



Department of Energy
Washington, DC 20585

January 23, 2009

Mr. Chuck Munns
President and Chief Executive Officer
Savannah River Nuclear Solutions, LLC
6160 Woodside Executive Court
Aiken, South Carolina 29803

Dear Mr. Munns:

From September 23 through September 26, 2008, the Office of Health, Safety and Security's Office of Enforcement conducted an onsite integrated program review of the Savannah River Nuclear Solutions, LLC (SRNS) regulatory compliance assurance programs. Our review included an evaluation of 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 SRNS management and independent assessment programs.

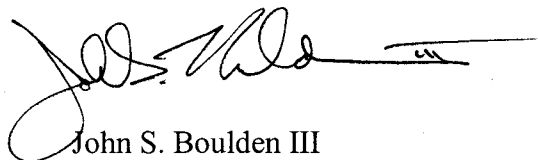
The integrated approach, used by SRNS, to implement your U.S. Department of Energy (DOE) Regulatory Compliance Program provides common processes across all enforcement disciplines (worker safety and health, nuclear safety, and classified information security) and benefits from direct access to senior management. 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 SRNS. 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.



No reply to this letter is required. If you have any questions regarding this review, please contact me at (301) 903-0324.

Sincerely,

A handwritten signature in black ink, appearing to read 'John S. Boulden III', with a long horizontal flourish extending to the right.

John S. Boulden III
Acting Director
Office of Enforcement
Office of Health, Safety and Security

Enclosure

cc: William Luce, SRNS

**OFFICE OF ENFORCEMENT
INTEGRATED PROGRAM REVIEW
SAVANNAH RIVER NUCLEAR SOLUTIONS, LLC**

I. Introduction

During September 23-26, 2008, the Office of Enforcement conducted an onsite integrated program review (IPR) of the regulatory compliance programs implemented by Savannah River Nuclear Solutions, LLC, (SRNS) at the U.S. Department of Energy's (DOE) Savannah River Site. This review included an evaluation of SRNS'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 SRNS's management and independent assessment programs and an evaluation of SRNS's efforts to improve the regulatory compliance program following the Price-Anderson Amendments Act (PAAA) program review that was conducted by the Office of Enforcement in 2005.

In August 2008, DOE transitioned a significant portion of the site contractor responsibilities (including nuclear materials management, deactivation and decommissioning, solid waste, tritium operations, and soil and water remediation) from the Washington Savannah River Company (WSRC) to SRNS. WSRC has retained responsibility for liquid waste operations, information technology, and cyber security. At the time of this IPR, SRNS had adopted the majority of WSRC program documents and procedures for use in implementing its responsibilities, including implementation of the regulatory compliance programs. Therefore, although this IPR focused on SRNS activities, the results may have general applicability to WSRC's regulatory compliance program implementation.

II. General Implementation

In addition to noncompliance tracking and reporting, the SRNS Enforcement Coordinator has responsibility for Contractor Assurance System processes (including occurrence reporting and the corrective action management system). The SRNS Enforcement Coordinator reports through the head of the Health/Safety/Performance Assurance Division to the Vice-President for Environment, Safety, Health and Quality. As chair of the Regulatory Compliance Committee (RCC; see below), the SRNS Enforcement Coordinator has direct access to senior managers as needed. Discussion with senior management indicated that the SRNS Enforcement Coordinator frequently discusses safety and enforcement related issues with them.

Noncompliance screening functions are performed by three designated Regulatory Points of Contact (RPOCs). One RPOC works directly for the SRNS Enforcement Coordinator; the other two RPOCs work in other divisions but meet and communicate with him regularly. All of the RPOCs have held their positions for extended periods. Relevant to security, the SRNS Enforcement Coordinator and safeguards and security management hold regularly scheduled meetings to discuss concerns and noncompliances.

SRNS also maintains an RCC, which meets formally to review and make decisions related to NTS reportability of issues. The RCC consists of the SRNS Enforcement Coordinator (RCC chair) and the RPOCs. Additionally, the meetings typically include SRNS legal representatives and the radiological control organization or other organizations providing subject matter experts (SMEs) for particular regulations.

