



Department of Energy
National Nuclear Security Administration
Washington, DC 20585

May 23, 2003

RECEIVED
2003 MAY 27 PM 3:57
DNF SAFETY BOARD

The Honorable John T. Conway
Chairman
Defense Nuclear Facilities Safety Board
625 Indiana Avenue, N.W.
Suite 700
Washington, D.C. 20004

Dear Mr. Chairman:

Ambassador Brooks has asked me to respond to your March 25, 2003, letter regarding Software Quality Assurance (SQA) deficiencies at the Pantex site. We understand and concur with your position.

The enclosed two BWXT letters outline actions to improve the SQA for the Integrated Electronic Procedures and the Move Right System, including independent verification and validation efforts. We have evaluated the actions proposed and believe that they will address your concerns. We will keep your site representative informed of BWXT's progress in completing the actions of this plan and will advise you of our assessment of their effectiveness after all actions are complete. If actions have not been completed by February 28, 2004, we will provide a status report and a revised plan.

If you have any questions, please contact me or have your staff contact Jeff Underwood at (301) 903-8303 or Steve Erhart at (806) 477-6150.

Sincerely,

A handwritten signature in black ink, appearing to read "Everet H. Beckner".

Everet H. Beckner
Deputy Administrator
for Defense Programs

2 Enclosures

cc w/enclosures:
J. McConnell, DNFSB
W. Andrews, DNFSB
M. Whitaker, DR
D. Glenn, PXSO



SEPARATION

PAGE

**BWXT
Pantex**

P.O. Box 30020 Amarillo, Texas 79120 806/477-3000

MAY 12 2003**RECEIVED
2003 MAY 27 PM 3:57
DNFSB SAFETY BOARD**

Mr. Daniel E. Glenn, Manager
U. S. Department of Energy
National Nuclear Security Administration
Pantex Site Office
P. O. Box 30030
Amarillo, TX 79120-0030

Re: NNSA/PXSO Memorandum, Glenn to Mallory, dated May 1, 2003, Comments to BWXT Pantex Response to Move Right System, Interactive Electronic Procedure System & Software Quality Assurance Concerns Cited by DNFSB and NNSA PXSO

Dear Mr. Glenn:

BWXT Pantex has taken aggressive actions to improve Software Quality Assurance (SQA) at the Pantex Plant since February, 2001, (see Appendix A for details). However, we are not satisfied with our progress and have identified the following actions to improve the process and results:

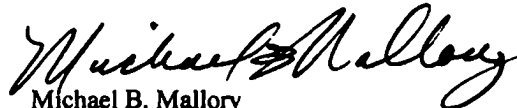
1. Re-assign the responsibilities for SQA to Engineering by June 1, 2003.
2. Perform an independent assessment of the process and procedures with external personnel by June 30, 2003. This review will evaluate system requirements, input and embedded data, human factors, testing/validation and documentation requirements. The end state SQA program will be clearly defined at the conclusion of this task.
3. Benchmark other government and industries sites by June 30, 2003.
4. Provide resource loaded Primavera schedules for MRS and Interactive Electronic Procedures (IEP) action plans by July 31, 2003.
5. Review and incorporate recommendations by July 31, 2003.
6. Implement training for Plant personnel by September 30, 2003, on the revised process/procedures.
7. Improve the Move Right System (MRS) by providing a comprehensive requirement specification for the entire move "system," testing/validation of Manufacturing Resource Planning (MRPII)/Computer Associates Software (CAS)/Track Right/Special Nuclear Database (SNUC) and the MRS interface and a comprehensive human interface evaluation (see Appendix B for details).
8. See Appendix C for IEP action plans. Lessons learned were incorporated into the IEP implementation plan (see Appendix D for details).

9. See Appendix E for executive summary of all compensatory measures taken/planned to ensure accuracy of SNM and HE material control.

BWXT Pantex is committed to assuring the SQA program will provide the defined results with confidence and credibility.

If you have any specific questions on the actions, please contact Gary E. Pool at 477-3782 for details.

