Department of Energy
Under Secretary for Nuclear Security
Administrator, National Nuclear Security Administration
Washington, DC 20585

December 16, 2022

Dr. James S. Peery
Laboratories Director
National Technology and Engineering Solutions of Sandia, LLC
Sandia National Laboratories
P.O. Box 5800, NS-0101
Albuquerque, New Mexico 87185

SEA-2022-01

Dear Dr. Peery:

This letter refers to the Department of Energy's (DOE) investigation into the facts and circumstances associated with an incident of security concern (ISOC) regarding the introduction of unauthorized electronic equipment into security areas at the DOE National Nuclear Security Administration (DOE/NNSA) Sandia National Laboratories in Albuquerque, New Mexico. The DOE Office of Enterprise Assessments' Office of Enforcement provided the results of the investigation to National Technology and Engineering Solutions of Sandia, LLC (NTESS) in an Investigation Report, *Unauthorized Electronic Equipment in Security Areas*, dated February 18, 2022. An enforcement conference was convened on April 12, 2022, with you and members of your staff to discuss the report's findings and NTESS's response. A summary of the enforcement conference and an attendance roster are enclosed.

Based on the evaluation of the evidence in this matter, including information presented at the enforcement conference, DOE/NNSA concludes that NTESS violated requirements enforceable under 10 C.F.R. Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*. Violations committed by NTESS include deficiencies in: (1) conducting thorough self-assessments, (2) conducting adequate and thorough IOSC inquiries, and (3) protecting and controlling classified information to prevent unauthorized disclosure.

Accordingly, DOE/NNSA hereby issues the enclosed Preliminary Notice of Violation (PNOV), which cites three Severity Level II violations with a total base civil penalty, before mitigation, of $410,000. This amount reflects the maximum applicable per-day base civil penalty authorized under 10 C.F.R. § 824.4(c) at the time of the security event.

Mitigating factors considered by DOE/NNSA are the timeliness and effectiveness of a contractor's causal analysis and corrective actions. As a result of the 2020 event, NTESS implemented timely and effective process changes regarding the introduction of controlled articles into security areas, updated the IOSC program procedures and implemented additional requirements for self-assessments and the introduction of controlled articles into security areas.

Consequently, the Office of Enforcement applied 50 percent mitigation for timely and effective corrective actions taken by NTESS. As a result, the total proposed civil penalty is $205,000.

Pursuant to 10 C.F.R. § 824.6, *Preliminary Notice of Violation*, paragraph (a)(4), you have the right to file a written reply within 30 calendar days of receipt of the enclosed PNOV. Your reply must contain a statement of all relevant facts pertaining to each alleged violation and must otherwise follow the requirements of 10 C.F.R. § 824.6(b). If you fail to exercise this option to submit a reply within the 30 calendar days, then in accordance with 10 C.F.R. § 824.6(c), you relinquish any right to appeal any matter in the PNOV, and the PNOV, including the proposed civil penalty assessment, will constitute a final order.

After reviewing your reply to the PNOV, including any proposed additional corrective actions, DOE/NNSA will determine whether any further activity is necessary to ensure compliance with DOE classified information security requirements. DOE/NNSA will continue to monitor the completion of corrective actions until this matter is fully resolved.

Sincerely,

Jill Hruby
Under Secretary for Nuclear Security
Administrator, NNSA

Enclosures: Preliminary Notice of Violation (SEA-2022-01)
Enforcement Conference Summary
Enforcement Conference Attendance Roster

cc: Dr. Daryl Hauck
Randy Castillo

Enclosure 1

Preliminary Notice of Violation

National Technology and Engineering Solutions of Sandia, LLC
Sandia National Laboratories

SEA-2022-01

A U.S. Department of Energy (DOE) investigation into the facts and circumstances associated with an incident of security concern (IOSC) revealed multiple violations of DOE classified information security requirements. The incident, which was discovered by National Technology and Engineering Solutions of Sandia, LLC (NTESS) in February 2020, involved the introduction of unauthorized electronic equipment (i.e., video cameras) into security areas, specifically in the Sandia National Laboratories Technical Library vault-type room (VTR) and the Limited Area outside the Technical Library (hereinafter referred to as the security event). NTESS is the management and operating contractor for the DOE National Nuclear Security Administration (DOE/NNSA) at the Sandia National Laboratories located in Albuquerque, New Mexico (SNL-NM).

