Department of Energy
Washington, DC 20585

May 21, 2018

Dr. Stephen Younger
Laboratories Director
National Technology and Engineering Solutions of Sandia, LLC
Sandia National Laboratories
P.O. Box 5800, MS-0101
Albuquerque, New Mexico 87185-0101

SEL-2018-01

Dear Dr. Younger:

The Office of Enterprise Assessments' Office of Enforcement completed a review of a security incident discovered in April 2017 involving the improper marking, sanitization, and storage of electronic test equipment used for classified processing at Sandia National Laboratories (SNL), Albuquerque, NM. Classified information was found in the memory of some electronic testing equipment, which was neither marked as classified nor controlled or protected from unauthorized access.

The Office of Enforcement recognizes that at the time of discovery of this security event, Sandia Corporation (Sandia) managed and operated SNL for the U.S. Department of Energy's (DOE) National Nuclear Security Administration (NNSA). However, the Sandia contract terminated shortly after the discovery of this event, on April 30, 2017. NNSA awarded the contract to National Technology and Engineering Solutions of Sandia, LLC (NTESS) on December 16, 2016. On May 1, 2017, NTESS began management and operation of SNL and thus became responsible for the response to this security event.

In June 2017, NTESS completed an incident closeout notification that identified this security incident as a category "B" incident (i.e., lower security significance). As defined in DOE Order 470.4B, Chg. 2, "*Safeguards and Security Program*," category "B" incidents are of lesser significance and are managed and resolved by the contractor cognizant security office; thus, category "B" incidents are not required to be reported in the DOE Safeguards and Security Information Management System (SSIMS). However, because of potential reporting culture concerns that NTESS identified during the Incident of Security Concern (IOSC) inquiry, NTESS voluntarily reported this security event to the Office of Enforcement in September 2017.

The Office of Enforcement's initial review of NTESS's incident inquiry report and supporting documents identified the following concerns: (1) the large amount of electronic test equipment used for classified processing involved in this security incident and the length of time this equipment was improperly marked,

sanitized, and stored; (2) line management involvement in the untimely reporting of this security concern; and (3) the categorization of this security incident as a category "B" IOSC and the limited scope of the inquiry. To confirm DOE's understanding of the facts and circumstances surrounding the security incident and to discuss NTESS's IOSC program, the Office of Enforcement conducted a fact-finding visit at SNL on December 11 through 13, 2017.

Due to allegations of potential reporting culture concerns within the division responsible for this security event, the NTESS Ethics Advisory & Investigation Services conducted an investigation in September 2017. Based on the results of this NTESS investigation, the Office of Enforcement fact-finding visit did not focus on the reporting culture concerns.

During the visit, the Office of Enforcement examined the various locations where electronic test equipment was used for classified work and staged prior to maintenance, as well as the maintenance locations. The Office of Enforcement also interviewed the facility personnel (e.g., technicians, maintenance personnel, and managers) directly involved with the security incident. The Office of Enforcement identified two principal areas of concern during the fact-finding visit: (1) work planning and control (i.e., life cycle management) of electronic test equipment used for classified processing, including use, marking, storage, and sanitization processes; and (2) the categorization of the security incident and the limited scope of the inquiry.

The procedures for identifying, marking, and sanitizing electronic test equipment used for classified processing involved in this security incident were deficient in both clarity and completeness. The sanitization procedure, informally created in 2011, addressed a sanitization process for only one specific type of testing equipment. The procedure did not define roles and responsibilities for sanitization and did not establish a process for documenting and tracking sanitization in accordance with NTESS corporate procedures. Additionally, electronic test equipment used for classified processing was improperly marked and stored due to incomplete and unclear procedural guidance. The Office of Enforcement determined that deficient procedures led to noncompliant classified information protection and control measures. In addition, the responsible NTESS division was found to operate independently and had less than adequate interaction with the NTESS security division; this condition contributed to inadequate work planning and control measures. Furthermore, the responsible NTESS division did not appropriately identify and mitigate the risks associated with using electronic testing equipment for both classified and unclassified work (i.e., dual use).

The responsible NTESS division has identified several actions that should adequately address the above concerns and prevent the likelihood of recurrence, including: (1) identifying all electronic testing equipment used for classified applications and determining the risk of classified information improperly remaining within the equipment's memory; (2) applying appropriate classification

markings to all electronic testing equipment used for classified activities; (3) storing all electronic test equipment used for classified processing in vault-type rooms and restricting movement of such equipment; and (4) engaging NTESS corporate cyber security in developing a security plan for electronic test equipment used for classified processing. Additionally, NTESS management apprised the Office of Enforcement of the following planned actions to address the concerns corporate-wide with electronic test equipment used for classified processing: (1) conducting a review of the functional alignment of the Computer Security Representatives and Security Coordinators to ensure that processes and capabilities are consistent throughout the organization; and (2) creating a Technical Hardware Evaluation Task Force to evaluate and determine the memory type of all electronic equipment used to perform classified work.

The second concern involved the categorization of this incident as a category "B" IOSC instead of a category "A" IOSC (i.e., higher security significance). The lack of a self-critical attitude when categorizing security incidents may reduce the rigor of the inquiry, the causal analysis, and the resulting corrective actions. Interviews revealed that NTESS's determination of security significance could have benefited from a more objective deliberation of all the related facts and circumstances.

The Office of Enforcement also concluded that the NTESS incident inquiry and causal analysis processes could be improved by: (1) using both the incident inquiry and the division critique teams to validate the facts and circumstances of an IOSC; and (2) ensuring that the responsible line organization includes an inquiry official as part of the causal analysis team. Causal analyses that are conducted by trained personnel and assisted by those who are most familiar with the incident are more likely to correctly identify the root cause(s) and implement effective corrective actions.

NTESS management attention is warranted to ensure that all corrective actions for the identification, marking, and sanitization of electronic testing equipment used for classified activities are completed and validated. In addition, NTESS management should ensure a self-critical view when determining the security significance of IOSCs. NTESS management's decision to report in SSIMS all IOSCs regardless of categorization should aid in this self-critical view. The Office of Enforcement is encouraged by NTESS's decision and transparency in reporting its IOSCs.

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 NTESS at this time. In coordination with NNSA, the Office of Enforcement will continue to monitor NTESS's efforts to improve security performance.

This letter imposes no requirements on NTESS, 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
Acting Director
Office of Enforcement
Office of Enterprise Assessments

cc: Jeffrey Harrell, NNSA/SFO
Gabriel King, NTESS