The SRNS nuclear safety (PAAA) and worker safety and health (WSH) noncompliance identification and reporting program is described in procedure CAP 11, *Identifying, Reporting, and Tracking Noncompliances Under the DOE Nuclear Safety and Worker Safety and Health Regulations*. The procedure uses the term “PAAA/WSH program” as a shorthand reference to the scope of the program. Procedure CAP 11 identifies the key program elements including roles and responsibilities, the PAAA/WSH noncompliance screening and reporting process, corrective actions, extent-of-condition determinations, and the qualifications requirements for key personnel.

The CAP 11 procedure does not address identification and reporting of classified information security noncompliances, but instead references a separate procedure (SRNS Security Manual 7Q, procedure 213). The SRNS Security Manual defines the requirements, roles, and responsibilities for implementing security policies and procedures (including the protection of classified information); however, this document is generally silent concerning requirements of 10 C.F.R. Part 824. The Foreword briefly acknowledges that violations relating to the safeguarding and security of Restricted Data or other classified information may result in enforcement action.

The SRNS Classified Matter Protection and Control (CMPC) Program and Cyber Security Program Managers are knowledgeable of their assigned responsibilities, and the programs were found to be proactive in providing support to the security incident and self-assessment programs, including timely sitewide notification of security lessons learned. The Cyber Security Program is consulted on all security incidents involving classified computing operations. This process is defined in a standard operating procedure and is designed to ensure that immediate actions are implemented to reduce the potential risk to sensitive and classified information.

CAP 11 requires the SRNS Enforcement Coordinator to regularly conduct assessments to evaluate implementation of the PAAA/WSH program. The most recent self-assessment of the PAAA/WSH noncompliance reporting program was completed in September 2008. That self-assessment was broad in scope and was conducted using the Energy Facility Contractors Group Peer Review Checklist. However, this IPR identified more screening deficiencies (see Section III, Identification and Screening) than the SRNS

self-assessment. For future self-assessments, SRNS should consider using larger sample sizes; SRNS reviewed only 38 PAAA/WSH screens during the September 2008 self-assessment. The Office of Enforcement also notes that SRNS should consider using external personnel (peer reviews) periodically when conducting such assessments.

CAP 11 identifies training requirements related to the PAAA/WSH regulatory enforcement programs. An overview module is included in General Employee Training. Additional how-to training is provided to individuals functioning as RPOCs. 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 program strengths were noted:

- The integration of the regulatory function into the contractor assurance system and other systems, including standards/requirements identification documents (S/RIDS), operating experience, occurrence reporting, and corrective action management, promotes efficiency and performance improvement.
- The RPOCs have extensive nuclear safety screening experience and have provided consistent screening performance over a number of years.
- The CAP 11 procedure includes a number of attachments providing extensive guidance on programmatic and repetitive issue determinations and a number of reporting examples and scenarios.
- An explicit NTS reporting threshold for issues involving retaliation is procedurally identified.
- The CMPC program is integrated with the security incident, training, cyber security, and self-assessment programs. In addition, the inventory of accountable classified removable electronic media (ACREM) has been significantly reduced, by approximately 63 percent.
- The cyber security program has implemented thin-client (“diskless”) technology and SecureNet.

The following weaknesses were noted:

- The Enforcement Coordinator does not have an appropriate level of security clearance to adequately support the review of issues for all SRNS facilities and activities.
- The provisions of 10 C.F.R. Part 824 are not included in relevant safeguards and security policies and procedures, or in training/briefings concerning the protection of classified information.

- The roles and responsibilities of the SRNS Enforcement Coordinator, as they relate to security enforcement, have yet to be formally defined and documented.

III. Identification and Screening

Screening of potential PAAA/WSH noncompliance issues is performed by the RPOCs utilizing the Local Contractor Tracking System, which provides for computer-based screening and documentation. The completed screening forms identify the screening results and areas of noncompliance. Primary inputs into the screening process include events, deficiencies, and issues from the Site Tracking, Analysis and Reporting (STAR) system, equipment noncompliance reports, and employee concerns. Other information sources related to worker safety and health include accident/injury site-specific reports, Occupational Safety and Health Administration 300 Logs, Computerized Accident/Incident Reporting System forms, subcontractor focused observations, and operating logs.

