**Department of Energy**
Washington, DC 20585

October 31, 2008

Mr. Michael Kluse
Battelle Memorial Institute
Laboratory Director
Pacific Northwest National Laboratory
P.O. Box 999
Richland, Washington 99352

Dear Mr. Kluse:

From June 24 through June 26, 2008, the Office of Health, Safety and Security's Office of Enforcement conducted an onsite integrated program review of the Pacific Northwest National Laboratory (PNNL) regulatory compliance assurance programs. Our review included an evaluation of Battelle Memorial Institute's (Battelle) processes for identifying noncompliances; reporting and tracking noncompliances in the Noncompliance Tracking System, Safeguards and Security Information Management System, and internal tracking systems; and correcting deficiencies to prevent recurrence. The Office of Enforcement also conducted a limited review of Battelle's management and independent assessment programs.

The integrated approach, used by Battelle, to implement your U.S. Department of Energy (DOE) Regulatory Compliance Program provides common processes across all enforcement disciplines (worker safety and health, nuclear safety, and classified information security) and benefits from direct access to senior management. In addition to the longstanding nuclear safety regulatory program, PNNL has established many important elements of an effective worker safety and health and classified information security regulatory compliance monitoring and reporting program. In addition to strengthening PNNL's culture of personal accountability, leadership is focused on integration of multiple processes to fulfill DOE noncompliance identification and reporting expectations. The results of this review, described in the enclosed report, revealed strengths and weaknesses in each of the enforcement disciplines.

Failure to correct the weaknesses noted in this report may result in a potential reduction or loss of mitigation as described in DOE's Enforcement Policies (10 C.F.R. Part 820 appendix A, 10 C.F.R. Part 851 appendix B, and 10 C.F.R. Part 824) for any future enforcement action against Battelle. In addition, should these weaknesses persist, the Office of Enforcement would be less likely to exercise enforcement discretion for noncompliance issues that are of lesser significance.

Printed with soy ink on recycled paper

No reply to this letter is required. If you have any questions regarding this review, please contact me at (301) 903-2178.

Sincerely,

Martha S. Thompson

Martha S. Thompson
Acting Director
Office of Enforcement

Enclosure

cc: Sandy English, PNNL

ENCLOSURE

# OFFICE OF ENFORCEMENT
# INTEGRATED PROGRAM REVIEW
# PACIFIC NORTHWEST NATIONAL LABORATORY

## I. Introduction

During June 24-26, 2008, the Office of Enforcement conducted an onsite integrated program review (IPR) of the regulatory compliance assurance programs implemented by Battelle Memorial Institute (Battelle) at the U.S. Department of Energy's (DOE) Pacific Northwest National Laboratory (PNNL). This review included an evaluation of PNNL's processes for identifying noncompliances; reporting and tracking noncompliances in the Noncompliance Tracking System (NTS), the Safeguards and Security Information Management System (SSIMS), and internal tracking systems; and correcting deficiencies to prevent recurrence. It also included a limited review of PNNL's management and independent assessment programs and an evaluation of PNNL's efforts to improve the regulatory compliance assurance program following the Price-Anderson Amendments Act (PAAA) program review that was conducted by the Office of Enforcement in 2005.

## II. General Implementation

Battelle (hereinafter referred to as PNNL) is transitioning from the PAAA terminology to the term "DOE Regulatory Compliance Program" (DRCP) to collectively describe the functions associated with its nuclear safety, worker safety and health, and classified information security compliance assurance program. PNNL has drafted a new program description that integrates the three DOE enforcement disciplines (nuclear safety, worker safety and health, and classified information security). The program description highlights the major aspects of each enforcement process as it applies to PNNL, and describes the implementation mechanisms deployed by the laboratory to fulfill DOE noncompliance identification and reporting expectations. With further refinement, this integration should result in increased reporting efficiency and improved analysis of worker safety, nuclear safety, and classified information security issues.

