Department of Energy
Washington, DC 20585

February 8, 2013

Mr. Dwayne Wilson
President and Chief Executive Officer
Savannah River Nuclear Solutions, LLC
Savannah River Site
Building 730-1B, Room 333
Aiken, South Carolina 29803

Dear Mr. Wilson:

The Office of Health, Safety and Security's Office of Security Enforcement conducted an onsite Regulatory Assistance Review of the classified information security program elements that support the Savannah River Nuclear Solutions, LLC (SRNS) regulatory compliance program during the period September 10-13, 2012. The review included an evaluation of SRNS processes for identifying, reporting and tracking classified information security noncompliances; SRNS internal tracking systems; and processes for correcting deficiencies to prevent recurrence. The Office of Security Enforcement also conducted a limited review of SRNS management and safeguards and security self-assessment programs.

Although SRNS is in the initial stages of integrating its classified information security program and 10 C.F.R. Part 824 into its existing regulatory compliance program, the Office of Security Enforcement is encouraged by the efforts SRNS management has taken toward establishing a fully integrated program. Collectively, these program elements will allow SRNS to effectively implement a functional classified information security regulatory compliance program that is in alignment with the guidance set forth in the Department of Energy's *Enforcement Process Overview.*

As described in the enclosed report, the regulatory assistance review identified a number of program strengths, as well as recommendations for your consideration to further improve the SRNS classified information security regulatory compliance program. Most notably, SRNS is encouraged to continue its efforts to integrate 10 C.F.R. Part 824 requirements into its regulatory compliance program and formally define and document the roles and responsibilities of the 824 coordinator. Program improvements, whether self-identified or through implementation of the recommendations noted in this report, may serve as a basis for mitigation for any future classified information security-related enforcement action against SRNS, as

described in the *General Statement of Enforcement Policy* (10 C.F.R. Part 824, appendix A).

No reply to this letter is required. If you have any questions regarding this review, please contact me at (301) 903-2178, or your staff may contact Ms. Carrianne Zimmerman, Acting Director, Office of Security Enforcement, at (301) 903-0107.

Sincerely,

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

Enclosure: Regulatory Assistance Review Report

cc: David Moody, SR
Douglas Dearolph, NNSA, SR
Zachary Smith, SR
Gregory Floyd, SRNS
Robert Martini, SRNS

OFFICE OF SECURITY ENFORCEMENT
REGULATORY ASSISTANCE REVIEW
SAVANNAH RIVER NUCLEAR SOLUTIONS, LLC

I. Introduction

During September 10-13, 2012, the Office of Security Enforcement, within the Office of Health, Safety and Security, conducted a regulatory assistance review of the classified information security program managed by Savannah River Nuclear Solutions, LLC (SRNS), located at the Savannah River Site (SRS) in Aiken, South Carolina. The review was conducted in a manner consistent with the guidance provided in the U.S. Department of Energy (DOE) *Enforcement Process Overview* (EPO), dated August 2012. The EPO document is located on the Office of Health, Safety and Security website at: http://www.hss.doe.gov/enforce/docs/overview/Enforcement_Process_Overview.pdf

This review included an evaluation of SRNS's processes for identifying classified information security noncompliances; reporting and tracking classified information security noncompliances in the Safeguards and Security Information Management System (SSIMS); using SRNS's internal deficiency tracking/trending systems; and correcting deficiencies to prevent recurrence. It also included a limited review of SRNS's management and safeguards and security internal assessment programs and an evaluation of SRNS's efforts to integrate its classified information security regulatory compliance program – as defined by 10 C.F.R. Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*, and Departmental security policies – with its existing Price-Anderson Amendments Act and worker safety and health compliance programs (hereinafter collectively referred to as the SRNS regulatory compliance program).

Although SRNS is in the initial stages of incorporating 10 C.F.R. Part 824 into its regulatory compliance program, it appears that SRNS has identified the key elements necessary to implement a regulatory compliance program that will enable the identification, reporting, evaluation, tracking, and correction of classified information security noncompliances to prevent recurrence. The review team identified a number of program strengths, as well as recommendations intended to improve the effectiveness of the SRNS regulatory compliance program for classified information security, that are discussed in detail in the appropriate sections of this report.