Very truly yours,


Michael B. Mallory
General Manager

Attachments: as stated

cc: D. White, PXSO, 12-36
D. Brunell, PXSO, 12-36
E. Burkholder, PXSO, 12-42U
E. Demerson, PXSO, 12-28
S. Erhart, PXSO, 12-36
H. Griffith, PXSO, 12-36A
E. Hogan, PXSO, 12-28
M. Reaka, PXSO, 12-36
M. Mallory, General Manager, 12-69
D. Swaim, Dep. General Manager, 12-69
B. McBride, CFO, 9060A
S. Baker, PAC, 12-6D
M. Carry, Campaigns, 12-69B
J. Clayton, DSW, 12-69B
C. Durham, Eng., 12-6F
D. Hampton, HR, 16-12C
V. Hughes, QA, 12-6D
J. Jones, Legal, 12-100A
R. Madison, RTBF, 12-69B
G. Pool, PSI, 12-69C
J. Yarbrough, Mfg., 12-6F
C. Moore, Infrastructure, 12-5G
J. Noon, SS&EO, 12-36B
L. Trent, ESH&E, 12-69A
C. Bowen, PSI, 12-2B
B. Pascal, IT, 12-106
B. Crabtree, IT, 12-106
T. Schwartz, IT, 12-106
File

APPENDIX A
SQA COMPLETED ACTIONS

Approximately 15 months ago BWXT Pantex began a series of actions designed to improve the SQA program and the focus on safety. Following are actions taken:

- An SQA Steering Committee was created to provide oversight and direction to the SQA program.
- The Steering Committee created a Safety Response Team from a cross-section of SQA knowledgeable individuals from the plant to identify and formally review existing safety software.
- The Safety Response Team created a Safety Plan document, based on IEEE 1228 "Software Safety Plans", to capture the analysis of possible hazards identified in any system that contains software.
- The Safety Response Team inventoried, categorized, and rated safety software at the Plant. The categorization and ratings identified were based on industry standards such as MIL-STD-882D.
- Software lifecycle templates based on IEEE standards have been created to help guide system owners.
- The Plant SQA standard has been revised to:
 - Incorporate the newly created safety plan concept for safety related software systems
 - Include a Software Material List as a tool to show hardware, software packages, code, manuals, and documentation associated with the software portion of the system in a one-page document
 - Incorporate the improved change control process for software to allow for greater control in identifying safety software, whether new construction or modification of an existing system
- A Software Process Advisory Group has been created. This working group allows system owners from across the Plant to participate in the SQA process and provides a forum for feedback on SQA issues that affect implementation.
- On April 30, 2003, additional support personnel were hired to augment the SQA program.
- Independent project reviews of software projects implementing critical safety TSR controls were implemented.
- On request SQA personnel from the Kansas City Plant (KCP) conducted reviews focused on the Move Right and the IEP software systems. Activities performed were:
 - Review of lessons learned
 - Interview key Move Right and IEP staff to identify possible gaps

APPENDIX B
MOVE RIGHT SQA UPGRADE PLAN

Action	Due Date
Develop and document the process for making changes to the MRS software as required during the process of SQA Upgrades	06/02/03
Create a plan to validate MRS system data	06/02/03
Publish the MRS Safety Plan	06/30/03
Provide NNSA/PXSO a Primavera Resource Loaded Schedule for plan activities	07/30/03
Perform a Gap Analysis between the current Move Right SQA Documentation and the new SQA Program requirements.	08/15/03
Upgrade the Requirements Specification to include the entire move "system," which would include all software that interfaces with MRS	10/01/03
Perform a comprehensive human factors evaluation of the entire move system and publish the evaluation report	01/15/04
Create and perform testing and validation of the Move Right System and the entire architectural structure of CAS, Track Right, and MRS Interfaces	01/15/04