The Office of Enforcement's review of multiple completed nuclear safety screens identified that a broad variety of information sources had been screened for potential noncompliances. Individual screens were typically timely and appropriately documented and categorized as to PAAA applicability and noncompliance status. One screen (related to a DOE letter on corrective actions) was noted to be significantly late; additionally, the Office of Enforcement identified one issue (dealing with software quality assurance) that was incorrectly screened as not having PAAA implications. These were viewed, however, as isolated examples.

In a few cases, screening of WSH issues or events did not identify regulatory noncompliances that appeared to have occurred. For example, the screenings for two 2008 occurrence reports involving potential employee exposures to chemicals did not identify relevant 29 C.F.R. 1910.1200 or 1910.1450 noncompliances. This appears to be attributable, in part, to the RPOCs' lack of knowledge in the numerous subject areas covered by 10 C.F.R. Part 851, inconsistent use of and referral to SMEs, time constraints (based on the number of source documents they are required to screen on a daily basis), and the failure of various assessors to consistently identify potential noncompliance issues as part of their deficiency identification processes. Although the Office of Enforcement is concerned about the RPOCs lack of knowledge and expertise in the 10 C.F.R. Part 851 subject areas, most screenings were adequately performed and these two exceptions were viewed as isolated examples.

Relative to the screening of classified information security issues, SRNS's Incidents of Security Concern Program is defined in a formal procedure to ensure that incidents are appropriately and consistently managed. The Incidents of Security Concern Program Manager, in consultation with SMEs and the DOE Savannah River Operations Office (DOE-SR) Information Protection Program Manager, determine the appropriate categorization of security incidents.

SRNS requires inquiries for all security incidents regardless of categorization as an Impact Measurement Index (IMI)-1, -2, -3, or -4. Interviews with inquiry officials found them to be knowledgeable of the site's security mission and their responsibilities. A review of six security incident files, identified as IMI-4 during fiscal years 2007 and 2008, confirmed the appropriate categorization of incidents. The incident files appropriately documented mitigating factors that ruled out the need to categorize and report the incidents as IMI-1, -2, or -3. Additionally, SRNS requires a fact finding meeting for each significant security incident to determine or better understand why the incident occurred.

The following program strengths were noted:

- During the 2005 program review, the Office of Enforcement noted that noncompliance screening was limited to higher significance (category 1 and 2) STAR issues. Since that program review, Significance Category (SC) 3 and 4 issues have been included as inputs to the screening process.
- The Security Incident Program is effective and appears to benefit as a result of inquiries being conducted for all IMI categories.
- Including SMEs and DOE-SR employees in the initial categorization of security incidents has a positive impact on the accuracy of security incident categorization.

The following weaknesses were noted:

- Radiation protection and WSH managers who were interviewed were unaware of the number of regulatory (i.e., 10 C.F.R. Part 835 and 10 C.F.R. Part 851) noncompliances being identified in their respective functional areas. Rollup reports with WSH noncompliance summaries from the screening database that are sorted by facility and date have not been routinely provided to appropriate managers or topical area SMEs for review. The Office of Enforcement believes that it is important for managers and support staff to have such information and perspectives.
- The Safety/Housekeeping Inspections Checklists completed by SRNS subcontractors, which are used to self-identify worker safety and health regulatory noncompliance issues, are not being reviewed by an RPOC to ensure that the noncompliances are tracked, corrected, and evaluated for NTS reportability.
- A vulnerability of the nuclear safety and WSH screening process is that it relies on issues being captured and entered appropriately into the STAR system. No formal or routine review is performed, however, to assess whether the STAR system is adequately capturing all intended issues, including security (see Section V, Issue Management and Trending).

IV. Evaluation of NTS and Security Reportability

The initial review of PAAA/WSH issues for NTS reportability is performed by the RPOCs as part of their screening process. When a potential NTS-reportable noncompliance is identified, the RPOCs discuss their initial determination with the responsible line manager and then forward the issue to the RCC for a second level of review and approval. RCC meetings are scheduled as needed to review noncompliances and make the final decision as to whether an issue will be reported into the NTS. When a positive reportability determination is made, the RCC chair informs the responsible line manager.

During the 2005 program review, the Office of Enforcement identified a weakness related to the percentage of Savannah River NTS reports that were related to operational events (approximately 75 percent) rather than through more proactive means (such as assessments). More recent reports reflect improvement; in 2007, 50 percent of NTS reports were event-related. It was noted this improving trend may be reversing, however, as approximately 67 percent of NTS reports for 2008 to date were event-related.

