Department of Energy
Washington, DC 20585

November 30, 2016

Mr. Morgan Smith
President and Chief Executive Officer
Consolidated Nuclear Security, LLC
Y-12 National Security Complex
P.O. Box 2009 MS8001
Oak Ridge, Tennessee 37831-8001

SEL-2016-02

Dear Mr. Smith:

The Office of Enterprise Assessments' Office of Enforcement completed an evaluation of four security incidents involving the presence of classified information in unclassified waste streams, as reported by Consolidated Nuclear Security, LLC (CNS) into the Department of Energy's (DOE) Safeguards and Security Information Management System. An Office of Enforcement review team visited the Pantex Plant in Amarillo, Texas, on August 2 through 4, 2016, to confirm DOE's understanding of the facts and circumstances surrounding these security incidents and to discuss CNS's incidents of security concern (IOSC) program, causal analysis methods, and corrective actions.

During the site visit, the review team conducted extensive facility walkdowns of the areas where the security incidents occurred. The review team examined various waste streams consistent with the type of waste processed out of each unique work area (e.g., sanitary, paper, low-level radiological). Each waste stream was examined from the initial source to the point of final disposition (e.g., shredding, loading on trash trucks destined for a landfill, or placed in bins for further examination and processing). The review team also interviewed the facility personnel directly involved with the security incidents or responsible for executing the associated processes. The following paragraphs discuss three principal areas of concern identified during the site visit.

The review team found that the procedures for disposing of the classified information involved in the security incidents are deficient in both clarity and completeness. One procedure described a specific method of disposal, while another procedure provided no guidance regarding disposal. Interviews with technicians responsible for working with and destroying this classified information revealed that when procedures lack specificity, they rely largely on "tribal knowledge," including creating their own "rules" for accomplishing work activities. The most recent security incident involved new employees who diligently reviewed the procedures to determine how to dispose of this classified information properly. The lack of clear, complete procedural guidance led them

to an incorrect decision for disposal and resulted in the security incident. The review team is concerned that incomplete and unclear procedural guidance could allow classified information to remain vulnerable to unauthorized disposition via inappropriate unclassified waste streams.

The second concern is that new employees may not remember their initial information security and classification training after the lengthy clearance processing time. CNS is executing a significant staffing campaign, hiring hundreds of new employees at Pantex. Given the delay in obtaining security clearances, the length of time between initial information security and classification training and actually performing duties involving classified matter may be up to 18 months. Training is not a significant issue for more-experienced personnel; many of those interviewed have over 20 years of experience performing their jobs and possess the "tribal knowledge" noted above. However, the gap between initial information security and classification training and performing classified work may allow less-experienced personnel who lack recent training to assume duties associated with the handling and protection of classified information.

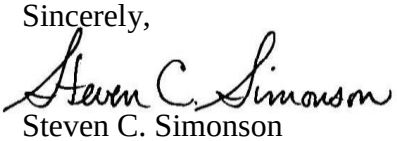
The last concern involves the IOSC program, specifically the categorization of incidents, the effectiveness of the causal analysis, and the corrective actions developed from that analysis. There have been four incidents involving classified information placed in an unclassified waste stream: one in 2012, two in 2014, and one in 2016. In one of the 2014 incidents, the categorization was lower than required, allowing this more-significant incident to be "bundled" with the other, less-significant waste stream incident discovered in 2014 (and with another security incident unrelated to classified information security). Lack of transparency and a self-critical attitude when categorizing security incidents may lead to less rigor in the inquiry, the causal analysis, and the corrective actions, as well as diminishing the ability to prevent recurrence. For example, the causal analyses performed in response to the two 2014 classified information security waste stream incidents were not explained in the security incident documentation and focused only on human performance issues. As revealed by the site review, the causes included both a lack of understanding of the classification of the information at issue and the comprehensiveness of the associated procedures.

CNS management attention is warranted to ensure the establishment of clear procedural processes for the disposition of classified information like that involved in these security incidents. Management attention is also warranted to ensure that the IOSC program categorizes incidents appropriately. These steps should allow for a more complete understanding of the facts and circumstances of incidents and should result in better causal analyses and more effective corrective actions. Management should also consider providing refresher training in classified information security and job-specific classification awareness if there is a significant time lapse between an employee's initial training and the actual performance of classified information security activities.

The Office of Enforcement has elected to issue this enforcement letter to convey the foregoing concerns. Issuance of this enforcement letter reflects DOE's decision to not pursue further enforcement activity against CNS at this time. In coordination with the National Nuclear Security Administration, the Office of Enforcement will continue to monitor CNS's efforts to improve security performance at Pantex.

This letter imposes no requirements on CNS, 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) 903-0107.

Sincerely,



Steven C. Simonson
Director
Office of Enforcement
Office of Enterprise Assessments

cc: Geoff Beausoleil, NA-NPO
Kathy Brack, CNS