II. General Program Implementation

The DOE Office of Environmental Management (EM), through the DOE Savannah River Operations Office (DOE-SR), is the primary program office responsible for operations and oversight at SRS, including the Plutonium Storage Facility, H-Area, and the general site. The National Nuclear Security Administration (NNSA), through the Savannah River Site Office (SRSO), operates tritium facilities, as well as facilities and programs associated with nonproliferation efforts designed to dispose of surplus highly enriched

uranium and weapons grade plutonium. SRNS is the management and operating (M&O) contractor for both the EM and NNSA operations at SRS. This configuration places SRNS in the position of performing as a single M&O contractor accountable to two Federal program offices. As a result of this unique configuration, SRNS has established two distinct security organizations within the overall contractor organization, each reporting to a separate vice president.

The SRNS EM security organization is responsible for information security and self-assessments for the EM managed facilities, and provides security infrastructure for the entire site (e.g., badge office, alarm testing and maintenance, cyber security). The SRNS EM Security organization reports to the Vice President of the Environment, Safety, Security and Health Division (ESS&H). The SRNS NNSA security organization is responsible for information security and self-assessments within the NNSA managed facilities, and reports to the Vice President of NNSA Operations Programs. Each SRNS security organization has its own security manual and implementing procedures. SRNS EM policies and procedures are based on the current DOE directives. SRNS NNSA follows the same policies and implementing procedures generally as SRNS EM documents, with the exception of certain requirements and guidance from NNSA that are based on NNSA Policy Letters (NAP) for Information Security and Physical Protection. Both SRNS security organizations (collectively referred to as SRNS Security) take day-to-day direction on security program operations from their respective site offices (i.e., DOE-SR or SRSO).

The SRNS EM and SRNS NNSA security directors have been able to make this structure work based on decades of working together, mutual respect and confidence, and professionalism of their respective staffs. No formal mechanism has been established to define these divergent, redundant roles and responsibilities. Without defined roles and responsibilities, a change in management could have an adverse impact on the site's security program, including the protection and control of classified information.

The SRNS regulatory compliance program is well established, but the integration of 10 C.F.R. Part 824 requirements into the existing regulatory compliance program is in the initial stages. Discussions with SRNS management and staff members demonstrated that they are aware of the regulatory requirements associated with 10 C.F.R. Part 824; however, much of the existing program documentation does not address the requirements contained in 10 C.F.R. Part 824. This review did determine that several security and regulatory procedures are being updated to include these requirements.

In August 2012, SRNS established the position of 10 C.F.R. Part 824 coordinator (hereinafter referred to as the 824 coordinator) within the SRNS EM security organization to address 10 C.F.R. Part 824 concerns for both the EM and NNSA SRNS organizations. In addition, the 824 coordinator serves as the Classified Matter Protection and Control (CMPC) Manager and Information Security Manager for SRNS EM. The recently-appointed SRNS regulatory compliance program coordinator (hereinafter referred to as the SRNS enforcement coordinator) works within the Quality Services/Contractor Assurance Group and has extensive experience in nuclear safety and

worker safety and health, but has limited knowledge of classified information security requirements. The SRNS enforcement coordinator currently holds an L clearance (awaiting an upgrade to Q) and therefore does not currently receive all information related to security incidents and noncompliances. However, the alternate SRNS enforcement coordinator currently holds a Q clearance. The SRNS enforcement coordinator's lines of authority and associated roles and responsibilities related to 10 C.F.R. Part 824 have not yet been formally defined or documented.

Interviews with the quality services manager and the SRNS enforcement coordinator indicated that management supports the SRNS regulatory compliance program and that there are open lines of communication with representatives of the senior management team. The quality services manager and the SRNS enforcement coordinator participate in quarterly senior management meetings to evaluate information that might indicate programmatic, systemic, or management-related noncompliances in classified information security, and to discuss corrective actions resulting from significant safety and security events. Any identified issues are placed on a watch list to ensure that they are addressed with appropriate corrective actions and tracked to closure.

The 824 coordinator acts as a conduit between SRNS EM and NNSA security organizations and the SRNS regulatory compliance program. The 824 coordinator participates in the Corrective Action Review Board (CARB) that meets monthly, or more frequently when necessary, to ensure that SRNS follows appropriate processes to address all security noncompliances or issues regardless of source; perform causal analysis; and develop corrective action plans. The CARB is composed of the security director, CMPC manager, the security incident program manager (SIPM), physical protection manager, material control and accountability manager, and any other managers assigned to SRNS Security.