**APPENDIX C
IEP SQA ACTION PLAN
UPDATED 5/6/2003**

Actions	Scheduled Completion
Publish all IEP Solumina SQA/SQLC documentation with all necessary reviews and approvals. This includes all of the following items:	6/30/2003
Individual Design Descriptions (DD), Test Plans (TP), and Installation Plans (IP) for each component of and interface to the IEP Solumina system. This includes documentation of contingency plans for missing or corrupted interface data identified in the Software Safety Plan (SP).	
Software Safety Plan (SP) updated with identification of safety elements in the system and flow down into all other SQLC documentation.	
<ul style="list-style-type: none"> ○ IEP Solumina System Technical Characteristic documents (CE1A2738, 3 volumes): System Architecture, Product Definition, and Qualification Strategy (SNL). 	
<ul style="list-style-type: none"> ○ Compatibility Definitions (CD1A2738, 4 volumes): internal and external interfaces, user interfaces, and host environment interfaces. (SNL). 	
<ul style="list-style-type: none"> ○ Qualification Requirements (PQ1A2738, 6 volumes) includes requirements to qualify the system at each remote site, at the software component level, the application functionality level, and the overall system level (SNL/LANL/LLNL). 	
<ul style="list-style-type: none"> ○ Materials Lists including a Flow Chart (FC1A2738) for the entire system and ML for each component. 	
Maintenance Procedures (MP1A32738, 4 volumes) and Maintenance Plan (MP-SW-000059) that document tasks required updating software components of the IEP Solumina system.	
<ul style="list-style-type: none"> ○ Detailed Test Plans (TP) including: the overall system testing plan, test cases with positive and negative outcomes, and test results (19 volumes). 	
<ul style="list-style-type: none"> ○ Education Plan (EP), training plans of instruction (POI) for all system users and technical training requirements for application developers and Help Desk personnel. 	
<ul style="list-style-type: none"> ○ User Documentation (UD): user manuals (4 volumes), Writer's Guide, and Plant Standard. 	
<ul style="list-style-type: none"> ○ Updated Requirements Specification (RS) and Quality Requirements. Updated RS includes all functions (both COTS and custom) and additions since procurement. 	
Complete Human Factors evaluation of the IEP Solumina shop floor interface and publish evaluation report (SNL/LANL).	5/31/2003
Perform a Gap Analysis between the current IEP SQA Documentation and the new SQA Program requirements.	6/30/2003
Provide NNSA/PXSO a Primavera Resource Loaded Schedule for plan activities.	7/30/2003

Actions	Scheduled Completion
Complete Readiness Verification of the IEP Solumina System by issuing BWXT Pantex Readiness letter.	7/30/2003
Complete Qualification of the IEP Solumina system by issuing six QERs: one for each remote site, software components, application functionality, and the overall system (SNL/LANL/LLNL).	7/30/2003
Complete IEP Nuclear Explosive Safety Master Study (NNSA).	8/31/2003
Maintain documentation of problem tracking and resolution as detailed in the QR, and follow SQLC for enhancements to the IEP Solumina System as detailed in the MP documents.	On-going

APPENDIX D
MRS LESSONS LEARNED
UPDATED 5/6/2003

The following lessons learned from the MRS implementation:

- *Validate all data input into a software system prior to implementation.*

IEP is creating separate Design Descriptions, Test Plans, and Installation Plans for each interface into IEP. Each interface has been evaluated for safety implications to production procedures in the IEP system, with contingency processes defined to mitigate identified safety impacts. Changes to any interfaced system will be evaluated for impacts to the IEP system interface, and the interface will be retested prior to implementation.

- *Generate a thorough Safety Plan for MRS, thus allowing for proper incorporation of safety related activities throughout the entire lifecycle.*

Because of early Nuclear Explosive Safety (NES) involvement, safety-related issues of the IEP system were incorporated into the Requirements Specification. IEP initiated the Safety Plan and its activities earlier in the software development lifecycle and was able to identify and document safety activities earlier. With the aid of Six Sigma black belts, Failure Modes and Effects Analyses (FMEA) were conducted on both the software and the procedure development processes. These FMEA results will be incorporated into the Safety Plan following Development.

- *Conduct a human-factors study prior to deployment of software.*

Under DOE O 452.2B, IEP initiated a Human Factors (HF) study for Nuclear Explosive Safety Study (NESS) input and approval. This HF study is evaluating the safety and quality aspects of the software that could introduce errors not found in the paper process when IEPs are used by technicians for nuclear explosive operations. Personnel from LANL and SNL are conducting the study.

- *Develop a complete system interface document for the implementation of system retrofits.*

A maintenance plan is being created that includes required tests and qualification activity for updates to the IEP system. This plan covers updates to COTS software (Solumina, Oracle, Windows), system interfaces, and customized Solumina code. Traceability, full product definition, and a complete system architecture are incorporated into the IEP qualification documents.

- *Ensure depth and formality of test plans, and qualifications based on the software quality level determined by safety, security or business impact.*

The IEP project has a Qualification Task Team, made up of Design Agency personnel, that will qualify six different levels of the IEP system (see Sandia document CE1A2738C). This includes:

- Three remote access site qualifications completed by IT personnel and IEP Solumina users at each of the three Labs.
- Application-level qualification that covers the functional procedures process. This qualification reviews the tasks required to author, review, approve, release, execute, archive, and change a procedure in the IEP Solumina system. This qualification is performed by system and surveillance engineers knowledgeable on the current paper procedures process from all three Labs.
- Component Software level qualification performed by SQA experts at SNL and LLNL.
- System level qualification covers issues not addressed in the other qualification activity including system level integration, training, maintenance, and access security (includes need-to-know controls).