PNNL implements a decentralized noncompliance identification and reporting program, with screening of issues performed by representatives within the various PNNL divisions. Issues that may be NTS reportable as safety noncompliances are referred to the DRCP Manager for a final determination. The security enforcement screening and reporting function, previously contained solely within the Safeguards and Security Division (SSD), was recently (within the past year) included in the PNNL regulatory compliance program. PNNL's approach to implementing the DRCP relies on common processes for laboratory-level assessments, reporting, issues management, and corrective actions to promote integration of the three regulatory disciplines (nuclear safety, worker safety, and classified information security). Integrating the three disciplines helps the DRCP Manager to monitor assessment results, evaluate the effectiveness of corrective actions, and trend noncompliance data.

The DRCP Manager is organizationally located within the Quality and Performance Management Directorate and has regular meetings with and ready access to the PNNL Chief Operating Officer. The DRCP Manager is supported by a DRCP Working Group, which includes representatives from each line and support division and evaluates events for NTS reportability. The DRCP Manager provides overall direction and administration of the DRCP, chairs the DRCP Working Group, and performs routine oversight of the implementation of the screening and reporting program.

Over the 2007-2008 timeframe, the DRCP Manager performed multiple self-assessments that focused on various aspects of the nuclear safety screening and reporting program. In addition, in January 2008, PNNL's Independent Oversight Office conducted an assessment of the implementation and effectiveness of its worker safety and health program that was led by an independent assessor from outside PNNL. The assessment included team members (including an enforcement coordinator) from another DOE site and employed the checklists developed by the Energy Facility Contractors Group (EFCOG) for peer program reviews as part of the assessment. Similarly, in February 2008, the DRCP Manager and representatives from the SSD conducted a management assessment of PNNL's security programs using the peer review question set developed by the EFCOG. The results of that security self-assessment identified areas that need improvement, including effectiveness reviews, corrective action plans, and the causal analysis process.

The enforcement program description mentioned above was updated and is in draft; however, the role of the DRCP Manager, as it relates to security enforcement implementation, has yet to be formally defined or documented. With respect to security enforcement, the DRCP Manager views her role as providing enforcement guidance and expertise for causal analysis and assistance to SSD.

Two levels of nuclear safety enforcement-related training are provided by PNNL. The PAAA Overview training (course 1300) is required for product line managers, project managers for work with PAAA implications, and personnel performing PAAA screening. Course 1595, involving interactive scenario reviews, is required for personnel performing noncompliance screens. At the discretion of the DRCP Manager, PAAA training may also be recommended for other groups. Two individuals responsible for issue screening had not received the PAAA screening training (course 1595), and one individual who received the training, showed deficiencies in knowledge of the types of potential noncompliances and the screening checklist used. Additionally, 10 C.F.R. Part 824 is included as a component of security education in several forums, including the required annual security education training for all employees.

The following general program strengths were noted:

- Senior management has been engaged in and recognized the need to recalibrate and to develop standards for corrective action plans. PNNL leadership recognized a significant shortcoming and was candid about quality problems discovered in corrective action plans. If uncorrected, these problems could have led to recurrent noncompliant conditions. This open admission is significant. It exemplifies not only management attention and accountability, but leadership in doing the right thing for the betterment of the worker environment and protection of national security assets.

- Senior management and division line managers demonstrate awareness of and support for the processes for identifying, evaluating, and addressing events and conditions that impact safety and security performance. Managers within the research and support directorates are familiar with the DRCP and the activities of the DRCP Manager. Safety and health managers reflected a high level of personal interaction and discussion relating to screening and reporting of nuclear safety (PAAA) and worker safety and health conditions.

- PNNL's assessment process has been refocused to better account for activity- and project-based assessments. In addition, PNNL leadership is working to ensure that personnel move from event-driven issues to self-identified issues and to resolve management performance issues, as well as attempting to solve staff frustration with complicated procedures and processes, via development of the "How Do I" system.

- The DRCP Manager is experienced, effectively communicates enforcement-related issues to the cognizant Associate Laboratory Director and among the PNNL staff, and is taking positive actions to facilitate the full integration of worker safety and health and classified information security programs with the existing nuclear safety program. The DRCP Manager regularly communicates with PNNL senior managers on significant issues and events. This practice facilitates senior management awareness of safety and security conditions and the status of corrective actions taken in response to noncompliant conditions.