An office-level procedure outlining the roles and responsibilities of the 824 coordinator has been developed, but these roles and responsibilities are not documented in the SRNS regulatory compliance program procedure. Currently, SRNS has no formal screening process documenting the regulatory considerations or decisions concerning 10 C.F.R. Part 824 related noncompliances. The development of a regulatory screening process for incidents of security concern (IOSC) and other classified information security noncompliances would help ensure that identified issues and noncompliances are communicated to the SRNS enforcement coordinator to receive appropriate regulatory consideration.

To better facilitate a proactive and effective security regulatory compliance program, SRNS security's regulatory compliance activities, as well as the new 824 coordinator's roles and responsibilities, should be clearly defined and integrated into the sitewide Quality Services organization. In addition, the relationship between the 824 coordinator and the SRNS enforcement coordinator should be formally defined and documented. The 824 coordinator should ensure that all available information is provided to the SRNS enforcement coordinator (upon receiving clearance), relative to SRNS performance in the area of protection and control of classified information, such as security inquiry reports,

internal assessment reports, trending and data analysis, protective force daily incident reports, external audit reports, DOE-SR security survey reports, Independent Oversight inspection reports, and other government agency investigations (e.g., Office of the Inspector General and Government Accountability Office).

The SRNS EM security director and company facility security officer has served in his current role since April 2011 but had been acting security director since approximately September 2010. He has extensive security experience at SRS. His responsibilities encompass safeguards and security activities for the entire site, except for the facilities under NNSA authority. The SRNS EM security program includes several sitewide security programmatic functions (including Tritium and other NNSA facilities), such as CMPC, the IOSC program, classification, and security awareness.

The SRNS NNSA security manager has served in his current role since September 2010 and also has extensive security experience at SRS. His responsibilities encompass all security-related activities at the NNSA facilities, but due to limited staffing, he relies on SRNS EM for certain security services (e.g., CMPC, IOSC, classification).

Beginning in March 2011, SRNS experienced an increase in IOSCs, largely because of incidents at the NNSA Tritium facility, which houses most of SRNS's classified matter. The SRNS NNSA security manager indicated that SRNS senior management is very supportive of the overall security program and is actively engaged in addressing the recent increase in IOSCs. For example, in July 2011, the SRNS ESS&H Senior Vice President; the DOE Safeguards, Security, and Emergency Services director; the SRNS EM security director; and the SIPM provided a briefing to the Office of Security Enforcement on SRNS efforts to address the increase and prevent recurrence. In addition, SRNS Security implemented a number of corrective actions to address the spike in IOSCs, including in-service CMPC awareness training, group briefings, training videos, and lessons-learned publications. The frequency of reported IOSCs has since decreased.

In June 2012, SRNS Security invited representatives from the Energy Facility Contractors Group (EFCOG) Safeguards and Security Working Group to conduct a peer review of its implementation of 10 C.F.R. Part 824 requirements, in preparation for this regulatory assistance review. The EFCOG peer review team provided SRNS Security with feedback on the strengths of its classified information security program, as well as recommendations to improve performance. SRNS Security has successfully implemented several of the peer review's recommendations.

The SRNS security awareness program includes information on 10 C.F.R. Part 824 in its initial, comprehensive, and annual refresher briefings. A formal, sitewide lessons-learned process, which includes the NNSA facilities, has been established for security issues. This process includes security lessons-learned updates, which are communicated in a timely manner through various methods (e.g., employee briefings, meetings, e-mail, and newsletters) to site employees when an incident of security concern occurs.

The SRNS CMPC program for EM currently maintains two vaults, one vault-type room (VTR), and 228 General Services Administration (GSA)-approved security repositories for storing classified information. SRNS NNSA maintains two vaults, four VTRs, and 89 GSA-approved security repositories.

SRNS cyber security personnel respond as needed to IOSCs and sanitize systems as required, with assistance from Information Technology in the case of managed servers. The SIPM consults with cyber security personnel concerning IOSC categorization, as appropriate.

Strengths

- The lines of communication between the SRNS security organizations supporting EM and NNSA interests, such as the 824 coordinator, the SRNS enforcement coordinator, and DOE-SR/SRSO, appear to be effective.

- Senior management is engaged, and their commitment to the overall security program is exemplified, in part, by their interest in a recent increase in security incidents and their treatment of security with the same level of significance as safety.

