-4 instead of QL-0, as is done by BNI at the Hanford Site, to more clearly denote the lessening rigor of controls and to avoid the unintended assumption that zero controls are acceptable.

OFI-HMIS-2: Consider providing a standard report form on the HISI website to assist users in selecting the minimum elements needed for a safety software inventory.

OFI-HMIS-3: Consider coordinating the establishment of a more consistent grading approach among the Hanford Site contractors to simplify maintenance of the HISI backend programming and ensure accurate grading for sitewide software.

Central Plateau Cleanup Company

OFI-CPCCo-1: Consider using the designation of quality level QL-4 instead of QL-0, as is done by BNI at the Hanford Site, to more clearly denote the lessening rigor of controls and to avoid the unintended assumption that zero controls are acceptable.

Washington River Protection Solutions, LLC

OFI-WRPS-1: Consider clarifying in the QAPD and QIP whether QAPjPs must receive concurrence from DOE and the WRPS Manager of Quality.

OFI-WRPS-2: Consider using the designation of quality level QL-4 instead of QL-0, as is done by BNI at the Hanford Site, to more clearly denote the lessening rigor of controls and to avoid the unintended assumption that zero controls are acceptable.

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 Hanford

Eric A. Ruesch

EA Assessment Team

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