- PNNL has developed a detailed and rigorous standard for the qualification of causal analysts. The PNNL standard includes formal training requirements, mentored experience requirements, establishes a requirement for a qualification board, and also identifies re-qualification frequencies. The requirement for analysts to be qualified to the new standard is being phased in and was scheduled to be fully implemented by October 1, 2008.

- Expertise associated with nuclear safety lessons learned and causal analysis processes is being applied to the evaluation of security noncompliances.

The following weaknesses were noted:

- Although employee concern program (ECP) procedures have been revised, the current revisions do not specifically address required communications when an instance of retaliation is substantiated. Documents reviewed during the IPR identified a substantiated "potentially retaliatory" action but the information had not been communicated to the DRCP Manager for review.

- The role and responsibilities of the DRCP manager, as they relate to security enforcement, have yet to be formally defined and documented.

## III. Identification and Screening/Categorizing

PNNL uses a wide variety of data streams as sources of safety and health noncompliance and performance information. These data streams include: the Integrated Operations System (IOPS) tool, employee call number data (events), injury and illness reports, and internal and external assessments. Potential nuclear safety noncompliances are identified through a variety of mechanisms, such as assessments, quality problem reports, radiological problem reports, employee concerns, events, and IOPS self-assessment checklists.

Screening for noncompliances is performed by designated individuals within the laboratory directorates using a decentralized approach. Additionally, subject matter experts (SME) in the support organizations have responsibility for screening potential noncompliances (e.g., the radiological control organization screens all radiological deficiencies and radiological problem reports).

Conditions that require action are entered by division representatives into the Assessment Tracking System (ATS). Those with a potential safety or security impact are assumed to be "noncompliances" (i.e., all of the conditions assigned to the safety and health category are assumed to represent noncompliances regardless of whether there is an actual noncompliance) and assigned a category for tracking and trending. If the nuclear or worker safety and health condition appears to meet the criteria for NTS reporting, it is expected to be forwarded to the DRCP Manager for review and possible evaluation by the DRCP Working Group. The DRCP Manager also performs independent reviews of the ATS to evaluate the effectiveness of line management in identifying a nuclear safety relationship and the elevation of issues for potential NTS reporting.[1]

PNNL's Incidents of Security Concern Program is defined in a formal procedure that includes a process for the prompt review of all events and the actions required by the SSD staff. Approximately 90 percent of security incidents are self-reported through the Operations Center.[2] In addition to mandatory security event reporting, all security noncompliances, including self-

[1] In addition, the DRCP reviews a multitude of documents to stay informed of current operations within PNNL and lessons learned from other DOE sites.

[2] The Operations Center technician promptly notifies the designated inquiry official and an immediate determination is made regarding the need for containment or mitigation if the incident involves a potential for mishandling or compromise of classified matter.

assessment results, are entered into ATS, to include the specific noncompliance citation and Impact Measurement Index (IMI) categorization.

**Worker Safety and Health**

The following weaknesses were noted:

- PNNL has multiple, well-established processes for identifying and documenting safety and health related conditions and events through a variety of reporting mechanisms. However, much of this information (e.g., IOPS assessments) is not being evaluated to determine whether there are regulatory noncompliances. Safety and health conditions that are entered into ATS with potential 10 C.F.R. Part 851 implications are designated by a particular category in the system, but this does not necessarily result in the information being screened for noncompliances. PNNL indicated that it is taking a conservative approach by assuming that all of those conditions represent regulatory noncompliances. As a result of this approach, PNNL does not have an accurate indication of its compliance status relative to 10 C.F.R. Part 851.

- PNNL does not adequately document in their screening worksheets the rationale for determining that a noncompliance has or has not occurred. The screening forms do not generally specify the regulatory requirements that were considered in deciding whether a noncompliance occurred. Thus, it is not possible to readily determine that the reported safety condition was properly evaluated against the applicable requirements.

- A number of the worker safety and health events and conditions captured in ATS appeared to be incorrectly categorized. For example, several incidences that were related to electrical safety deficiencies were labeled as "Housekeeping." This weakness may be impacting the quality of PNNL's trending of safety conditions and its ability to effectively target areas for improvement.

**Nuclear Safety**

Identified nuclear safety conditions are entered and tracked in ATS. For the majority (approximately 75 percent) of nuclear safety-related issues, the results of the screening process are documented on an organization-specific checklist or form. In some cases, however, the issue is simply annotated as PAAA applicable on the ATS system, without additional documentation of the screening results.