Following the investigation, DOE issued an investigation report, *Unauthorized Electronic Equipment in Security Areas*, to NTESS on February 18, 2022. On April 12, 2022, DOE convened an enforcement conference with NTESS representatives at SNL-NM to discuss the findings and NTESS's response. A summary of the conference and list of attendees are enclosed.

Pursuant to section 234B of the Atomic Energy Act of 1954, as amended, and DOE regulations set forth at 10 C.F.R. Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*, DOE/NNSA hereby issues this Preliminary Notice of Violation (PNOV) to NTESS.

Violations committed by NTESS include deficiencies in: (1) conducting thorough self-assessments, (2) conducting adequate and thorough IOSC inquiries, and (3) protecting and controlling classified information to prevent unauthorized disclosure. DOE/NNSA has categorized the three violations as Severity Level II violations.

Severity levels are defined in Part 824, Appendix A, *General Statement of Enforcement Policy*, paragraph Vb. which states that "Severity Level II violations represent a significant lack of attention or carelessness toward the responsibilities of DOE contractors for the protection of classified information which could, if uncorrected, potentially lead to an adverse impact on the national security."

In consideration of factors discussed in Section II of this PNOV, DOE/NNSA imposes a total proposed civil penalty of $205,000 for three Severity Level II violations.

As required by 10 C.F.R. § 824.6 and consistent with Part 824, Appendix A, the violations are listed below.

I. VIOLATIONS

A. Conducting Thorough Self-Assessments

DOE Order 470.4B, Chg. 2, *Safeguards and Security Program*, Attachment 2, *Contractor Requirements Document Safeguards and Security Program Planning*, Section 2, *Survey, Review and Self-Assessment Programs*, paragraph 2, *Purpose*, states that "[s]urveys, self-assessments, and review programs are conducted to ensure that S&S [safeguards and security] systems and processes at facilities/sites are operating in compliance with Departmental and national-level policies, requirements, and standards for the protection of security assets and interests. These programs provide the means for timely identification and correction of deficiencies and noncompliant conditions to prevent adverse events and validate the effectiveness of corrective actions implemented to address identified deficiencies."

Paragraph 7 states that all contractors must "conduct formal self-assessments at intervals consistent with risk management principles and/or as directed by the DOE cognizant security office." In addition, subparagraph a. states that "[s]elf-assessments must have sufficient scope, depth, and frequency to ensure that at any point the facility is in compliance with all security requirements appropriate to the activities, information, and conditions at the location."

Contrary to the above requirements, and based on the following facts, the NTESS self-assessments did not evaluate the adequacy or effectiveness of activities related to the presence of unauthorized recording devices that could compromise classified information in security areas. The Office of Enforcement reviewed physical protection self-assessment reports and more than 40 integrated self-assessment reports from October 2016 to January 2020. Three of these reports – FY18SA-SS-RPT-004, *FY18 Physical Protection Self-Assessment Report*; FY19SA-SS-NM-RPT-005, *Safeguards and Security FY19 Sandia National Laboratories/New Mexico Safeguards and Security Physical Protection Self-Assessment Report*; and FY20SA-SS-RPT-005, *Safeguards and Security SNL/NM Physical Protection Self-Assessment Report* – contained high-level programmatic assessments of the NTESS Controlled Article Registration Process (CARP); however, the implementation of the process (i.e., the mechanics of submitting items to Physical Security for approval) was not reviewed. Also, these assessments did not evaluate the communication of the CARP to the workforce or the level of program compliance (e.g., there was no verification that the controlled articles identified in security areas were appropriately authorized). The last assessment conducted by NTESS of the VTR where the unauthorized cameras were discovered was in December 2018. In the December 2018 report, NTESS Physical Security personnel stated that no further self-assessments of the VTR would be performed because the "risk was low" and there were "frequent interactions with the VTR custodian."

