May 4, 2007

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

FROM: Stephen D. Dingbaum /**RA/**
Assistant Inspector General for Audits

SUBJECT: STATUS OF RECOMMENDATIONS: EVALUATION OF THE NRC'S USE OF PROBABILISTIC RISK ASSESSMENT IN REGULATING THE COMMERCIAL NUCLEAR POWER INDUSTRY (OIG-06-A-24)

REFERENCE: DEPUTY EXECTIVE DIRECTOR FOR MATERIALS, WASTE, RESEARCH, STATE, TRIBAL, AND COMPLIANCE PROGRAMS MEMORANDUM DATED NOVEMBER 27, 2006, AND SUPPLEMENTARY RESPONSE DATED APRIL 25, 2007

Attached is the Office of the Inspector General (OIG) analysis and status of the recommendations as discussed in the agency's responses dated November 27, 2006, and April 25, 2007. Based on these responses, recommendations 1 and 3 are resolved and will be closed pending completion of the actions contained in the agency's responses and OIG's review of those actions. Recommendation 2 is closed. We ask that your office provide an updated status of recommendations 1 and 3 by September 14, 2007.

If you have questions or concerns, please call me at 415-5915 or Tony Lipuma at 415-5910.

Attachment: As stated

cc: V, Ordaz, OEDO
M. Malloy, OEDO
P. Tressler, OEDO

**Audit Report**

**Evaluation of the NRC's Use of Probabilistic Risk Assessment in Regulating the Commercial Nuclear Power Industry**
**OIG-06-A-24**

**Status of Recommendations**

**Recommendation 1:** Develop and implement a formal, written process for maintaining PRA models that are sufficiently representative of the as-built, as-operated plant to support model uses.

**Agency Response Dated November 27, 2006:** Agree. The staff completed the Standardized Plant Analysis Risk (SPAR) Model Quality Assurance Plan, Revision 0, (SPAR Model QA Plan), and it became effective on September 15, 2006 (ML063070084) subsequent to the IG review. The agency established its formal quality assurance (QA) and configuration control plan using existing practices for SPAR model development. Section 7 of the SPAR Model QA Plan specifies that "each SPAR model will largely reflect actual plant design" and provides additional guidance to achieve that requirement. Use of the SPAR Model QA plan establishes a sufficient level of confidence in the SPAR models for the staff to support the agency's risk-informed regulatory activities (e.g., audit, review and screening tool). Currently, staff is reviewing the proposal to revise and update the SPAR models. The updates are based on recently identified Plant changes, which will be evaluated for risk significance. Note that SPAR models are not used as a basis for a licensee's licensing or design-bases activities.

In conclusion, the SPAR Model QA Plan implements a formal, written process for maintaining PRA models that are sufficiently representative of the as-built, as-operated plant to support model uses.

**Audit Report**

**Evaluation of the NRC's Use of Probabilistic Risk Assessment in Regulating the Commercial Nuclear Power Industry**
**OIG-06-A-24**

**Status of Recommendations**

**Supplementary Response Dated April 25, 2007:**

The initial response to this recommendation in my November 27, 2006 memorandum discussed and provided documentation on the Standardized Plant Analysis Risk (SPAR) model Quality Assurance (QA) plan and its implementation. The SPAR model QA plan provides reasonable assurance that the SPAR models used by NRC risk analysts and senior reactor analysts (SRAs) represent the as-built, as-operated plants to the extent intended within the scope of the SPAR models.

In the meetings between RES and Office of the Inspector General (OIG) staffs to discuss the response, the OIG staff raised a question about how the SPAR models are kept current to represent the plants and whether the processes for doing so were documented. The RES staff explained that the models are kept current via the supplemental verification activities that are routinely carried out as part of the analytic process associated with NRC risk applications, such as incident investigation (under Management Directive 8.3, "NRC Incident Investigation Program"), the Significance Determination Process (SDP), and Accident Sequence Precursor (ASP) evaluations. Regional inspectors and engineers who are knowledgeable of the as-built, as-operated plant are normally involved by the analyst to ensure that the SPAR model represents the current plant for the application.