The following strength was noted:

- As in the 2005 Office of Enforcement program review, PNNL continues to be routinely conservative in identifying issues as PAAA applicable.

The following weaknesses were noted:

- For the nuclear safety issues that are screened without a supporting checklist, screening decision documentation is limited and does not include identification of the specific citation for the noncompliance and the initial reportability evaluation.

- The DRCP Manager has not reviewed all of the screening forms used by the various organizations that perform screening since 2006. The Office of Enforcement reviewed the PAAA screening checklist (dated September 10, 2005) used by the Facilities and Operations division and noted that the "and" and "or" connectors for screening potential 10 C.F.R. Part 830 issues have the potential to screen out valid 10 C.F.R. Part 830 noncompliances. This appeared to be a problem with the checklist only; as noted above, PAAA applicability decisions appeared to be routinely conservative.

- In several instances, the screening results for radiological events did not identify apparent violations of 10 C.F.R. § 835.104 (involving failure to comply with radiological procedures). However, these examples were routinely categorized as violations of 10 C.F.R. Part 830 and were, therefore, included as PAAA noncompliances.

- PAAA applicability of ATS items is flagged without distinction as to whether the item is a noncompliance, an issue, or a positive finding; the database includes all three. Consequently, there is no way to sort for PAAA noncompliances.

**Security**

The Incidents of Security Concern Program Manager is responsible for determining the appropriate categorization of security incidents; these responsibilities are documented in the formal procedure. While this process has been implemented, the Classified Matter Protection and Control (CMPC) Program Manager and the Cyber Security Manager (who are SMEs for their respective programs) have not been consulted in the categorization of security incidents dealing with their specific subject matter.

IMI categorizations of security incidents are accomplished within the required 24-hour timeframe; however, PNNL has defined a "near miss" category that can, in some instances, overlap with the IMI table reporting (required by Departmental policy). For example, introduction of a controlled article (i.e., cellular phone) into a security area has, in some cases, been inappropriately categorized as a "near miss" –rather than as a reportable IMI-4.14. In the past 3 years, 93 security incidents have been categorized as "near misses." If the "near miss" category continues to be used by PNNL, this process needs to be formalized as a policy deviation and approved by the cognizant security authority.

A review of PNNL's listing of IMI-4s that occurred over the past 24 months called into question some of the categorization determinations, specifically those categorized as IMI-4 non-reportables. Procedures, including SAP-513, do not define the process for this categorization. The categorization was based on mitigating factors that ruled out confirmed or potential compromise of classified information, and the use of this category has ceased since the update of the PNNL procedures in March 2008.

The Office of Enforcement's review of ten security incident files, categorized as IMI-4 non-reportable in fiscal years (FY) 2006 and FY 2007, confirmed the concerns about the accuracy of the categorization of these incidents. For example, one of the incidents reviewed involved a compact disk containing Secret/Restricted Data that was left unattended for three days in a Limited Security Area; PNNL categorized this incident as IMI-4 non-reportable, although it clearly met a higher IMI reporting threshold. In addition to the categorization concern, no adequate documentation was found in the files to support the determination of "no compromise" based on mitigating factors. Furthermore without the accurate categorization of security incidents, PNNL may not conduct a complete, documented inquiry process, formal causal analysis, or develop appropriate corrective actions. These concerns also bring into question the potential effectiveness of PNNL's trending of security incidents.

The following weaknesses were noted:

- PNNL's use of an additional security incident categorization, the "near miss," is not consistent with DOE reporting requirements, and no policy deviation has been approved to allow its use.

- During incident categorization, not all subject matter expertise is involved in the decision-making process.

- A review of FY 2006 and FY 2007 security incidents revealed a lack of documentation to support the conclusions of "no compromise" and the resulting IMI categorization. Further, the categorization of IMI-reportable incidents is not consistent with Departmental policy and, therefore, calls into question the accuracy of the current trending.