In response to the security event, NTESS announced and conducted a targeted self-assessment of the VTRs (*Fiscal Year [FY] 2021 Sandia National Laboratories – New*

Mexico [SNL-NM] and Sandia National Laboratories – California [SNL-CA] Targeted VTR Assessment) on March 3 – 19, 2020. The objective of the targeted assessment was to verify that no unapproved controlled articles or prohibited items were in the 241 VTRs at SNL-NM and SNL-CA. The assessment included interviews with managers and custodians and "on-site physical inspection of VTR space for controlled articles." Due to the pandemic, NTESS assessed only 205 VTRs during the prescribed period. Although the assessment was announced and coordinated with NTESS at least two weeks in advance, NTESS still identified 66 unapproved controlled articles in 23 separate VTRs.

During interviews with NTESS issues management personnel, the Office of Enforcement learned that the "on-site physical inspection" for controlled articles consisted of a walkthrough that identified only the controlled articles that were in plain sight. The assessors did not inspect storage areas or cabinets. There were some positive aspects of the targeted VTR assessment – for example, self-assessments of the VTRs were performed by managers, custodians, residents, and Deployed Security Professionals (DSPs); additional training was provided on the policy for controlled and prohibited articles located in VTRs during the assessment; and Physical Security personnel validated the registration and approval of all controlled articles located in the VTRs. Advance notification of the assessment limited the effectiveness of the inspection, preventing NTESS from obtaining a more realistic assessment of the extent of the concerns (i.e., failure to prevent the introduction of controlled articles into secure areas). NTESS conducted interviews based on a checklist (standard question set) and provided it to the interviewees before the interviews, limiting the effectiveness of the assessment. Furthermore, the self-assessment did not include other security areas that contain classified information (e.g., sensitive compartmented information facilities and Limited Areas). Managers, custodians, residents, and DSPs are expected to be aware of controlled articles introduced into security areas and ensure articles are not introduced without approval.

This noncompliance constitutes a Severity Level II violation.
Base Civil Penalty – $82,000
Proposed Civil Penalty (as adjusted for 50 percent reduction for NTESS's corrective actions) – $41,000

B. Conducting Adequate and Thorough IOSC Inquiries

DOE Order 470.4B, Chg. 2, *Safeguards and Security Program*, Attachment 5, *Incidents of Security Concern*, Section 1, *Incident Identification and Reporting Requirements*, paragraph 4, *Conduct of Inquiries*, states that "[a]n inquiry must be conducted to establish the pertinent facts and circumstances surrounding the security incident." Paragraph 5, *Inquiry Officials*, subparagraph e. states "[i]nquiry officials are responsible for conducting the inquiry and maintaining all documentation associated with the inquiry" and e.(1) requires Inquiry Officials to "[c]ollect all information and physical evidence associated with the security incident."

Contrary to these requirements and as demonstrated by the following facts, the 2019 report of video cameras located within a security area did not prompt further investigation to establish the facts and circumstances or collect all information necessary to fully evaluate the security incident. In April 2019, Organization 8551 personnel reported concerns to the Security Incident Management Program (SIMP) about the presence of cameras inside a VTR and directed at Sandia Classified Network (SCN) terminals (2019 security incident). In an interview with the Office of Enforcement, IOSC program personnel who evaluated the 2019 security incident stated that the reported cameras were video-teleconferencing cameras. Based on that assumption and the fact that the SCN terminals were turned off when the cameras were discovered, IOSC program personnel determined that the incident was a "non-event." Thus, no further actions regarding the incident were taken, as the program receives similar calls frequently and, due to the incident caseload, no further inquiry was conducted.