Additional activities included in the IEP project are:

- Test cases are being built from the Requirement Specification document, which include both positive and negative outcomes.
 - 9-point data collection limits testing.
 - Critical software components identified in the Safety Plan that must be retested for each update to the system (identified in the Maintenance Plan).
 - Internal peer review of SQA during Readiness Verification.
 - NESS evaluation includes an SQA technical expert.
- *Track problems and resolutions prior to system release.*

Issues identified during validation and verification (V&V) are recorded and tracked in a change manager database. SQLC documentation has been updated with system scope changes and clarifications made during design and development. This includes Appendix D of the Requirements Specification (RS-SW-000059) that republishes the requirements definition since procurement.

APPENDIX E
COMPENSATORY ACTIONS TAKEN/PLANNED

Event	Actions
Improve the timeliness of detection of errors.	<ul style="list-style-type: none"> • By June 30, 2003, a daily check comparing the material in the CAS (MRP II) inventory by location to the inventory in the MRS will provide an additional layer of detection to improve timeliness by quickly identifying inventory errors. This check will be for all nuclear materials across the plant.
ORPs # ALO-AO-BWXT-PANTEX-2003-0007 - Unauthorized movement of nuclear material from one zone to another.	<ul style="list-style-type: none"> • Create an Operator Aid as a checklist in the Operations Center to validate the number of items authorized in the computer system for movement and for the OC personnel to check the printer for any error messages that would stop the move. • Provided training to OC personnel and Transportation personnel on validation of the move authorization. • Initiate Change Request for the MRS to enhance MRS interface with Track Right.
NCR #29008184 -/A Unit physically located in Zone 4 Magazine 105 was shown in the Move Right System as being in Zone 12 Building 104, Bay 04.	<ul style="list-style-type: none"> • Serial Number Verification was performed on 100% of Category 1A materials in Zone 12 on March 29, 2003, with no discrepancies identified in the SNUC Material Accountability System. • Limited the access to Receipt Modification transaction to only a few key people. • Daily verification of the Receipt and Receipt Modification transactions to ensure accuracy. Created a Corrective Action Plan to provide documentation for Roles & Responsibilities and clarify SQA requirements.
New NCR- Data Error in Move Right resulting in Inventory anomaly.	<ul style="list-style-type: none"> • Standing Order OPS03-003 was issued requiring a validation of explosive inventory weights in the MRS against the facility placard. • Daily validate MRS explosive inventory weights to the facility placard as part of the facility pre-op check. • Before each move is initiated, the individual item explosive weight in MRS matches the part number definition explosive weight in MRS.
ORPs # ALO-AO-BWXT-Pantex-2003-0019 Movement of 3.3 grams of 1.2 explosives from a facility in the Zone 12 MAA outside of the HE window.	<ul style="list-style-type: none"> • Moves were stopped until the system was checked to verify that all facilities in the Zone 12 MAA were identified in the system as being in the MAA, which is required for restrictions on moves outside the HE window.

SEPARATION

PAGE

**BWXT
Pantex**P.O. Box 30020 Amarillo, Texas 79120 806/477-3000

MAY 20 2003

Mr. Daniel E. Glenn, Manager
U. S. Department of Energy
National Nuclear Security Administration
Pantex Site Office
P. O. Box 30030
Amarillo, TX 79120-0030

Subj: NNSA/PXSO Memorandum, Glenn to Mallory, dated May 1, 2003, Comments to BWXT Pantex Response to Move Right System, Interactive Electronic Procedure System & Software Quality Assurance Concerns Cited by DNFSB and NNSA PXSO

Ref: Letter to Daniel E. Glenn of May 12, 2003

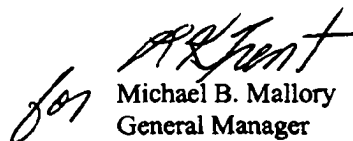
Dear Mr. Glenn:

This letter provides an updated schedule of the Software Quality Assurance (SQA) activities for the Interactive Electronic Procedures (IEP) system. The attached schedule reflects the increased depth and rigor of validation testing to assure quality and readiness of this safety-related system. The principal difference between the attached IEP schedule and the initial schedule submitted May 12, 2003, is six weeks of additional validation testing. Software and migration package testing includes rigorous validation of the commercial off-the-shelf software (COTS), BWXT Pantex customizations, and all system interfaces.