## IV. Evaluation of NTS and Security Reportability

Issues identified as being potentially reportable by the line and support divisions are forwarded for evaluation to the DRCP Working Group. The DRCP Working Group, with representatives from the research and support divisions, reviews issues screened as potentially reportable to the NTS and makes a final recommendation regarding such reportability. The DRCP Working Group meets monthly and includes senior representatives from the various laboratory line and support organizations that perform screening activities. The DRCP Working Group meetings are routinely attended by Pacific Northwest Site Office (PNSO) representatives. DRCP Working Group meeting minutes indicate that, in addition to reviewing identified deficiencies for applicability or reportability, the group routinely discusses overall performance and trending and lessons-learned information (for example, results of enforcement actions and program reviews at other sites).

Metrics maintained by PNNL for the period FY 2006 through the second quarter of FY 2008 identified that overall a slight majority (52 percent) of NTS reports communicated self-identified issues (versus those less preferably identified through events or external reviews). However this percentage of self-identified issues has declined significantly over the period (100 percent in FY 2006, 57 percent in FY 2007, and 25 percent in 2008) indicating the need for continuing attention to this metric by PNNL.

PNNL has recently started entering security incident data into SSIMS. A review of SSIMS data identified three entries over the past 24 months: two are closed, and one is pending completion of a final inquiry report. The open incident is within the requisite 60 days for completing the inquiry process.

The following strengths were noted:

- The DRCP Manager consults with SMEs from a number of PNNL organizations for technical expertise and regulatory applicability support. This practice enhances the evaluation of events for regulatory compliance impact and provides ongoing feedback to SMEs on incidents that may warrant further consideration for programmatic or procedural improvements.

- The DRCP Working Group, in addition to evaluating reportability, provides an effective opportunity for sharing enforcement lessons learned. The DRCP Working Group meeting minutes include multiple examples in which enforcement actions or NTS reports from other sites were discussed among the DRCP members for dissemination back to PNNL divisions.

- PNNL's reporting approach includes a streamlined process for events that are NTS reportable based on Occurrence Reporting Processing System (ORPS) categorization. This approach results in more timely identification and correction of noncompliant conditions. The DRCP Manager generates a draft NTS report for review and comment by the DRCP Working Group prior to submission to the Laboratory Chief Operating Officer for approval.

**Worker Safety and Health**

No strengths or weaknesses were noted.

**Nuclear Safety**

The following weaknesses were noted:

PNNL's NTS reporting does not meet the Office of Enforcement's 20-day guideline for prompt reporting. Metrics maintained by the DRCP Manager indicate an average of approximately 45 days from identification of a noncompliance to NTS entry.

- Two recent PNNL issues (extremity exposure event and worker retaliation concern) were viewed by the Office of Enforcement as potentially meeting reporting thresholds; neither of the issues was reported to the NTS. The extremity exposure event had been reviewed by the DRCP Working Group and did not exceed ORPS-based reporting thresholds; however, the Office of Enforcement views the multiple procedural and communication breakdowns in that event as representing a "vertical" programmatic issue that meets the programmatic reporting threshold.

Office of Enforcement review of the ECP database identified a recent staff concern which was dispositioned as "substantiated" and potentially retaliatory per PNNL policy and 10 C.F.R. Part 708. The results of the ECP investigation, however, had not been communicated to the DRCP Manager and the DRCP Working Group, and consequently the concern had not been evaluated for reportability in a timely fashion. Subsequent PNNL review concluded the concern did not represent a 10 C.F.R. Part 708 noncompliance; however, this review was prompted by the Office of Enforcement's communication of the issue.

### Security

No strengths or weaknesses were noted.

## V. Corrective Action Management

This review was performed to determine whether PNNL conducted effective causal analyses, implemented appropriate corrective actions, and performed suitable effectiveness reviews. PNNL requires formal tracking and closure of corrective actions associated with unwanted conditions. NTS corrective action development and tracking are included in the PNNL Standards Based Management System (SBMS).

In addition to tracking security incidents and survey/inspection findings in SSIMS, PNNL uses ATS to consolidate all security incidents; findings; corrective actions, including formal validation and closure; and process improvements.

### A. Causal Analysis

Roles, responsibilities, and the general process for conducting a causal analysis are contained in an SBMS procedure, "*Conducting a Causal Analysis*," dated August 2005.