The Office of Enforcement's review indicated that the majority of nuclear safety related NTS reporting decisions appeared appropriate for those noncompliances involving event reporting thresholds. One example of a failure to report a programmatic issue is discussed below.

SRNS has been entering security incident data into the SSIMS for the past several years. A review of SSIMS data identified three active inquiries and one notification dealing with the protection of classified matter that are pending completed inquiries. Over the past 24 months, SRNS has reported 24 security incidents dealing with the protection of classified matter. A review of this data, as well as a review of security incident files, found timely and accurate reporting. No specific security strengths or weaknesses were identified.

The following strength was noted:

- NTS reports are issued in a timely manner, well within Office of Enforcement guidelines. SRNS metrics indicate an average of eight days from the date of noncompliance determination to NTS reporting.

The following weaknesses were noted:

- Discussions with SRNS staff indicate the site has an ongoing issue with the performance and effectiveness of the self-assessment process. This issue was identified by a DOE Headquarters assessment in 2006, and although corrective actions were taken, follow-up assessments by DOE-SR and WSRC in 2007 indicated that the corrective actions had not resulted in consistent implementation. Review of the causal analysis conducted by WSRC in November 2007 identified related concerns in such areas as training; assessment focus, scope, and rigor; scheduling;

and management involvement. Collectively, these concerns reflect a potential programmatic noncompliance with the management assessment requirements contained in 10 C.F.R. § 830.122(i); however, no NTS report was issued upon initial identification of the issue or upon subsequent reviews and evaluations of corrective action effectiveness.

- Numerous assessments performed from 2006 through 2008 – including SRNS industrial hygiene program self-assessments, SRNS internal independent assessments, DOE-SR monthly reports, and an Office of Environmental Management review – noted repeated weaknesses associated with the exposure assessment methodology that affected multiple WSH programs (e.g., bloodborne pathogens, carcinogen control, laboratory hygiene, and beryllium). The Office of Enforcement’s review of these assessments indicates a potential programmatic or repetitive noncompliance issue. However, SRNS has not evaluated the results of these assessments to determine whether a programmatic or repetitive issue exists that warrants reporting into NTS.

V. Issue Management and Trending

Office of Enforcement personnel reviewed SRNS processes related to causal analysis, trending, and corrective action implementation. Emphasis was directed toward issues related to nuclear safety, WSH, and classified information security regulatory noncompliances.

The SRNS corporate level corrective action program is described in policy 5.35, Rev. 10, *Corrective Action Program*. The SRNS manages issues on the STAR database in a tailored manner, based on an initial significance categorization of the issue. The SCs of issues range from 1 to 4, with 1 representing the most significant. NTS reportable PAAA/WSH issues are generally assigned SC 1; this categorization requires a formal root cause determination for the issue, determination of the extent of condition, and a corrective action effectiveness review. Non-reportable PAAA/WSH issues are generally assigned SC 3 or SC 4 and require less rigorous evaluation unless they collectively indicate a programmatic or more significant issue. The STAR database is also used to manage the resolution of all issues resulting from security incidents, self-assessments, and surveys/inspections.¹

SRNS typically utilizes the Apollo method when conducting root cause determinations and conducts approximately 50 causal analyses per year. Approximately 20 staff (from both SRNS and WSRC) are currently qualified as causal analysts.

In addition, SRNS has established a problem analysis methodology which is documented in WSRC-SCD-9, *Problem Analysis Manual*. Analysis of issues is accomplished in a tailored manner to support the development of appropriate corrective actions. A significance categorization determination establishes the rigor of the problem analysis

¹ See SRNS Management Policy 5.35, *Corrective Action Program*, and Management Requirements and Procedures 4.23, *Site Tracking, Analysis, and Reporting (STAR)*.

process and determines whether a root cause analysis, apparent cause analysis, or no analysis is necessary.

Section VII of this report discusses ongoing contractor initiatives related to improvements in the corrective action process and the causal analyst training and qualification process.