- The SRNS personnel with key responsibilities for information security within the EM and NNSA areas of operation are well trained, and knowledgeable of their program responsibilities.

- The SRNS EM security awareness program (which provides services to SRNS NNSA) is well established and includes 10 C.F.R. Part 824 requirements in its initial, comprehensive, and annual security briefings.

Recommendations

- Formally document applicable requirements identified in 10 C.F.R. Part 824 in all of the SRNS local CMPC, Security Incident Program (SIP), and classified cyber security program training and procedures.

- Define and formally document the SRNS regulatory compliance program structure as it relates to the protection and control of classified information for both SRNS EM and NNSA, including: lines of authority and communication between the SIPM, the 824 coordinator, and the SRNS enforcement coordinator; integration of 10 C.F.R. Part 824 into the existing SRNS regulatory compliance and SRNS Security programs; and associated roles and responsibilities.

- Develop a formal regulatory screening process that considers all available information addressing SRNS performance related to the protection and control of classified information. To facilitate this process, the newly appointed SRNS enforcement coordinator should obtain a Q clearance and should receive regular

briefings from the 824 coordinator regarding SRNS EM and NNSA performance in protection and control of classified information.

III. Identification and Reporting of Incidents of Security Concern

SRNS Procedure 213/Rev. 7, *Incidents of Security Concern Management*, dated April 2, 2012, describes the requirements for reporting IOSCs, conducting inquiries, and performing corrective/disciplinary actions. Security incidents reported to the SIP that occur within the general site are categorized and resolved in accordance with DOE Order 470.4B, *Safeguards and Security Program, Attachment 5, Incidents of Security Concern*, dated July 21, 2011. Although the SRNS NNSA procedure mirrors the SRNS EM procedure for conducting IOSC inquiries, SRNS NNSA follows NNSA guidance, which requires them to utilize the Impact Measurement Index (IMI) tables from DOE Manual 470.4-1, Chg. 1, *Safeguards and Security Program Planning and Management*, dated March 7, 2006, to categorize and report security incidents that occur at NNSA facilities. As a result, the SIPM is required to categorize IOSC inquiries differently, depending on where the incident occurs (i.e., EM versus NNSA facilities).

The purpose of the SIP is to ensure that IOSCs are appropriately managed in a consistent, documented manner. According to the SIP procedures, all SRNS employees are responsible for immediately reporting any observations, findings, or information regarding a potential IOSC to SRNS Security. Any person who discovers classified matter, special nuclear material or nuclear material, controlled unclassified information, or other DOE security interest at risk must make reasonable steps to safeguard and secure those security interests appropriately until relieved by authorized personnel. The SRNS SIPM appears to use a conservative approach for initially categorizing security incidents involving classified information. The SRNS EM director and the SRNS NNSA security manager are then responsible for coordinating the notification to DOE-SR and SRSO, respectively.

During this regulatory assistance review, the SIPM appeared to be knowledgeable of program requirements and SRNS operations. Eighteen inquiry officials have successfully completed the inquiry training by the DOE National Training Center; 14 are assigned to SRNS EM, and 4 are assigned to SRNS NNSA. A new Inquiry Official training class is scheduled at SRS on September 24-27, 2012.

The review team examined five security incident files related to the 2011 increase in IOSCs and two that occurred more recently. The review team determined that the IMI categorizations were accurate, all required initial reporting and incident inquiry timelines were met, and the final inquiry reports were completed in a timely manner. The reports included the required information, but the information was not well organized, and the inquiry narratives were difficult to understand unless the reader was familiar with the site security configuration, policies, and procedures. Narratives that are written to follow the progression of the inquiry are more effective in communicating the circumstances surrounding the incident. The EFCOG peer review in June 2012 identified the same issue, and the inquiry reports produced since the peer review show some improvement.

Discussions indicated that when classified information is discovered on unapproved systems, whether EM or NNSA, cyber security personnel are consulted during incident categorization and are actively involved in minimizing any further damage by isolating and sanitizing all affected systems. If classified information is found to have been processed or stored on an unclassified information system, the cyber security staff takes the appropriate actions to contain and sanitize all affected systems and provide support to the inquiry official, as needed.

Strengths

- SRNS EM appears to use a conservative approach to ensure the accuracy of initial categorization of IOSCs, including consultation with DOE-SR.

- The SRNS SIPM manages inquiry officials located in both SRNS EM and NNSA areas, and all are available to respond to IOSCs. The SIPM is proactive in responding to security incidents, is knowledgeable of program requirements, and has years of investigative experience.