The failure to obtain relevant information about the 2019 security incident that was reported to SIMP led to the incident being incorrectly categorized as a "non-event." Due to this "non-event" determination, NTESS management did not resolve this issue and the cameras remained in place for another 10 months until the concern was reported again to SIMP in February 2020, after which appropriate corrective actions were taken.

This noncompliance constitutes a Severity Level II violation.
Base Civil Penalty – $82,000
Proposed Civil Penalty (as adjusted for 50 percent reduction for NTESS's corrective actions) – $41,000

C. Protecting and Controlling Classified Information to Prevent Unauthorized Disclosure

DOE Order 473.3A, Chg. 1, *Protection Program Operations*, Attachment 3, *Physical Protection*, Section A, *General Requirements*, Chapter II, *Security Areas*, paragraph 8, *Prohibited and Controlled Articles*, clause b.(1) states that "[c]ontrolled articles, such as portable electronic devices, both Government and personally owned, capable of recording information or transmitting data (e.g., audio, video, radio frequency, infrared, and/or data link electronic equipment) are not permitted in LAs, PAs, or MAAs without prior approval."

DOE Order 471.6, Chg. 3, *Information Security*, section 4, *Requirements*, paragraph a.(5) states that "[a]ll classified information must be protected from unauthorized access." Paragraph a.(6) states that "[m]ethods to deter, detect, respond to, and mitigate unauthorized access to classified information must be implemented." Paragraph a.(7) states that "[a]ll classified information, including but not limited to that which is generated, received, transmitted, used, stored, reproduced, or permanently placed (buried according to the requirements of this Order) — until it is destroyed or otherwise no longer classified — must be protected and controlled commensurate with its classification level, category, and caveats (if applicable). All pertinent attributes must be used to determine the degree of protection and control required to prevent unauthorized

access to classified information." Subsection 4.a., *General*, states that "[a]ll individuals who are authorized for access to classified information must receive instruction with respect to their specific security duties as necessary to ensure that they are knowledgeable about their responsibilities and applicable requirements."

Contrary to these requirements and as demonstrated by the following facts, unapproved electronic equipment capable of recording and transmitting classified information was introduced into a VTR and used for more than 10 months. NTESS also used similar unapproved equipment for approximately two years in a Limited Area outside of the VTR.

NTESS developed the CARP in 2019 to provide a means of introducing controlled articles into security areas and to ensure that such articles are evaluated and approved for use. The Office of Enforcement determined that the NTESS CARP Physical Security approval and authorization process could accomplish this task; however, other conditions (i.e., lack of management support, incomplete self-assessments, other NTESS policies/procedures, and lack of training) limited the CARP's effectiveness and prevented the intended purpose from being accomplished.

Although NTESS management support of the CARP is imperative to the success of the process, the Office of Enforcement found that management support for the process was not consistent throughout NTESS. At the time of the security event, management of Organization 8511 was unaware of the existence of the CARP established in 2019 and the previous process established in 2010. During the SNL-NM and SNL-CA targeted VTR assessment in March 2020, 14% of the VTR owners and custodians interviewed by NTESS were unaware of the CARP. The NTESS targeted VTR assessment also indicated that many of the 213 registered controlled articles found in 53 separate VTRs had been registered in the CARP only after the security event was discovered; the exact number of recently registered controlled articles could not be determined because the NTESS self-assessment teams did not establish a method for capturing this information during the onsite physical inspections.

The lack of consistent support for and awareness of the CARP is also indicated by the number of controlled articles submitted for approval in the CARP database from January to March 2020. In January 2020 (before the security event), 62 items were submitted for approval. From February 3 (date of discovery of the security event) to March 19, 2020 (completion of the VTR assessment), 352 items were submitted for approval. VTRs were not the only places where the use of these items was requested, but many of the items submitted during this time were devices capable of recording voice and/or images. The management attention created by the security event, coupled with the announced targeted VTR assessment, resulted in a large spike in submissions of articles for approval. These results indicate that NTESS may have unknowingly allowed the use and/or storage of unapproved controlled articles in security areas, demonstrating a neglect of or inattention to the CARP among some managers and members of the workforce.