The SRNS NTS report closure process includes independent verification of the completion of corrective actions and subsequent performance of an effectiveness review approximately 6 months after the corrective actions are completed. With respect to the timeliness of NTS corrective action closure, statistics maintained by SRNS indicate that only 2 of 151 NTS-related corrective actions closed over the past 2 years were late. This compares favorably with non-NTS related corrective actions; similar statistics maintained by SRNS show that for a random sample of 207 closed corrective actions, 46 actions were completed late.

Office of Enforcement staff reviewed closure documentation associated with selected NTS reports. Causal analyses were completed for reviewed reports, and closure evidence for corrective actions was maintained. One weakness related to the selection of corrective actions listed in NTS reports was identified and is discussed below.

Corrective actions resulting from security incidents, self-assessments, and surveys/inspections are required to be entered into the STAR/Security Assessment Management System (SAMS) system for tracking and monitoring purposes. Additionally, managers of facilities where the noncompliance occurred are consulted and involved with the implementation of corrective actions. However, during this review it was determined that corrective actions resulting from a security incident that occurred in 2007 were not reflected in the STAR/SAMS system. Based on this discovery, it was determined that no mechanism is in place to ensure that corrective actions resulting from security incidents are entered into the STAR/SAMS system.

All corrective actions associated with an incident or finding are assigned to an individual and tracked until corrective actions are closed and independently validated. The STAR/SAMS system has an alerting mechanism to notify responsible individuals of upcoming and past due corrective action milestones. In addition, the SRNS Security Director meets monthly with the security staff to discuss the status of corrective action plans.

The following strength was noted:

- Use of the STAR/SAMS system for tracking security-related issues ensures that appropriate oversight and resources are deployed to address identified program security weaknesses. In addition, all listed security noncompliance entries in the STAR/SAMS system identify the specific DOE directive or policy citations.

The following weaknesses were noted:

- Examples were noted in which NTS reports included only those corrective actions directed toward preventing recurrence of a specific issue or event. Although more generic corrective actions (such as those directed at preventing a similar event or preventing the event at another facility) were identified and implemented as part of the site causal analysis/corrective action process, they were deliberately not included as part of the corrective actions listed on the NTS report.

The Office of Enforcement recognizes that contractors may list only the more significant corrective actions on an NTS report in cases where a large number of corrective actions have been developed. However, the Office of Enforcement has historically emphasized the development of corrective actions to address the generic implications of an issue, and looks for such corrective actions in the review of submitted NTS reports. In light of this emphasis, and in recognition of the significant potential difference in closure timeliness between NTS-related and non-NTS related corrective actions discussed above, the SRNS practice of deliberately excluding generic corrective actions on the NTS report is viewed as a weakness.

- SRNS causal analyses do not routinely include a review for prior similar events or issues (precursor review). The Office of Enforcement has recommended such reviews to determine whether similar problems or issues have arisen and, if so, to evaluate why prior corrective actions were not effective in preventing recurrence.
- No mechanism has been established to ensure entry of data into STAR. For example, two assessments (ESH-EPG-2008-00069 Exposure Assessment Program and a 2006 Office of Independent Oversight Inspection of ES&H Programs at the Savannah River Site) were not linked and identified in STAR. Additionally, some corrective actions resulting from an incident of security concern were not entered into the STAR/SAMS system.

The Office of Enforcement review team also evaluated trending activities performed by SRNS. Utilizing the STAR database, SRNS follows the performance of a series of monthly “dashboard” indicators and also performs more in-depth analysis of a broader range of indicators on a quarterly basis. Trend analysis is used to identify recurrent issues, and such issues have been reported to NTS. The analysis also identifies and focuses attention on potentially developing or emerging trends through the use of “alerts” and a watch list.

This review identified that trending of security incidents is conducted, and the results are summarized in an annual report that is provided to the SRNS Security Director and the DOE-SR security organization. This report is also provided to all facility management and the SRNS Enforcement Coordinator.

The following trending-related strengths were noted:

- The STAR system trending module has robust capabilities for analyzing a variety of data inputs that can be used as metrics for monitoring PAAA/WSH regulatory contractor assurance program functions. STAR enhancements continue, as indicated by a recent modification for “other conditions – high relative risk” for WSH.
- The radiation protection organization has developed and is tracking a detailed set of indicators to monitor radiological control performance. This trending has led to the early recognition and subsequent development of corrective actions for emerging repetitive problems. Examples include a problem with glovebag seams, radiation work permit suspensions, and a Pu-238 contamination control issue.
- The trending of security incidents and the wide distribution of the annual report summarizing the trending results are effective in providing lessons learned.