- SIP personnel conduct thorough security incident inquiries and produce timely inquiry reports.

- Cyber security and other subject matter experts are integrated into the SRNS SIP and are utilized appropriately.

Recommendation

- Continue improvements in inquiry report development so that readers who are unfamiliar with the site security configuration, policies, and procedures can understand and follow the progression of the inquiry and all circumstances surrounding the incident.

IV. Issues Management and Trending

SRNS uses the Site Tracking Analysis and Reporting (STAR) system as its designated internal issues management system. This system tracks all SRNS noncompliances and resulting corrective actions from internal and external reviews, assessments, security incidents, security surveys, and other evaluation activities. The SRNS corrective action program, including STAR, is managed and administered by the Quality Services organization. Noncompliances are entered and tracked through closure in accordance with SRNS Procedure 4.23/Rev. 7, *Corrective Action Program*, dated January 12, 2012, which implements a corrective action program designed to correct and prevent recurrence of issues affecting personal safety, operational safety, regulatory compliance, or business operations. The program is required to be used to manage all issues that are identified through incidents or events, as well as issues identified through internal and external review processes. The program is primarily aimed at preventing recurrence of

consequential events or issues and trending/tracking low-impact, low-consequence issues. The goal is to ensure that consequential events or issues are analyzed and that appropriate corrective actions are assigned, effectively implemented, and accurately closed in STAR.

All company personnel are responsible for identifying and documenting issues for evaluation. The individual who identifies the issue notifies the management responsible for the activity, and the issue is then entered into the STAR system. Issues are then assigned a significance category by a trained causal analyst assigned by the responsible manager:

- **Significance Category 1**: Issues in this category have a *significant impact* on safe/secure facility operations.

- **Significance Category 2**: Issues in this category have a *moderate impact* on safe/secure facility operations.

- **Significance Category 3a and 3**: Issues in this category have a *minor impact* on safe/secure facility operations.

- **Significance Category 4**: Issues in this category have a *minor impact* on safe/secure facility operations, *and are limited* to issues that are corrected on the spot or errors that do not warrant further corrective action.

- **Significance Category T**: Issues designated for *tracking* are necessary and/or appropriate to address and manage, but do not require a causal determination or full application of corrective action program elements.

Significance Category 1 and 2 issues require a root cause analysis by a trained causal analyst; an extent-of-condition review; a review of previous similar incidents or conditions; and a determination of whether the issue could reasonably have been identified through assessment activities. Category 3a issues require only an apparent cause analysis by a trained causal analyst, although a root cause analysis may be performed at the discretion of the responsible manager or the CARB. Category 3 issues may receive an apparent cause analysis by a trained causal analyst at the discretion of the responsible manager or the CARB.

SRNS EM uses the Apollo methodology for causal analysis, but other apparent cause methodologies are available. The SRNS SIPM conducts causal analyses for incidents that occur within the general site. SRNS NNSA uses Causal Analysis Mistake Proofing for causal analyses of incidents at NNSA facilities. Both methods produce a cause determination, and the causal analyst develops recommended corrective actions, which are sent to the responsible manager for review. The responsible manager approves the corrective actions and then assigns an employee to be responsible for completing the assigned action and documenting objective evidence of completion in STAR. All corrective action closures are required to be verified and undergo a corrective action

effectiveness review. The rigor of the verification and the effectiveness review is based on the assigned significance of the issue.

The responsible manager reviews the closure statements to ensure that they fully address all aspects of the corrective actions, and that the closure documentation has adequately addressed the corrective actions. The issue is then closed out in STAR.

Interviews revealed that all DOE survey findings and IOSCs receive a significance category of 3a or higher, based on the recommendation of the responsible manager or the CARB. SRNS has not fully developed specific criteria for applying the significance categories to IOSCs and information security-related noncompliances. Interviews with SRNS EM and NNSA security staff indicated that the criteria were originally established for safety events, and security was added at a later time. Since the inception of this ranking system, only one Significance Category 1 security event has occurred (a lock and key issue). Developing specific ranking criteria for information security-related noncompliances, including incidents and findings, for use in applying the sitewide corrective action program's significance categories would help ensure that the appropriate level of causal analysis and corrective action is provided.

