**Department of Energy**
Washington, DC 20585

August 20, 2019

Mr. Stuart MacVean
President and Chief Executive Officer
Savannah River Nuclear Solutions, LLC
203 Laurens Street, SW
Aiken, South Carolina 29801

SEL-2019-01

Dear Mr. MacVean:

The Office of Enterprise Assessments' Office of Enforcement has completed a review of the Savannah River Nuclear Solutions, LLC (SRNS) incidents of security concern (IOSC) program at the Savannah River Site (SRS). The Office of Enforcement conducted this review as a result of continued noncompliance with requirements for timely notification and closure of Category A IOSCs reported by SRNS. DOE Order 470.4B, Chg. 2, *Safeguards and Security Program*, requires the initial reporting of Category A IOSCs in the Safeguards and Security Issues Management System (SSIMS) within a maximum of 5 calendar days and closure in SSIMS within 90 calendar days of preliminary incident notification. The Office of Enforcement reviewed 21 Category A IOSCs reported by SRNS in fiscal years (FYs) 2016 through 2018, finding that 8 of the 21 IOSC notifications exceeded the 5-day notification period and 16 of the 21 IOSCs significantly exceeded the 90-day closure period (i.e., one to two years in most cases).

When SRNS simultaneously closed seven Category A IOSCs on July 13, 2018, the Office of Enforcement reviewed the IOSC final inquiry reports and identified numerous concerns in addition to the lack of timely notification and closure. For example, the inquiry reports did not thoroughly reconstruct the security incidents and sometimes omitted a chronological sequence of events before and after the incidents. In addition, the Office of Enforcement identified concerns about extent-of-condition reviews and issues management processes (causal analysis and corrective actions). In August 2018, the Office of Enforcement communicated these concerns to SRNS.

However, on November 28, 2018, SRNS closed three additional Category A IOSCs in SSIMS, and all three IOSC closures exceeded the 90-day required closure period; in fact, one IOSC closure was 762 days late. The Office of Enforcement conducted an in-depth review of all three inquiry reports and identified the same concerns communicated to SRNS in August 2018. As a result, the Office of Enforcement conducted a fact-finding visit at SRS from April 2 through 4, 2019, to gain a better understanding of SRNS's IOSC program implementation. During the fact-finding visit, the Office of Enforcement reviewed documents and interviewed Savannah River Operations Office (DOE-SR), Savannah River Field Office (SRFO), and SRNS personnel whose roles and responsibilities include the IOSC program, information security, and contractor assurance (i.e., issues management).

The Office of Enforcement reviewed 16 IOSC case files during the fact-finding visit and observed the same concerns identified in July and November 2018 (i.e., timely reporting, and completeness of inquiry reports and supporting documentation), but also noted that the recent inquiry reports are more thorough than previous ones. However, the case files were difficult to navigate to determine all pertinent facts and circumstances. Most of the files contained redundant or irrelevant documentation and often omitted the necessary supporting documentation (e.g., cyber sanitization records or documented evidence to support mitigating factors). DOE-SR, SRFO, and SRNS personnel shared their perspective on the effect of resource constraints on adequate conduct of inquiries and timely entry of IOSC data into SSIMS, and SRNS discussed its plans to hire three new security representatives who will be trained as inquiry officials within the next year. With increased resources, SRNS will have the opportunity to continue to improve the timeliness, completeness, and clarity of IOSC inquiry reports in the future by including: (1) a chronological sequence of all facts and circumstances (i.e., who, what, when, where, and why) associated with a security incident; (2) documented evidence for any actual or potential disclosures of classified information; and (3) an appropriate causal analysis, extent-of-condition review, and resulting corrective action plan to preclude recurrence.

With respect to corrective actions, the results of the Office of Enforcement's fact-finding visit were similar to those of a cross-functional team that SRNS established after self-identifying a negative trend in IOSCs during FY 2017 and the first quarter of FY 2018. Both the Office of Enforcement and the SRNS cross-functional team observed that the IOSC corrective actions included in closed inquiry reports appeared to be incomplete or did not address the potential causes of the security incident. More specifically, some of the corrective actions SRNS provided in the inquiry reports did not directly relate to identified causes and were presented as actions that SRNS planned to take (e.g., conduct risk ranking, conduct causal analysis, consider need for additional training, or develop a corrective action plan).

The Office of Enforcement found that the IOSC program is well integrated with other information security programs (i.e., classified matter protection and control, classification, and cyber security), as well as with the SRNS regulatory compliance program; however, the integration efforts are mostly driven by individuals and are not based on formal processes and procedures. In addition, the Office of Enforcement found the SRNS issues management processes and procedures to be heavily oriented toward safety and lacking the same level of rigor for security-related issues. The SRNS IOSC program could improve integration and implementation by formalizing processes and revising procedures so that they formally describe the involvement of key SRNS organizational elements (e.g., security management, classification, cyber security, issues management, or regulatory compliance) at all stages of the IOSC process, including: (1) identification, categorization, risk ranking, containment, and initial notification; (2) conduct of inquiries and development of final inquiry reports; and (3) issues management processes and results.

The Office of Enforcement recognizes that in response to the cross-functional team's review in May 2018, SRNS revised the SRS Safeguards and Security Review Board

Charter (effective July 12, 2018) to make the IOSC Events Review Board subcommittee responsible for reviewing IOSC events, extent-of-condition reviews, and issues management results. Additionally, the subcommittee will monitor SRNS IOSC data to identify trends and track all associated activities to ensure timely completion, as well as identify lessons learned. The SRNS IOSC Events Review Board subcommittee is encouraged to consider and support improvements in all of the above-mentioned areas of concern.

The Office of Enforcement has elected to issue this Enforcement Letter to convey these concerns and provide feedback on the measures that SRNS is implementing to address them. Issuance of this Enforcement Letter reflects DOE's decision to not pursue further enforcement activity against SRNS at this time. In coordination with the DOE Office of Environmental Management and the National Nuclear Security Administration, the Office of Enforcement will continue to monitor SRNS's efforts to improve security performance.

This letter imposes no requirements on SRNS, and no response is required. If you have any questions, please contact me at (301) 903-7707, or your staff may contact Ms. Carrianne Zimmerman, Director, Office of Security Enforcement, at (301) 903-8996.

Sincerely,

Kevin L. Dressman
Director
Office of Enforcement
Office of Enterprise Assessments

cc: Michael Budney, DOE-SR
Nicole Nelson-Jean, NA-SV
Tamara Baldwin, SRNS