The Office of Enforcement also reviewed numerous plans, policies, and procedures, including training programs, dating from 2017 to 2021. The documents included NTESS site security plans, controlled-article policies, VTR manuals and policies, information technology policies, procurement and acquisition documents, and policies pertaining to electronic devices. This review found that SS007, *Controlled and Prohibited Articles Policy*, contained three sentences stating that controlled articles must be registered and personnel must contact NTESS Physical Security for assistance before using controlled articles in security areas. This policy did not address the CARP explicitly or include details such as which items require authorization, who to contact for authorization, or how to submit a request form for approval; however, SS007 contained hyperlinks to the Laboratory Policy System definition of a controlled article and to the CARP, to which all members of the workforce have unfettered access. IT004, *Manage Controlled Electronic Devices and Media Policy*, states that covered devices and features must be approved and registered using the CARP. Other NTESS policies/procedures that have direct relevance to the security event (such as SS004, *Vaults and Vault-Type Rooms Policy*, Safeguards and Security Man-028, *VTR Manager and Custodian Manual*, and all documents relating to procurement and acquisition) did not address controlled articles. NTESS had no formal procedures describing coordination between procurement processes or the acquisition of controlled articles by personnel working in security areas.

Regarding training, controlled articles were identified in the comprehensive security awareness briefing; however, there was no mention of the CARP. SEC180, *Vault and Vault Type Room (VTR) Training*, did not contain any reference to controlled articles or the CARP.

Unauthorized access to classified information is prevented by establishing protection and administrative programs, and through the actions of individuals with authorization to access such information. NTESS developed the CARP to provide a way to detect and deter the presence of unapproved devices that are capable of compromising classified information within security areas. NTESS Physical Security personnel established an approval and authorization process for the equipment and devices identified as controlled articles. This process is to be performed prior to the introduction and use of such devices in security areas where classified information is generated, received, transmitted, used, stored, reproduced, permanently placed, or destroyed. However, this process is only effective if managers and members of the workforce submit these devices for approval.

During the Office of Enforcement interviews, management and employees of Organization 8551 stated that they were unaware of the CARP and the associated requirements. Additionally, management had only visited the VTR once because of the distant location to the VTR. After the initial report to the SIMP in April 2019, Organization 8551 management directed the removal of the cameras from the VTR, but because the SIMP indicated that the presence of cameras in the VTR was a "non-event," Organization 8551 management did not ensure that the cameras were removed. Moreover, Organization 8551 personnel did not initially inform the VTR owner about the introduction of cameras into the VTR, and the VTR owner remained unaware of the incident until it was reported again in February 2020.

Classified information was vulnerable to potential compromise and placed at unacceptable risk due to management, procedural, and programmatic breakdowns associated with the NTESS CARP. Although no classified information was confirmed to have been compromised in this incident, the Office of Enforcement determined that NTESS did not effectively implement appropriate methods to deter or detect the introduction of unapproved controlled articles with audio and/or visual recording capability into security areas.

Collectively, these noncompliances constitute a Severity Level II violation.

Base Civil Penalty – $246,000 ($82,000 for one day for the underlying violation and two additional days for the extended duration of the violation)
Proposed Civil Penalty (as adjusted for 50 percent reduction for NTESS's corrective actions) – $123,000

II. DETERMINATION OF CIVIL PENALTIES

The significance of the processes and procedures involved in the security event and the long-standing nature of the noncompliant conditions (e.g., despite the discovery of 2019 security incident, the cameras remained in place for another 10 months until reported again in 2020) are the primary factors in DOE/NNSA's determination of appropriate civil penalties. DOE/NNSA proposes the assessment of civil penalties for the violations cited in Section I of this PNOV.