While the STAR system allows managers to keep track of a range of issues and corrective actions, there is limited tracking and trending of information relative to classified information security that could aid in identifying and informing managers of precursor incidents that may indicate a repetitive, programmatic, or systemic problem. SRNS should continue implementing a trending and analysis process using all of the data maintained in STAR. This trending data should include the site's significance categorization determination and all information (regardless of organizational origin) pertaining to the protection and control of classified information, such as the SIP, internal assessments, security surveys, and external audits.

Strengths

- Security noncompliances identified as a result of external/internal assessments are maintained in the SRNS STAR, which is a centralized system designed to ensure the effective management of noncompliances.

- SRNS has a causal analysis guidance procedure in place and requires training for all personnel responsible for conducting causal analysis. Currently, SRNS Security (EM and NNSA) use different causal analysis processes, and both appear to be adequate.

Recommendations

- Improve the trending and analysis process by documenting the specific ranking used for information security-related noncompliances, including incidents and findings, for use in applying the sitewide corrective action program's significance categories to ensure that the appropriate level of causal analysis and corrective action is provided.

- Continue implementing a trending and analysis process using the data maintained in STAR. This trending data should include significance categorization and all information (regardless of organizational origin) pertaining to the protection and control of classified information, such as the SIP, internal assessments, security surveys, and external audits.

V. Assessments

The SRNS EM director and NNSA security manager are responsible for implementing the safeguards and security self-assessment program for their respective areas. Interviews with these managers indicated a strong desire to implement an effective assessment program, and both were well aware of the importance of this program in preventing a significant security event.

Safeguards and security assessments that are performed within the general site (EM) are conducted in accordance with DOE Manual 470.4-1, Chg. 1, *Safeguards and Security Program Planning and Management*, dated March 7, 2006. SRNS Procedure 208, *Safeguards and Security Assessments*, dated January 9, 2009, describes the process for conducting assessments within the general site. All assessors receive four hours of general training that addresses how to develop lines of inquiry (LOI) and how to document results in STAR. In addition, those conducting assessments for information security have attended the National Training Center's Survey/Self-Assessment training course.

The SRNS EM security self-assessment staff develops an annual site assessment plan and schedule that covers four site areas: 1) Program and General Site; 2) Savannah River National Laboratory; 3) 100K- and L-Areas; and 4) 200 H-Area. The assessments occur over an eight-month period, just prior to the DOE-SR survey for the identified area. After each assessment, a summary report is issued to the facility manager, the SRNS EM security director, applicable senior managers, and personnel responsible for corrective actions.

In contrast to the SRNS EM self-assessment methodology, SRNS NNSA security self-assessments are planned and developed annually utilizing a risk-based approach by the functional area managers and functional area program managers within the SRNS NNSA security organization. These managers evaluate their respective areas of responsibility and identify areas, items, services, or programs that contribute the greatest risk to quality, safety and mission, which are then assessed with the greatest degree of rigor and frequency. Findings are documented in a summary report within the STAR system and distributed to personnel identified as requiring review and approval. All assessments are rolled up into a year-end report in October. The assessments conducted by SRNS NNSA staff are shadowed by SRSO and take the place of an annual survey. The new risk-based self-assessment process was implemented at the beginning of fiscal year 2012.

For both the general site and the NNSA facilities, assessors develop LOI for each topical area and then enter the LOI and results into the STAR system. "Serious" findings are

assigned a significance category of either 1 or 2, and the responsible manager or the CARB has the option to elevate or modify the significance category. As noted above, there are no specific criteria for defining "serious" with respect to information security noncompliances.

The review team's interviews determined that information security assessments are conducted by experienced personnel with sufficient training to assess the assigned security topics. Noncompliances identified during the assessments are entered into STAR and tracked to closure. Interviews also determined that SRNS was unaware of the available process for reporting self-identified issues such as assessment findings, programmatic and repetitive concerns to the Office of Security Enforcement through SSIMS. The review team provided this information as an additional means of tracking issues and addressing potential precursors to more serious incidents.