### Worker Safety and Health

Since May 25, 2007, PNNL has submitted six NTS reports that were categorized as worker safety and health (individually or combined with nuclear safety). Two reports were associated with self-disclosing events, whereas the remaining four were contractor-identified conditions resulting from an internal assessment. To evaluate the effectiveness of the management of corrective actions in this area, the Office of Enforcement reviewed two of the more significant PNNL NTS reports and an ORPS event with possible regulatory implications.[3] In both NTS

[3] NTS-RL—PNNL-PNNLBOPER-2008-0001, Lock and Tag Procedural Noncompliance (LOTO); NTS-RL—PNNL-PNNLBOPER-2007-0003, Weaknesses in the Implementation of the Pressure Safety Program; SC—PNSO-PNNL-PNNLBOPER-2007-0009, Damaged Direct-Buried 277V Cable Encountered During Sprinkler Repair

cases and the ORPS events that were reviewed, causal analyses were performed in accordance with established procedures and reflected the appropriate depth and breadth of analysis.

No specific strengths or weaknesses were noted.

### Nuclear Safety

The following strengths were noted:

- PNNL has established an Independent Internal Review committee, consisting of senior-level operational managers, to evaluate developed corrective action plans and their completion status. Reviews conducted by the team have identified the need to improve corrective action plan development (see next bullet).

- The May 2008 revision to the subject area of *Issue Management* provided additional emphasis and guidance on the development of corrective action plans. The subject area requires that developed corrective actions meet a SMART standard (specific, measurable, accountable, reasonable, and timely).

### Security

A review of recent IMI-2 and 3 incidents found thorough inquiry reports, causal analyses, and corrective action plans. The current causal analysis process appears effective and has incorporated lessons learned from past nuclear safety events.

The following strengths were noted:

- PNNL's use of ATS for tracking security-related issues is assuring that appropriate oversight and resources are being deployed to address identified program security weaknesses. In addition, all listed security noncompliance entries in ATS identify the specific DOE directive or policy citations.

- The security approach for causal analysis is noteworthy for seeking engineered solutions rather than solely depending on administrative controls to address recurring security concerns. For example, based on a causal analysis, PNNL decided to selectively use a "secure safe" to monitor whether a security repository is opened or closed, which has significantly reduced the number of security incidents involving open and unattended safes. Based on this success, PNNL plans to implement the system throughout the laboratory.

The following weakness was noted:

- PNNL's methodologies for the conduct of causal analysis, relative to classified information security events/conditions, are formally defined; however, PNNL relies upon only one individual as it relates to security event causal analysis.

## B. Corrective Actions

### Worker Safety and Health

The worker safety and health corrective actions associated with both NTS cases and the reviewed ORPS event appear to correlate to the root, direct, and contributing causes. Corrective actions were entered into and tracked to closure in ATS, and ATS tracking numbers are also identified in the associated ORPS reports. Corrective actions were completed either ahead of schedule or on time.

### Nuclear Safety

The DRCP Manager monitors NTS-related corrective action completion activity by the various action owners. Although metrics maintained by the DRCP Manager indicate that more than 95 percent of NTS corrective actions were closed on time (for FY 2008), the DRCP Manager has identified an excessive number of deadline extensions associated with such NTS-related actions. In response, PNNL is currently revising the NTS corrective action extension process to require a higher level of management approval for such extensions, thereby strengthening the process.

### Security

PNNL tracks security incidents and survey/inspection findings in SSIMS and also uses ATS to consolidate all security incidents, findings, and process improvements and to track corrective actions through completion, including formal validation and closure. The progress and completion of corrective actions are monitored and reported to PNSO and the Safeguards and Security Director, and SSD Managers validate closure after SME review.

The following strength was noted:

- The PNNL process for tracking security incidents and survey/inspection findings is robust and effectively integrates with ATS.

## C. Report Closeout

Upon completion of NTS-related corrective actions, the DRCP Manager schedules a closeout meeting with the PNSO enforcement coordinator and the responsible action owner/manager. The DRCP Manager prepares a closeout book that includes documented evidence of corrective action closure. During the closeout meeting, the action owner/manager presents the case that the corrective actions have been completed and are adequate to address the issue. PNNL prepares a formal closure package and presents the package to PNSO. PNNL Safeguards and Security also prepares a formal closure package for survey findings and presents the package to PNSO for validation and closure.

