Department of Energy
Washington, DC 20585

October 13, 2023

Dr. Richard Tighe
President and Chief Operating Officer
Consolidated Nuclear Security, LLC
Y-12 National Security Complex
P.O. Box 2009
765 Perimeter Road, K-1065D
Oak Ridge, Tennessee 37831

SEL-2023-01

Dear Dr. Tighe:

The Office of Enterprise Assessments' Office of Enforcement has completed an evaluation into five incidents of security concern (IOSCs) involving the compromise or potential compromise of classified combinations and the handling and protection of classified information, as reported into the Department of Energy's (DOE) Safeguards and Security Information Management System (SSIMS). Per DOE Order 471.6, *Information Security*, all classified information must be protected from unauthorized access. To meet the requirements of DOE Order 474.2, *Nuclear Control and Accountability,* two-factor authentication combinations are classified and must be separated. Classified matter must be stored under conditions designed to deter and detect unauthorized access, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person. Based on this evaluation, the Office of Enforcement identified concerns that warrant management attention by Consolidated Nuclear Security, LLC (CNS) at the DOE/National Nuclear Security Administration's (DOE/NNSA) Y-12 National Security Complex in Oak Ridge, Tennessee (Y-12).

In March 2023, CNS transmitted the inquiry files, causal analyses, and corrective actions documentation to the Office of Enforcement for two IOSCs involving the compromise of and failure to appropriately protect classified combinations used for two factor authentication. CNS discovered the subject IOSCs on May 11, 2022, and May 16, 2022, and closed the inquiries for the IOSCs in SSIMS on August 8, 2022, and January 1, 2023, respectively. The two IOSCs are summarized as follows:

- On May 9, 2022, while attempting to unlock an access door to complete nightly checks, an employee was shown a combination for which they were unauthorized, resulting in a compromise of classified information. The combination was part of a two-factor authentication consisting of "A" and "B" combinations. The employee who shared combination "B" with

the unauthorized person later reported to management that they had affixed the classified combination to the back of their badge, resulting in the failure to protect the combination. This employee stated they knew that storing a classified combination in this manner was noncompliant with DOE requirements. In response to this IOSC, CNS did the following: (1) stopped all work in the area of the security containers and changed the lock combinations; (2) conducted an inventory of the involved security containers and accounted for the classified contents; (3) briefed all employees on the requirements for handling classified combinations and required all employees to read and sign a one-page document titled *Lock and Key Requirements*; and (4) removed the responsible employee's access to classified information and eventually terminated the employee.

- On May 16, 2022, an employee found a classified combination written on the *Lock and Key Requirements* document that was issued in response to the May 11, 2022, incident (without classification markings). It was unsecured on a desk in a supervisor's office. Writing the combination and leaving it unsecured on a desk resulted in a failure to protect classified information. CNS again paused the mission and changed all associated combinations. The employee responsible for writing down the combination was not identified, so it is unknown whether this incident was deliberate or an act of gross negligence.

Based on these two events, the Office of Enforcement searched for similar CNS IOSCs involving the failure to protect classified combinations, and identified three additional incidents, and subsequently received and reviewed the case files. The three additional incidents are summarized as follows:

- In July 2021, an employee removed scrub pants from a clean laundry cart and discovered a piece of paper in a pocket. Two legible combinations were written on the paper, both of which were determined to be classified. CNS identified the employee who had written the combinations and determined the employee did not have a need to know for one of the combinations, which resulted in a compromise of classified information. This employee stated that the combinations were changed while they were on personal leave. Upon return to the workplace, the employee received the new combinations and wrote them down to aid in memorization, which resulted in a failure to protect classified information. The employee forgot the paper was in the scrub pants' pocket, and at the end of their shift, put the pants in the dirty laundry bin. The pants were laundered at an off-site, uncleared facility and were returned with the piece of paper containing legible combinations.

- In August 2022, an employee wrote a classified combination in a personal notebook after they returned to work and learned that the combination had been changed in their absence. The employee later lost control of the

notebook. Employees without a need to know the combination found and handled the notebook resulting in a compromise of classified information. The employee who lost the notebook did not report it missing, believing it was not a concern because it went missing inside a Material Access Area.

- In November 2022, an employee reported storing a copy of a classified combination in their wallet for approximately one year. The employee stated that storing a combination in a wallet was permitted.

The Office of Enforcement's review of these five incidents identified three principal areas of concern: (1) the protection and control of classified combinations to prevent unauthorized access; (2) the level of awareness of personnel regarding the storage of classified combinations in unapproved locations; and (3) the method of informing personnel of combination changes and providing adequate time for memorization of combinations prior to assuming job responsibilities. Given the nature of these incidents in which classified combinations were not protected and involved personnel who appeared unaware of security responsibilities, the information security culture within CNS requires management attention.

The Office of Enforcement acknowledges that CNS implemented corrective measures for the identified concerns. CNS has: (1) evaluated the site training (*Classified Matter Protection and Control, Repository Custodian, and Lock and Key Procedures*) to ensure that requirements for sharing, writing down, and protecting classified combinations are clear and understood by employees; (2) evaluated the frequency at which training is administered to validate it is conducted at appropriate intervals to ensure employees are aware of combination handling requirements; (3) encouraged organizations to evaluate the number of combinations that individuals are required to remember and to determine whether changes to how combinations are managed within CNS organizations are necessary; (4) conducted a CNS-wide (Y-12 and Pantex) awareness campaign encouraging employes to *Maintain a Security Mindset – Be Focused, Be Informed, Be Aware*; (5) required all employees in the affected areas to read and sign the *Combination Holder Responsibilities* briefing acknowledging site unclassified, factory set, and classified combination holder responsibilities; (6) adjusted the Lock, Key and Repository Program operating procedures for more stringent protection of classified combinations; and (7) identified a June 29, 2023, date in the corrective action plan to form a Black Belt Team to analyze the process of protecting classified information to ensure effective implementation and identify improvements. These corrective measures should reduce the likelihood of similar incidents in the future; however, senior management attention is essential to ensure that classified information is protected from unauthorized access, specifically the handling and storage of classified combinations.

The Office of Enforcement has elected to issue this Enforcement Letter to convey its concerns and provide feedback on the measures that CNS has implemented to address the concerns revealed by the five IOSCs. Issuance of this Enforcement Letter reflects DOE/NNSA's decision not to pursue further enforcement activity against CNS at this time. In coordination with the DOE/NNSA, the Office of Enforcement will continue to monitor CNS's efforts to improve security performance.

This letter imposes no requirements on CNS, and no response is required. If you have any questions, please contact me at (301) 903-4033, or your staff may contact Ms. Carrianne Zimmerman, Director, Office of Security Enforcement, at (301) 351-1186.

Sincerely,

Anthony C. Pierpoint
Director
Office of Enforcement
Office of Enterprise Assessments

cc: Teresa Robbins, NNSA/NPO
Katherine Brack, Consolidated Nuclear Security, LLC