VI. Assessment Program

As part of this IPR, the Office of Enforcement performed a limited review of the implementation of SRNS management and independent assessment programs. SRNS continues to utilize the Facility Evaluation Board (FEB) process, formerly implemented by WSRC, as the basis of its independent assessment process. In this approach, FEB teams consisting of senior site personnel with significant experience and expertise are used to conduct assessments of site facilities and functional areas. The assessment team members are selected for each scheduled assessment to ensure independence and the requisite experience for the assessment scope. The FEB assessments are formally planned and scheduled, and the schedule is formally approved by the SRNS President. The FEB documents findings, observations, and good practices. In addition, FEB reports discuss similar deficiencies that have been identified in prior assessments.

The FEB assessment process is also used to conduct the triennial assessments required by 10 C.F.R. § 835.102. Discussions with the FEB radiation protection specialist and review of selected FEB reports indicate assessments of this functional area were effective in identifying substantive issues and that all required areas were being evaluated.

Within the scope of this review, the FEB process was noted to be a well-structured and formal approach, with a technically diverse and experienced set of assessors. The FEB has historically provided senior management with a comprehensive independent examination of the standards of performance of its operating organizations. As the site contract transition progresses, the FEB continues to offer useful insight to SRNS management regarding operational performance.

Overall, the FEB process was noted as a strength; however, one weakness related to FEB effectiveness was identified. As part of their reviews, the FEB routinely evaluates

facility self-assessment performance and has often identified specific issues related to that area. The FEB was not instrumental, however, in identifying the site self-assessment issue discussed below and in the following section.

SRNS utilizes their self-assessment program (conducted in accordance with Manual 12Q, *Assessment Manual*, SA-1, Rev. 12, *Self-Assessment*) to meet Departmental management assessment requirements. The site conducts a large number of self-assessments; statistics provided by SRNS indicate that approximately 6000 self-assessments were conducted during the period August 2007 to August 2008.

As noted above, the site has an ongoing improvement initiative related to the self-assessment program. A 2006 assessment by the DOE Office of Independent Oversight identified an issue with the effectiveness of the program; assessments performed by WSRC and DOE-SR in 2007 questioned the effectiveness of undertaken corrective actions, and a subsequent causal analysis by WSRC identified additional actions. The IPR review team noted that although recognized as an issue, the self-assessment program was not listed on the current SRNS “watch list” of potential problem areas.

Office of Enforcement reviews of SRNS self-assessment results indicated a current weakness in the analysis of functional area self-assessment results. Specifically, the Office of Enforcement noted that although self-assessment activities are conducted, there is little in the way of formal review of the collective results or evaluation of the efficacy of the assessment process itself. Further discussions identified that a mechanism has been developed (as part of the annual functional appraisal conducted in accordance with PA-2, Rev. 0, *Functional Area Program Performance Analysis*) to provide such an overview; however, this is a new initiative and thus is not currently performed effectively. As an example, Office of Enforcement staff reviewed the most recent annual performance analysis of the radiation protection functional area program. Although the report included a section on assessments, it contained no analysis of such areas as the collective results of the numerous self-assessments performed, whether the approach or frequency should be modified, and whether the self-assessments identified significant issues.

The SRNS security assessment program is documented in SRNS Security Manual, 7Q, 208, *Safeguards and Security Assessments*, and SRNS Assessment Manual, 12Q, SA-1, *Self-Assessment*. SRNS conducts six facility-specific compliance- and performance-based security assessments annually. In addition, a security awareness management assessment and general site property protection area assessment are conducted annually. SRNS established a Findings Review Board in 2006 to ensure a consistent approach in identifying discrepancies and findings by assessment team members. The assessments are completed by knowledgeable SRNS security staff and SRNS security field team representatives.

A review of the last 6 assessments conducted over the past 18 months was performed. Although these assessments were found to be comprehensive, they identified a recurrent

issue but noted no findings or suggestions. As a result, this recurrent issue was not entered into the STAR/SAMS system. In turn, no corrective actions were taken to specifically identify why this issue continues to be a problem. Subsequently, this issue was identified during a DOE security survey, and a finding was issued. The self-assessment process should be used as a tool to self-identify all concerns and take appropriate measures to identify the root cause and implement corrective actions that will prevent recurrence.