**Audit Report**

**Evaluation of the NRC's Use of Probabilistic Risk Assessment in Regulating the Commercial Nuclear Power Industry**
**OIG-06-A-24**

**Status of Recommendations**

Guidance is provided to SPAR model users in the Risk Assessment of Operating Events Handbook to ensure analytic results are sufficiently representative of the as-built, as-operated plant. Specifically, the handbook provides guidance where SPAR models are used in incident investigations, SDP, and ASP evaluations. The use of the handbook for SDP Phase 3 risk assessments is recommended in Inspection Manual Chapter 0609, "Significance Determination Process."

Over the years, the NRC staff has developed processes that ensure that risk-based regulatory decisions are based on the as-built and as-operated plant. These processes include:

- The use of the draft Risk Assessment of Operating Events Handbook (more commonly referred to as the Risk Assessment Standardization Project or RASP Handbook) that provides guidance on basic principles of risk assessment, appropriate methodology (i.e., tool box of techniques), and documentation standards.

- An internal review of the risk evaluations by experienced analysts.

- A consensus review for major decisions and high-risk events, which ensures that both the licensee and the NRC are using state-of-the-art approaches and complete plant information.

Other means are also used to ensure that decisions made are based on the as-built and as-operated plant. These include:

**Audit Report**

**Evaluation of the NRC's Use of Probabilistic Risk Assessment in Regulating the Commercial Nuclear Power Industry**
**OIG-06-A-24**

**Status of Recommendations**

- The use of well-trained and experienced risk analysts with years of NRC or external PRA experience and who have taken NRC training courses (SRAs have been through a formal qualification program). Their backgrounds ensure that they know how to use and interpret PRA results in light of the current plant design and the event being analyzed. These analysts are also knowledgeable about potential PRA and SPAR model limitations, boundary conditions, and uncertainties in results.

- The expert support from our contractor Idaho National Laboratory (INL) as part of the RES-funded "help desk" for SPAR and Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) technology.

More specific details about the above processes are provided in Enclosure 1, "Additional Information on NRC Processes for Ensuring Risk-Based Decisions are Based on the As-Built and As-Operated Plant."

In summary, as discussed with the OIG, the revised RASP Handbook will provide a formal, written process for maintaining PRA models that are sufficiently representative of the as-built, as-operated plant to support model use. Revision 1 of the RASP Handbook will be completed during Calendar Year 2007.

**OIG Analysis:** The proposed corrective action addresses the intent of OIG's recommendation. Recommendation 1 will be closed when NRC provides evidence that its revised RASP Handbook is issued and implemented.

**Status:** Resolved.

**Audit Report**

**Evaluation of the NRC's Use of Probabilistic Risk Assessment in Regulating the Commercial Nuclear Power Industry**
**OIG-06-A-24**

**Status of Recommendations**

**Recommendation 2:** Develop and implement a fully documented process to conduct and maintain configuration control of PRA software (i.e., SAPHIRE, GEM).

**Agency Response Dated November 27, 2006:** Agree. Idaho National Laboratory (INL), NRC's contractor, documented this process in the Program[m]ers Workbench, SAPHIRE Development Manual (Enclosure 1), which was not provided to the Inspector General reviewers (Scientech). This document describes configuration management as—

> SAPHIRE software configuration is managed using a Revision Control System (RCS). An RCS allows developers to manage multiple revisions of files by keeping a complete history of the changes performed to the files. This allows the developer to see how and when a file was changed, or to quickly return to a previous revision of a file.

This configuration control approach is an acceptable practice commonly used by software developers.

In conclusion, the existing RCS satisfies the requirements for a fully documented process to conduct and maintain configuration control of PRA software (e.g., SAPHIRE, GEM).

**Audit Report**

**Evaluation of the NRC's Use of Probabilistic Risk Assessment in Regulating the Commercial Nuclear Power Industry**
**OIG-06-A-24**

**Status of Recommendations**

**Supplementary Response Dated April 25, 2007:** At a meeting with the staff on February 23, 2007, the OIG requested additional documentation with respect to Recommendation 2. Additional documents were provided to the OIG as listed in Enclosure 2. At a subsequent meeting, the staff explained to the OIG that at the time the OIG was performing the audit, the INL was developing a new software quality assurance program as a result of the split of Idaho National Engineering and Environmental (INEEL) into INL and the Idaho Cleanup Project.