A. Severity Level of the Violations

DOE's investigation produced sufficient evidence that classified information was vulnerable to potential compromise and placed at unacceptable risk due to management, procedural, and programmatic breakdowns that resulted in the introduction of unapproved electronic equipment into security areas.

B. Mitigation of Civil Penalties

DOE/NNSA provides strong incentives, through the opportunity for mitigation, for contractors' timely self-identification and reporting of security non-compliances before a more significant event or consequence arises. NTESS should have identified that unauthorized electronic equipment was introduced into security areas in 2019. Before the security event, the CARP was not well publicized and the CARP process was not exercised effectively, preventing members of the workforce from successfully complying with the program. Consequently, DOE/NNSA finds that NTESS is not entitled to mitigation for self-identification and reporting.

Another mitigating factor considered by DOE/NNSA is the timeliness and effectiveness of a contractor's causal analysis and corrective actions. As a result of the security event, NTESS implemented process changes regarding the introduction of controlled articles into security areas and updated the IOSC program procedures.

After the security event, NTESS immediately escorted the responsible individual (RI) from the Limited Area, confiscated the RI's security badge, and placed the RI in an unclassified workspace. The manager at the time of the event implemented access restrictions on the RI and provided counseling on the incident. NTESS immediately removed the unapproved electronic equipment from the VTR (Technical Library) and terminated the RI's system administrator privileges. The VTR manager implemented a requirement that each user or resident of the Technical Library read, acknowledge, and sign a memorandum of record, *Technical Library Vault Security Agreement*. The memorandum of record serves as documentation requiring that personnel attend the annual security refresher briefing and that they understand the content of the briefing as well as SEC180, *Vault and Vault Type Room Training*. The *NM Technical Library Vault Operations Policy* was revised to include specific language and an addendum to address the requirements that outside organizations using the VTR must follow. This policy update was discussed with managers and directors of all the organizations that use the Technical Library. SEC180 was updated to include requirements for the CARP, and this training is now required every two years. An annual security refresher briefing was developed for all users and residents of the Technical Library, and managers have been made aware of the CARP and its requirements. Finally, a policy has been implemented that no equipment testing will be performed inside the Technical Library.

NTESS implemented the following corrective actions to promote thorough self-assessments:

1. Required annual, documented VTR manager walkthroughs that include top-level management.
2. Terminated all ad-hoc testing of equipment in the Technical Library and created a dedicated, compliant test lab.
3. Ensured completion of all corrective actions developed as a result of SNL-NM FY21SA-RPT-005, *FY21 Physical Protection Self-Assessment.*
4. Added management of controlled articles within VTRs and surrounding security space in Limited Areas as a 2021 Programmatic Essential Element and required an annual review during the Sandia self-assessment.
5. Included a targeted approach for the FY 2022 Physical Protection self-assessment to review and evaluate CARP implementation and to follow up on the effectiveness of corrective actions.
6. Implemented a reorganization of Safeguards and Security, including the creation of a new department, Safeguards and Security Assurance and Contract Security Management.

Regarding the IOSC program, NTESS updated the inquiry process to include a two-person review for all events and updated the initial question set for inquiries. NTESS also updated the SIMP database to include a "notes" field for VTR events. Additionally, NTESS now requires an annual validation requirement of CARP registration via the Controlled Article Categorization Process.

NTESS implemented the following improvements for controlled articles in security areas and for the Physical Security staff:

1. Required annual updates to VTR security plans, including a mandatory field for the VTR manager to certify that all controlled articles in VTRs have been registered and approved in CARP.
2. Updated the CARP software to require VTR manager approval for all controlled articles requested to be used in a VTR.
3. Incorporated controlled articles into the procurement process to ensure that all methods of material acquisition are covered by the controlled-article policy.
4. Updated annual VTR training to include a module specific to controlled articles.
5. Emphasized controlled articles during integrated assessments conducted by Physical Security.
6. Trained High Risk Embedded Security Professionals and DSPs to discuss policy related to controlled and prohibited articles during line organization staff meetings and Tier Boards.
7. Included information about the CARP in the annual security refresher briefing
8. Recommended that CARP approval paperwork be kept with the approved device at all times.
9. Hired a limited term employee to manage the CARP program in Physical Security (previously an additional duty).
10. Created a security awareness campaign concerning the CARP.