The review team analyzed the *SRNS Safeguards and Security Self-Assessment Report for H-Area Nuclear Material Disposition Safeguards and Security*, dated June 13, 2011. The review validated that the SRNS EM security assessment methodology included procedure reviews, document validations, file reviews, performance tests, employee interviews, tests of employee knowledge, observation of work activities, equipment functional testing, and alarm and response testing. The assessment approach was found to include both compliance-based and performance testing activities. The information protection section of the report describes the performance objectives and lists the knowledge areas to be tested during employee interviews. This area received an overall rating of Satisfactory, and the assessors documented no findings. The CMPC section describes the performance objectives and indicates that the assessor conducted walkdowns of the building, evaluated procedures, conducted document reviews and performance tests, and interviewed employees based on the requirements of DOE Manual 470.4-4A, Chg. 1, and the SRNS Safeguards and Security Manual. Training records and over 600 documents were reviewed, and only 23 discrepancies (mostly minor marking errors) were noted. This area received an overall rating of Satisfactory, and the assessors documented no findings.

Although the review team found the assessment to be thorough, more emphasis could be placed on performance-based activities during the CMPC assessments; for example, employees could be asked to demonstrate important information security tasks required of their positions. Increasing the frequency and broadening the scope of meaningful performance-based activities designed to demonstrate program effectiveness could enhance the SRNS self-assessment program and could provide added value to management, as well as a basis for making programmatic decisions about the SRNS information security program.

Strengths

- SRNS management for both SRNS EM and NNSA recognize the overall importance of having a viable self-assessment program and the ability to self-identify noncompliant conditions.

- A formal process is in place to provide timely notification to the appropriate manager (SRNS EM or NNSA) and other designated personnel when noncompliances are identified during assessment activities.

- Personnel performing self-assessments for both SRNS EM and NNSA are trained and possess subject matter expertise in the areas they assess.

Recommendations

- Both SRNS security organizations should consider coordinating with DOE-SR and SRSO to begin entering self-assessment findings and programmatic issues into the self-reporting process available in SSIMS.

- Enhance both SRNS security-related self-assessment programs by including performance-based activities designed to demonstrate program effectiveness, and reducing the reliance on compliance-based reviews alone.

VI. Summary

This review indicated that SRNS is in the process of establishing a comprehensive security regulatory compliance program. Both the SRNS EM and SRNS NNSA security organizations have a wealth of site security and operational experience, and the personnel assigned to key positions displayed a high level of professionalism, technical competence, and dedication to accomplishing the mission of protecting national security interests. SRNS has a well established IOSC program that appears to provide accurate categorization of security incidents and the conduct of inquiries. The SIPM faces a particularly difficult challenge by following two different procedures when conducting inquiries in the EM and NNSA facilities.

Although SRNS has been actively working to integrate 10 C.F.R. Part 824 requirements into its regulatory compliance program, these requirements have not been fully defined or documented in the appropriate SRNS security training or procedures that specifically address classified information security topics. Additionally, the roles and responsibilities of the 824 coordinator, as they relate to the SRNS regulatory compliance program and SRNS enforcement coordinator, still need to be formally defined and documented.

A number of recommendations throughout this report provide opportunities to further improve the SRNS classified information security regulatory compliance program. SRNS senior management's continued attention and commitment to the overall security program are crucial to the successful integration of the classified information security programs with the SRNS regulatory compliance program.

By addressing the recommendations identified during this review, SRNS should expect to realize improved performance in the ability to avoid or reduce the severity of classified information security noncompliances; facilitate the Office of Security Enforcement's

exercise of discretion for noncompliant conditions that are considered to be less significant; support mitigation consideration in any future enforcement action; and ensure that classified information security shortcomings receive appropriate recognition and corrective actions. Any actions taken to address these recommendations should be appropriately coordinated with EM, DOE-SR, and NNSA/SRSO.

Acronyms

CARB	Corrective Action Review Board
C.F.R.	Code of Federal Regulations
CMPC	Classified Matter Protection and Control
DOE	U.S. Department of Energy
DOE-SR	Savannah River Operations Office
EFCOG	Energy Facility Contractors Group
EM	Office of Environmental Management
EPO	Enforcement Process Overview
ESS&H	Environment, Safety, Security and Health Division
GSA	General Services Administration
IMI	Impact Measurement Index
IOSC	Incident of Security Concern
LOI	Lines of Inquiry
M&O	Management and Operating
NAP	NNSA Policy Letter
NNSA	National Nuclear Security Administration
SIP	Security Incident Program
SIPM	Security Incident Program Manager
SRNS	Savannah River Nuclear Solutions, LLC
SRS	Savannah River Site
SRSO	Savannah River Site Office
SSIMS	Safeguards and Security Information Management System
STAR	Site Tracking Analysis and Reporting
VTR	Vault-Type Room