The area/facility managers are responsible for resolution of findings for their specific facilities. Each finding is entered into the STAR/SAMS system with the associated risk value resulting from the SRNS formal deficiency analysis. Formal and independent validation is required before a finding is closed in the STAR/SAMS system.

The STAR/SAMS system has robust trending and lessons learned capabilities that are being used. The results are provided to the security awareness organization, and, as needed, sitewide security bulletins are issued. In addition, the SRNS Enforcement Coordinator has access to all safeguards and security findings contained in the STAR/SAMS system.

The following strengths were noted:

- Many of the self-assessment program elements are comprehensive and provide an effective compliance- and performance-based evaluation of the SRNS safeguards and security program.
- The entry of self-assessment findings in the STAR/SAMS system and the implementation of a formal/independent validation process for closure of security deficiencies were found to be effective.

The following weakness was noted:

- Although the SRNS security self-assessments are comprehensive, the process needs to ensure a self-critical approach in identifying issues as findings and entering them into the STAR/SAMS system for tracking and trending purposes.

VII. Ongoing Initiatives

The following items were identified as areas of weakness or areas for improvement during the course of this IPR. Subsequent discussion, however, identified that SRNS had previously identified or was aware of these areas of concern, and evidence was produced to show that ongoing initiatives were under way to improve performance. Consequently, specific weaknesses in this report were not identified for these items, and they are instead listed here:

- Corrective action program – DOE assessments have identified various concerns related to implementation of the site corrective action program. These

include closing actions prematurely, not conducting effectiveness reviews within timeframes, and not completing corrective actions on schedule. A causal analysis has been performed, and corrective actions are under way.

- Self-assessment program – A summary of deficiencies in this program is provided in section VI of this report.
- Causal analyst training and qualification – The site has an interim process in place for qualification of causal analysts but has expressed an intent (in WSRC-IM-99-00022, Rev. 3, *Causal Analysis*) to develop a more structured, formal qualification program. Review of the existing qualification process determined it to be adequate; however, the Office of Enforcement strongly endorses and encourages SRNS's stated intent to further enhance that program.
- Functional area appraisal process – This process has been re-instituted recently and provides an opportunity to evaluate the effectiveness of the various functional area self-assessment programs; however, implementation is limited in effectiveness (see section VI).

VIII. Conclusion

Strengths within the WSH program currently include a vigorous tracking and trending capability. Areas in need of improvement include accurately identifying noncompliances during the screening process, consistently screening subcontractor self-inspection data, and evaluating assessment information for repetitive or programmatic NTS reporting. Since the PAAA program has been expanded to include the WSH function, SRNS is successfully meeting the challenge of identifying and reporting worker safety-related noncompliances.

In the area of nuclear safety, the IPR team identified specific strengths in the areas of general program implementation, issue screening, trending, and independent assessments. Several areas of weakness were identified; additional areas of deficient performance were also identified but not highlighted as specific weaknesses due to SRNS's ongoing initiatives in these areas. Overall, SRNS processes for the identification and reporting of nuclear safety-related noncompliances were found to be mature and effective.

The security enforcement program is in the initial stages of integration with the SRNS Enforcement Program. Although the SRNS Enforcement Coordinator has access to self-assessment and trending results listed in the STAR/SAMS system and meetings are held with the SRNS Safeguards and Security Director to discuss the data, the roles and responsibilities of the Enforcement Coordinator have not been formally defined and documented. Notable strengths include the overall robust Security Incident Program, specifically the conduct of comprehensive inquiries by knowledgeable staff for all IMI categories (1, 2, 3, and 4), as well as the inclusion of SMEs and DOE-SR in the initial categorization of security incidents. The use of the STAR/SAMS system for tracking security-related issues has proven that appropriate oversight and resources are being deployed to address identified program security weaknesses and to ensure that

appropriate corrective actions are implemented and validated. However, SRNS should develop a formal process to ensure that corrective actions resulting from an incident of security concern are entered into the STAR/SAMS system as required. Failure to capture this information has the potential to impact the identification of adverse trends and the implementation of corrective actions.