### Worker Safety and Health

No strengths or weaknesses were noted.

### Nuclear Safety

As part of the current evaluation, closure documentation for a sample of completed NTS reports was reviewed. Documentation was found to be complete and maintained in a logical manner in a central location.

### Security

The following strength was noted:

- SSD managers validate all corrective actions deemed closed by the SMEs within their assigned topical area. This system is robust and effective.

## VI. Assessment Program

As part of this IPR, the Office of Enforcement evaluated the implementation of PNNL assessment programs, since an effective assessment program is the most proactive method to identify and address safety and classified information security problems before they result in serious incidents. The Office of Enforcement's review in this area was limited in scope and does not constitute a comprehensive evaluation of the assessment program.

### Worker Safety and Health

The following strengths were noted.

- The IOPS provides a mechanism for performing space- and activity-based assessments and identifying potential safety noncompliances. The IOPS assessments applicable to a particular work activity or location are tailored according to the hazards identified during the job planning process, providing an advantage over general, non-specific safety evaluation tools.

- PNNL's assessment processes provide a large set of safety performance data that is used to proactively identify, analyze, and trend incidents and conditions for potential safety deficiencies. These assessments range from focused, laboratory implementation-based inspections to programmatic, management systems reviews to evaluate the effectiveness of laboratory-level procedural requirements.

- PNNL has implemented procedures for evaluating and overseeing onsite subcontractors to ensure that they perform work in accordance with laboratory and DOE safety requirements. PNNL Office of Internal Audit performed an audit in September 2007 of construction management practices to ensure that subcontractors retained by PNNL were adhering to 10 C.F.R. Part 851 requirements and that PNNL oversight was adequate.

**Nuclear Safety**

PNNL is on schedule to complete management-level assessments of all 10 C.F.R. Part 835 functional areas within the 3-year period. The Office of Enforcement reviewed two management assessment activities associated with technical safety requirement (TSR) implementation at the Radiochemical Processing Laboratory (RPL), which categorizes checklist assessment findings within their various labs on a risk basis and tracks cumulative risk per lab, using a color-coded facility map. The RPL TSR assessments focused only on whether programs and procedures were in place to implement the administrative TSRs and did not evaluate compliance with the requirements. After discussions with PNNL representatives (including RPL management) and review of additional assessment data, the Office of Enforcement concluded that collectively, TSR implementation was being adequately assessed.

The following strengths were noted:

- The PNNL independent assessment program has improved in response to previously identified weaknesses. During the Office of Enforcement program review in 2005, significant deficiencies were noted in PNNL's independent assessment program, ultimately resulting in an enforcement action (EA 2008-01). Corrective actions have since been completed, and the earlier deficiencies appear to be resolved. Corrective actions included the designation of a new manager, an organizational realignment (the Independent Oversight office now resides within the Quality and Performance Management Division), and augmentation of staff assessment resources. A strategic assessment scheduling approach has been developed, and, during the last completed assessment period (April 2007-March 2008), 14 of 15 planned assessments were completed and issued (one assessment was withheld due to quality concerns with the report).

- PNNL has incorporated an error precursor review into their checklist for performing activity-based assessments.

- The quarterly analysis of assessment data is comprehensive and is providing information for strategic decision making related to revisions of the assessment process. In a similar vein, the RPL analysis of assessment data and determination of cumulative risk by lab area allows for the timely refocusing of assessment activities and increased management emphasis.

- PNNL implements a comprehensive program for the trending of radiological problem reports. The Office of Enforcement's staff also noted through discussion with radiological control management that repeat issues not meeting the statistically established threshold for a positive trend were still receiving investigation and follow-up (an example was noted with respect to continuous air monitor alarms).

The following weakness was noted:

- An April 2007 assessment of the external dosimetry program was conducted by the SME within the radiological controls organization with responsibility for external dosimetry. This conflicts with the requirements for separation of duties in the controlling PNNL procedure (SHP-3.02, *Safety and Health Self-Assessments*) and in recommended DOE guidance (*DOE Guide 441.1-1c*). In fact, five out of the thirteen 10 C.F.R. Part 835 subject area assessments conducted thus far, in the 3-year assessment cycle, have been conducted by the SME for that area.