On April 2, 2007, the new INL software quality assurance program was implemented. On April 5, 2007, the staff provided the OIG with confirmation of this action (by email and follow-up call) and with the following INL documents: INL Report PDD-13610, Rev. 2, "Software Quality Assurance Program," Effective Date April 2, 2007 and INL Report LWP-13620, Rev. 3, "Software Quality Assurance," Effective Date April 2, 2007. The INL's SAPHIRE development project will now make use of this new software quality assurance program. These documents will be incorporated into NRC statements of work to ensure continued use. Thus, a fully documented process to conduct and maintain configuration control of PRA software (i.e., SAPHIRE, GEM) has been developed and implemented.

We consider actions to address this recommendation to be completed.

**OIG Analysis:** The proposed corrective action addresses the intent of OIG's recommendation. Based on NRC's documentation and implementation of the new INL software quality assurance program this recommendation is closed.

**Status:** Closed.

**Audit Report**

**Evaluation of the NRC's Use of Probabilistic Risk Assessment in Regulating the Commercial Nuclear Power Industry**
**OIG-06-A-24**

**Status of Recommendations**

**Recommendation 3:** Conduct a full verification and validation of SAPHIRE Version 7.2 and GEM.

**Agency Response Dated November 27, 2006:** Disagree. In the staff's judgment, SAPHIRE version 7 is sufficiently tested and benchmarked to support current use so that the staff may focus on implementing SAPHIRE version I. Version 8 will satisfy the requirements described in the audit report for test documentation. The agency decided several years a go to perform limited validation and verification (V&V) on SAPHIRE version 7.2. It is impractical to "fully" test every feature and option under all different conditions in any complex system. INL compared the test, verification, and validation (TV&V) process for SAPHIRE version 7 to IEEE Standard 1012-1988, "IEEE Standard for Software Verification and Validation Plans," and documented its findings in "Comparison of the SAPHIRE TV&V to the IEEE V&V Process," dated may 20, 2003 (Enclosure 2). The staff did not provide this report to the Inspector General reviewers (Scientech). In the comparison, INL documented how the SAPHIRE TV&V does and does not satisfy the IEEE requirements. While extensive testing documentation exists related to each incremental release of SAPHIRE, not all parts of the IEEE Standard documentation are currently in place. Once key reason the SAPHIRE TV&V does not satisfy the IEEE requirements is a lack of a formal definition of "software integrity levels" as defined in the Standard. INL has tested all vital features of SAPHIRE in the version 7 series. TV&V, as well as experience through the staff's use of SAPHRIE in conjunction with the SPAR models for risk-informed regulatory activities (e.g., Reactor Oversight Process (ROP), Significance Determination Process (SDP), Management Directive (MD) 8.3, the Accident Sequence Precursor (ASP) program, and risk-informed license

amendment reviews) has demonstrated that SAPHIRE does perform accurate probabilistic risk assessment (PRA) analysis calculations.

**Supplementary Response Dated April 25, 2007:** At a meeting with the staff on February 23, 2007, the OIG acknowledged that performing a full verification and validation (V&V) of SAPHIRE Version 7 would not be justified at this time due to the development schedule for SAPHIRE Version 8. The INL recommended the implementation of four recommendations from INEEL Report No. CCN 42566, "Submittal of Final Report under Job Code Number (JCN) Y6394, Task 8," dated May 30, 2003, for the SAPHIRE Project verification and validation. These recommendations are consistent with the Institute of Electrical and Electronics Engineers Standard for Software Verification and Validation 1012-1998. Subsequent discussions with the OIG staff indicated that the addition of these four recommendations, combined with code testing, would satisfy full verification and validation of SAPHIRE Version 8. The INL will implement these recommendations as requested by the NRC statement of work for JCN N6423 (SAPHIRE Version 8). Beta testing is anticipated to take 1 to 2 years. No general release date for SAPHIRE Version 8 has been set at this time, although it is anticipated in CY 2009. Because V&V efforts will continue throughout the software development process, this recommendation will remain open until Version 8 is released.

**OIG Analysis:** The proposed corrective action addresses the intent of OIG's recommendation. Recommendation 3 will be closed when NRC releases Version 8.

**Status:** Resolved.