Following the enforcement conference, NTESS provided documentation to DOE that described a number of significant improvements that have been implemented in security incident management and self-assessment programs. This documentation included validation that no outstanding corrective actions remain open.

C. Civil Penalties Assessment

DOE/NNSA concludes that civil penalties are fully warranted in this case. While civil penalties levied under Part 824 should not be unduly confiscatory, they should nonetheless be commensurate with the gravity of the violations at issue. In this regard, DOE/NNSA considered the nature, number, and severity of the violations identified here, as well as the circumstances of the case.

Pursuant to 10 C.F.R. § 824.4(d), DOE/NNSA may propose a civil penalty for each continuing violation on a per-day basis. In consideration of the longstanding nature of the security event, DOE/NNSA elected to cite violation C (Protecting and Controlling Classified Information to Prevent Unauthorized Disclosure) for two additional days.

Based on these considerations, DOE/NNSA proposes the imposition of a total proposed civil penalty of $205,000 for three Severity Level II violations.

III. REPLY

Pursuant to 10 C.F.R. § 824.6(a)(4), NTESS may submit a written reply within 30 calendar days of receipt of this PNOV. NTESS may submit a request for a reasonable extension of time to file a reply to the Director, Office of Enforcement, in accordance with 10 C.F.R. § 824.6(d). The reply should be clearly marked as a "Reply to the Preliminary Notice of Violation."

If NTESS chooses not to contest the violations set forth in this PNOV, then the reply should clearly state that NTESS waives the right to contest any aspect of this PNOV, including the proposed civil penalties. In such case, the total proposed civil penalty of $205,000 must be remitted within 30 calendar days after receipt of this PNOV by check, draft, or money order payable to the Treasurer of the United States (Account 891099) and mailed to the address provided below. To remit the civil penalty by electronic funds transfer (EFT), please request your accounting department to contact the Office of Enforcement docketing clerk at (301) 903-4033 for EFT wiring instructions. This PNOV will constitute a final order upon filing of the reply.

If NTESS disagrees with any aspect of this PNOV, including the proposed civil penalty, then as applicable and in accordance with 10 C.F.R. § 824.6(b), the reply must: (1) state any facts, explanations, and arguments that support a denial of an alleged violation; (2) demonstrate any extenuating circumstances or other reason why the civil penalties should not be imposed or should be further mitigated; and (3) discuss the relevant authorities that support the position asserted, including rulings, regulations, interpretations, and previous decisions issued by DOE. In addition, 10 C.F.R. § 824.6(b) requires that the reply include copies of all relevant documents.

Please send the appropriate reply by overnight carrier to the following address:

Director, Office of Enforcement
Attention: Office of the Docketing Clerk, EA-10
U.S. Department of Energy
19901 Germantown Road
Germantown, MD 20874-1290

or by email to: enforcementdocketclerk@hq.doe.gov.

A copy of the reply should also be sent to my office and the Manager of the Sandia Field Office.

Pursuant to 10 C.F.R. § 824.6(c), if NTESS fails to submit a written reply within 30 calendar days of receipt of this PNOV, NTESS relinquishes any right to appeal any matter in this PNOV, and this PNOV, including the proposed civil penalties, will constitute a final order.

IV. CORRECTIVE ACTIONS

Corrective actions that have been or will be taken to avoid further violations should be delineated with target and completion dates in DOE's Safeguards and Security Information Management System.

Jill Hruby
Under Secretary for Nuclear Security
Administrator, NNSA

Washington D.C.
This 15 day of December 2022