



Department of Energy

Washington, DC 20585

November 4, 2022

Dr. John C. Wagner
President and Laboratory Director
Battelle Energy Alliance, LLC
Idaho National Laboratory
2525 North Fremont Avenue
Idaho Falls, Idaho 83415-3695

SEL-2022-02

Dear Dr. Wagner:

The Office of Enterprise Assessments' Office of Enforcement has completed an evaluation into an incident of security concern (IOSC) involving the improper storage and protection of classified matter as reported into the Department of Energy's (DOE) Safeguards and Security Information Management System in November 2021. DOE Order 471.6, Chg. 3, *Information Security*, requires that classified information in all forms must be protected and stored in accordance with all applicable laws, regulations, policies, directives, and other requirements. Based on this evaluation, the Office of Enforcement identified concerns that warrant management attention by Battelle Energy Alliance, LLC (BEA) at the DOE Idaho National Laboratory in Idaho Falls, Idaho.

In June 2021, a BEA physical security officer (PSO) reported an IOSC involving a repository located in a Limited Area which contained classified matter in the form of computing equipment and media at the Confidential/Restricted Data (C/RD) level and category. The PSO reported that a BEA locksmith drilled the repository open after the locking mechanism failed, thereby invalidating its General Services Administration (GSA) certification. The repository and its classified contents were then improperly secured overnight by means of "security tamper tape," hourly administrative checks, and protective force checks. The next day, a new lock was installed, and the security tamper tape was removed; however, the classified matter remained in the uncertified and unapproved repository for seven days before it was transferred to an approved and secure location. BEA did not store the C/RD computing equipment and media in a properly secured repository in accordance with DOE and Idaho National Laboratory security requirements.

BEA inquired into the repository IOSC and determined that: (1) the repository's custodian was not present for approximately 24 minutes after a locksmith, who was appropriately cleared but did not have a need-to-know, drilled through the repository's locking mechanism, rendering it open; (2) after the locksmith drilled the repository open,

BEA staff used security tamper tape to seal the repository and applied both hourly administrative checks and four-hour protective force checks from late that afternoon until the following morning; and (3) BEA staff did not locate the classified combination for the drilled-open repository.

After learning of the incident, the Office of Enforcement asked BEA for additional information and documentation regarding the IOSC. The Office of Enforcement's evaluation identified two areas of concern: (1) storage and protection of classified matter; and (2) ineffective work planning and control processes; specifically, the coordination amongst BEA information system security officers/repository custodians, locksmiths, and the PSO responsible for this security activity. The Office of Enforcement confirmed that the classified combination packet for the subject repository could not be located.

The Office of Enforcement also confirmed previous instances of improper storage and protection of classified matter regarding this same repository. The Office of Enforcement determined that in July 2014 and September 2015 BEA used the same repository to improperly store classified matter in the form of computing equipment and media. In both instances, the repository did not have a functioning locking mechanism, and it was sealed with security tamper tape while awaiting repairs.

Lastly, the Office of Enforcement concluded that ineffective work planning/control practices and the lack of coordination between BEA staff (i.e., information system security officers, repository custodians, locksmiths, and the PSO) prevented BEA from fully understanding the scope of work, arranging for approved alternative classified storage locations in advance, and evaluating and controlling the vulnerabilities associated with repairing and/or replacing locking mechanisms on GSA-approved repositories. Consequently, a lack of effective communication and work planning/control practices was the primary cause of this IOSC.

The Office of Enforcement acknowledges that BEA has implemented corrective measures for the identified concerns. These include: (1) providing a pre-job briefing for custodians, locksmiths, and security personnel before beginning work on repositories; (2) requiring locksmiths to engage with PSOs before initiating the change of locks and/or combinations in order to facilitate the PSO's attendance at the activity; (3) directing PSOs to initial and verify that new repository combination packets received from custodians provide the proper information; (4) directing PSOs to create a written list of repository combination packets in their custody; and (5) sharing this IOSC with BEA staff to ensure an understanding of GSA certification requirements and that use of security tamper tape is not permitted to secure repositories. These corrective measures should reduce the likelihood of similar incidents in the future.

In addition, BEA conducted a management assessment, *LP-ASMT-2022-0206 - Safe and Vault Assessment*, dated June 15, 2022. The purpose and scope of BEA's assessment was to examine: (1) all repositories and vaults containing classified material to determine

whether prior drilling of these containers occurred; and (2) all repositories and vaults for any indication of security tamper tape having previously been applied. BEA did not identify any issues at the conclusion of its assessment.

The Office of Enforcement has elected to issue this Enforcement Letter to convey the foregoing concerns and provide feedback on the measures BEA has implemented to address the vulnerabilities revealed by this incident. While the likelihood of compromise of classified information is remote and 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 the DOE Office of Nuclear Energy, the Office of Enforcement will continue to monitor BEA's efforts to improve information security performance.

This letter imposes no requirements on BEA, and no response is required. If you have any questions, please contact me at (301) 903-9981, or your staff may contact Ms. Carrienne Zimmerman, Director, Office of Security Enforcement, at (301) 903-8996.

Sincerely,

A handwritten signature in black ink that reads "Robin M. Keeler". The signature is written in a cursive style with a large initial "R" and "K".

Robin M. Keeler
Deputy Director
Office of Enforcement
Office of Enterprise Assessments

cc: Robert Boston, DOE-ID
Dee Ann Brown, DOE-ID
Sherry Kontes, Battelle Energy Alliance, LLC