BWXT Pantex is committed to assuring the SQA program will provide the defined results with confidence and credibility.

If you have any specific questions on the actions, please contact Gary E. Pool at 477-3782 for details.

Very truly yours,


Michael B. Mallory
General Manager

Attachments: as stated

**APPENDIX C
IEP SQA ACTION PLAN
UPDATED 5/15/2003**

Actions	Scheduled Completion
<p>Publish all IEP Solumina SQA documentation with all necessary reviews and approvals. Over 120 documents have been identified to complete this activity including the following items:</p> <ul style="list-style-type: none"> ○ Updated Requirements Specification (RS) and Quality Requirements (QR). Updated RS includes all functions (both COTS and customization) and additions since procurement. ○ Software Safety Plan (SP) updated with identification of safety elements in the system and flow down into all other SQA documentation. ○ Maintenance Procedures and Plans (MP) that document tasks required to coordinate and modify software components of the IEP Solumina system across five sites. ○ Individual Design Descriptions (DD), Test Plans (TP), and Installation Plans (IP) for each component of and interface to the IEP Solumina system. This includes documentation of contingency plans for missing or corrupted interface data identified in the Software Safety Plan (SP). Test Plans will be detailed to include overall system testing procedures, test cases with positive and negative outcomes, regression testing, and test results. ○ IEP Solumina System Technical Characteristic (CE) documents include: System Architecture, Product Definition, and Qualification Strategy (SNL). ○ Materials Lists including a Flow Chart (FC1A2738) for the entire system and ML for each system component and interface. ○ Education Plan (EP), describing training plans of instruction (POI) for all system users and technical training requirements for application developers and Help Desk personnel. ○ User Documentation (UD) includes User manuals (4 volumes), Writer's Guide, and Plant Standard on the IEP System. 	6/30/2003
Complete Human Factors evaluation of the IEP Solumina shop floor interface and publish evaluation report (SNL/LANL).	5/31/2003
Perform a Gap Analysis between the current IEP SQA Documentation and the new SQA Program requirements.	6/30/2003
Provide a resource-loaded schedule for SQA plan activities to NNSA/PXSO.	6/30/2003
Complete Validation Testing of IEP System. This includes validation of COTS Solumina software, Pantex customization, and all system interfaces. Testing will be performed twice, once for validation of software, and second time for validation of the migration package.	8/15/2003

Actions	Scheduled Completion
Complete Qualification Requirements (PQ), which includes requirements to qualify the system at each remote site, at the software component level, the application functionality level, and the overall system level (SNL/LANL/LLNL).	7/30/2003
Complete Qualification of the IEP Solumina system by issuing six QERs: one for each remote site, software components, application functionality, and the overall system (SNL/LANL/LLNL).	9/12/2003
Complete Readiness Verification of the IEP Solumina System by issuing BWXT Pantex readiness letter.	9/15/2003
Complete IEP Nuclear Explosive Safety Master Study (NNSA).	10/31/2003
Maintain documentation of problem tracking and resolution as detailed in the QR, and follow SQLC for enhancements to the IEP Solumina System as detailed in the MP documents.	On-going

cc: D. White, PXSO, 12-36A
D. Brunell, PXSO, 12-36A
E. Burkholder, PXSO, 12-42U
E. Demerson, PXSO, 12-28
S. Erhart, PXSO, 12-36A
H. Griffith, PXSO, 12-36A
G. Wisdom, PXSO, 12-36A
E. Hogan, PXSO, 12-28
M. Reaka, PXSO, 12-36A
M. Mallory, General Manager, 12-69A
D. Swaim, Dep. General Manager, 12-69A
B. McBride, CFO, 9060A
S. Baker, PAC, 12-6D
M. Carry, Campaigns, 12-69B
J. Clayton, DSW, 12-69B
C. Durham, Eng., 12-6F
D. Hampton, HR, 16-12C
V. Hughes, QA, 12-6D
J. Jones, Legal, 12-100A
S. Kennedy, DSW, 12-69B
R. Madison, RTBF, 12-69B
G. Pool, PSI, 12-69C
J. Yarbrough, Mfg., 12-6F
C. Moore, Infrastructure, 12-5G
J. Noon, S&S, 12-36B
L. Trent, ES&H&ES, 12-69A
B. Pascal, IT, 12-106
B. Crabtree, IT, 12-106
C. Bowen, PSI, 12-2B
H. Haines, Eng., 12-6F
J. Crockett, IT, 12-106

File