### Security

Procedure SAP-801 establishes the processes, responsibilities, controls, and methods for performing SSD self-assessments in order to provide assurance that security interests and activities are protected at required levels and to provide a basis for line management to make decisions regarding safeguards and security program implementation. Whenever possible, SSD utilizes both external (i.e., PNNL National Security Directorate or other "sister" Laboratory personnel) and internal SSD staff to form their self-assessment teams.

PNNL also conducts trending of security assessment/survey results, including applicable line management assessments.[4] The trending results are incorporated into the biennial self-assessment report under the Program Management and Planning Section or as a separate report. The trending data was comprehensive and could be useful as a management tool to assess the effectiveness of the PNNL Safeguards and Security Program. However, concerns regarding the categorization process (see Section III, Security) bring into question the effectiveness of the trending of security incidents program. Annually, the Security Incidents Program Manager distributes a detailed trending report that provides incident information to PNNL senior management, line management, SSD management, the CMPC program manager, and the Security Education and Awareness specialist.[5]

Currently, PNNL's security incident trending process is not integrated to include results from the various security activities (assessment program, incident program, external reviews, etc.) that are conducted throughout the year.

The following strengths were noted:

- The self-assessment process is comprehensive, and employs external resources to provide the benefit of a fresh look at the PNNL security programs. The self-assessment process provides an effective compliance- and performance-based evaluation of the PNNL Safeguards and Security Program.

- The implementation of a formal validation process for closure of security deficiencies was found to be effective.

[4] The process for this trending is addressed in SAP-801.

[5] The process for trending incidents of security concern is addressed in SAP-513.

The following weakness was noted:

- The DRCP Manager stated that a review of the self-assessment process had been conducted by SSD; however, the DRCP Manager is not given the results of topical/subtopical assessments as they are completed throughout the year, which reflects a lack of full integration at this time.

- PNNL's security incident trending process is not comprehensive, in that it does not include results from the various security activities (assessment program, incident program, external reviews, etc.) that are conducted throughout the year.

## VII. Conclusion

With respect to worker safety and health, PNNL has established some important elements of an effective worker safety and health regulatory compliance monitoring and reporting program. In order to meet the Office of Enforcement's expectations, PNNL needs to formalize the noncompliance screening process for all of its data streams to ensure that noncompliances are being appropriately identified, tracked, and corrected. PNNL's approach in considering all "safety and health conditions" requiring an action as noncompliances does not provide an accurate representation of regulatory compliance across the laboratory and does not facilitate the identification, correction, and trending of noncompliant conditions. PNNL should identify and associate specific 10 C.F.R. Part 851 requirements, including those identified in §§ 851.23, 851.27, and appendix A, with identified conditions and corrective actions. This is necessary to ensure that repetitive and programmatic issues that are associated with regulatory requirements or have regulatory implications are identified promptly and to ensure that noncompliant conditions are corrected effectively through institutional controls, such as SBMS or operating procedures to prevent recurrence.

The PNNL nuclear safety noncompliance identification and reporting process is generally sound and well-established. Screening decisions are routinely conservative and the majority of NTS reporting decisions appear appropriate. The DRCP Working Group is providing an effective forum for the discussion and dissemination of enforcement lessons-learned. Significant improvement was noted in the management support for and implementation of the independent assessment program. Several specific weaknesses were noted, including weaknesses in the timeliness of NTS reporting, the level of documentation of a subset of screening decisions, and the independence of 10 C.F.R. Part 835 assessments. Although these areas should be addressed, overall implementation of the nuclear safety identification and reporting process was viewed as satisfactory.

The security enforcement program is in the initial stages of integration with the PNNL enforcement program. The DRCP Manager has recently become involved with the security incident and security self-assessment programs. Notable strengths include the use of external SMEs in the comprehensive self-assessment program, and the use of ATS, which gives management a real-time status of program deficiencies and specific noncompliance citations. A significant weakness involves the less-than-accurate categorization and reporting of security incidents. Inaccurate categorization and the use of the laboratory "near miss" category have the potential to greatly impact the identification of adverse trends and the implementation of corrective actions.