Department of Energy

Washington, DC 20585

May 5, 2021

Ms. Michelle M. Reichert
President and Chief Executive Officer
Consolidated Nuclear Security, LLC
Pantex Plant
US Highway 60 and FM2373
Amarillo, TX 79120-0020

SEL-2021-01

Dear Mrs. Reichert:

The Office of Enterprise Assessments' Office of Enforcement completed an evaluation of a security incident discovered in March 2019 involving the unauthorized use of classified information systems and potential disclosure of classified information by Consolidated Nuclear Security, LLC (CNS) at the Pantex Plant (Pantex) in Amarillo, Texas. CNS completed its inquiry and closed the security incident in the Safeguards and Security Information System in August 2019. CNS provided the completed inquiry report including the causal analysis and corrective action plan for this security incident to the Office of Enforcement in December 2019. The Office of Enforcement subsequently held a virtual fact-finding with CNS from October 27 through 29, 2020, to understand the facts and circumstances surrounding this security incident.

In March 2019, a CNS employee found an unclassified U.S. government-issued laptop unattended in a government vehicle parked in a Pantex Property Protection Area parking lot. The CNS Pantex incident of security concern (IOSC) team determined that the unattended laptop belonged to CNS Pantex communication security (COMSEC) personnel who work in the CNS Pantex Communications Center (COMMCENTER). The initial CNS Pantex inspection of the unclassified laptop determined that there had been no compromise of sensitive information on the subject laptop; however, the CNS Pantex COMSEC Manager noticed that the subject laptop lacked the standard encryption software, and two subsequent inspections revealed the presence of unauthorized software (i.e., gaming software) and evidence that the laptop was used to watch non-work related digital video discs (DVDs). The CNS Pantex inspection of the unclassified laptop also revealed the past connection of unauthorized universal serial bus (USB) devices to the subject laptop. Based on these findings, CNS Pantex conducted three separate inspections of the COMMCENTER workspace and operations.

The inspections of the COMMCENTER by CNS Pantex revealed the following concerns: 1) a classified standalone computer (CSA) had been connected to multiple unauthorized portable USB hard drives and an unclassified printer; 2) classified information was stored on an unclassified networked computer; and 3) classified information was improperly transmitted outside of the Pantex firewall via a second unclassified networked computer.

Prior to the fact-finding, the Office of Enforcement confirmed with the DOE Central Office of Record (a function administered by AU-1.22) that there are no concerns relative to the protection

and control or operation of COMSEC equipment at Pantex. As a result, the Office of Enforcement's evaluation focused on classified information and cyber security operations performed within the CNS Pantex COMMCENTER unrelated to the COMSEC program operations.

The Office of Enforcement confirmed that three inspections conducted by CNS led to the discovery of the unauthorized use of a CSA computer, improper protection and control of classified information, and the potential disclosure of classified information. The Office of Enforcement interviewed facility personnel (i.e., IOSC program personnel, cyber security personnel/managers, and the COMMCENTER manager) directly involved with the security incident and identified three principal areas of concern: (1) protection of classified information and cyber security assets within the COMMCENTER, and COMMCENTER security incident reporting; (2) coordination among Pantex IOSC, cyber security, and COMMCENTER personnel on security inquiry activities and incident reporting; and (3) CNS oversight of security operations in the COMMCENTER.

First, the Office of Enforcement confirmed several instances of inadequate protection of classified information and cyber security assets. The Office of Enforcement determined that CNS did not approve the COMMCENTER CSA computer to process classified information in accordance with CNS CSA computer registration and approval processes. CNS also did not address potential extent-of-conditions for other CSAs in use at Pantex that may not have requisite approvals. The Office of Enforcement confirmed that the CSA computer within the COMMCENTER had been connected via USB cables to an unclassified network printer and 11 unauthorized USB storage devices.

In addition, the Office of Enforcement confirmed that two classified documents were stored on an unclassified networked computer and classified information was transmitted via an unclassified network computer located in the COMMCENTER on two separate occasions, neither of which had been reported to the CNS Pantex IOSC office. In both instances, the Office of Enforcement determined that the likelihood of compromise of classified information is remote.

Second, the Office of Enforcement concluded that the lack of coordination between CNS Pantex programs (i.e., IOSC, cyber security, and COMMCENTER personnel) prevented timely recognition and resolution of this security incident. Consequently, the process of understanding the security incident extended over a six-month inquiry involving three separate examinations of the unattended unclassified laptop and three separate inspections of COMMCENTER operations.

Lastly, CNS oversight of security operations within the COMMCENTER was lacking. While the responsible employees' failure to adhere to established policies and procedures was the primary cause of this incident, these employees were emboldened by working in an area with minimal oversight, and therefore, there was little chance of unauthorized actions being detected. In addition, CNS has not performed CMPC or CSA computer assessments within the COMMCENTER.

CNS Pantex has implemented significant measures to correct the concerns identified as a result of this incident to include: (1) updating the COMMCENTER CSA computer with the current CNS

CSA image; (2) conducting frequent unannounced visits by COMMCENTER management; (3) ensuring that the COMMCENTER CSA computer complies with established requirements (i.e., on a security plan and recorded in the property accountability system); (4) reviewing information system security officer roles and responsibilities for the COMMCENTER CSA computer; and (5) enhancing the approval, maintenance, and review of standalone classified computing equipment/systems procedures. In addition, the CNS Pantex causal analysis and corrective action plan included tasking CNS Pantex Cyber Security to: (1) collaborate with the CNS Pantex IOSC program to formalize roles and responsibilities for incidents involving information technology equipment; and (2) address cyber reporting requirements. These corrective measures, if effectively implemented and sustained, should reduce the likelihood of similar incidents in the future.

The Office of Enforcement has elected to issue this Enforcement Letter to convey the foregoing concerns and provide feedback on the measures that CNS Pantex has implemented to address the vulnerabilities revealed by this incident. While the actual national security consequences from this incident were minimal, under slightly different circumstances the security significance could have been much higher. In coordination with 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) 903-8996.

Sincerely,

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

cc: Teresa Robbins, NNSA/NPO
Kathy Brack, CNS