Department of Energy
Washington, DC 20585

February 25, 2011

CERTIFIED MAIL
RETURN RECEIPT REQUESTED

Mr. John J. Grossenbacher
Director, Idaho National Laboratory
and President, Battelle Energy Alliance, LLC
P. O. Box 1625
Idaho Falls, Idaho 83415-3695

SEA-2011-01

Dear Mr. Grossenbacher:

The Office of Health, Safety and Security's Office of Enforcement has completed its investigation into the facts and circumstances associated with an incident of security concern regarding the introduction of classified information into unapproved information systems (security event) at the U.S. Department of Energy's (DOE) Idaho National Laboratory (INL). Based on the on-site investigation and evaluation of the evidence in this matter, and in consideration of information presented by you and other Battelle Energy Alliance, LLC (BEA) officials during the enforcement conference on July 8, 2010, DOE is issuing the enclosed Preliminary Notice of Violation (PNOV) to BEA in accordance with 10 C.F.R. § 824.6, *Preliminary Notice of Violation*. A summary of the enforcement conference is also enclosed.

DOE has determined that the introduction of classified information into unapproved information systems at INL resulted in multiple violations of DOE classified information security requirements. Violations committed by BEA include: (1) a lack of a requisite classification determination when developing project information addressing classified subject areas; (2) ineffective protection and control of classified information; (3) use of unapproved/unaccredited information systems to develop, store, and disseminate classified information; and (4) ineffective internal assessment processes to self-identify noncompliances related to the protection and control of classified information. BEA's security management deficiencies relating to control of classified information are detailed in the enclosed PNOV, which includes three Severity Level I violations, and one Severity Level II violation, and a total proposed civil penalty of $425,000. Pursuant to 10 C.F.R. § 824.4(d), DOE may assess a civil penalty for each day of a continuing violation. In consideration of mitigation efforts undertaken by BEA, DOE has elected to cite each violation for two separate days. Each violation 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.

Pursuant to 10 C.F.R. § 824.6(a)(4), BEA has the right to submit a written reply within 30 calendar days of receipt of the enclosed PNOV. A reply must contain a statement of all relevant facts pertaining to the violations alleged, and must otherwise follow the requirements of 10 C.F.R. § 824.6(b). Pursuant to 10 C.F.R. § 824.6(c), failure to submit a written reply within 30 calendar days constitutes relinquishment of any right to appeal any matter in the PNOV; and the PNOV, including the civil penalty assessment, will constitute a final order.

After reviewing your response to the PNOV, including any proposed additional corrective actions, a determination will be made on whether further action is necessary to ensure BEA's compliance with DOE's classified information security requirements.

Sincerely,

John S. Boulden III
Acting Director
Office of Enforcement
Office of Health, Safety and Security

Enclosures: Preliminary Notice of Violation, SEA-2011-01
Enforcement Conference Summary

cc: Richard Provencher, NE-ID
Thomas Middleton, Battelle Energy Alliance, LLC
Alan Wagner, Battelle Energy Alliance, LLC

Preliminary Notice of Violation

Battelle Energy Alliance, LLC
Idaho National Laboratory

SEA-2011-01

The Department of Energy's (DOE) Office of Enforcement conducted an investigation into the facts and circumstances surrounding an incident of security concern regarding classified information being introduced into unapproved information systems (security event) at the Idaho National Laboratory (INL), which is managed and operated for DOE by Battelle Energy Alliance, LLC (BEA).[1] Following the investigation, DOE issued an investigation report, *Classified Information Introduced into Unapproved Systems: Battelle Energy Alliance, LLC* (Investigation Report) to BEA on May 11, 2010.[2] On July 8, 2010, an enforcement conference, attended by DOE and BEA representatives, was held to discuss the findings of the Investigation Report.[3]

The purpose of the investigation was to evaluate the security event, and to identify potential violations that could be subject to an enforcement action.[4] The Investigation Report identified multiple security violations of DOE classified information security requirements that resulted in the security event. Violations committed by BEA include: (1) a lack of a requisite classification determination when developing project information addressing classified subject areas; (2) ineffective protection and control of classified information; (3) use of unapproved/unaccredited information systems to develop, store, and disseminate classified information; and (4) ineffective internal assessment processes to self-identify noncompliances related to the protection and control of classified information.

Pursuant to section 234B of the Atomic Energy Act of 1954, as amended, and DOE regulations at 10 C.F.R. § 824.6 (2010), DOE hereby issues this Preliminary Notice of Violation (PNOV) to BEA and proposes a total civil penalty for three Severity Level I violations, and one Severity Level II violation of DOE classified information security requirements contained in DOE Manual 205.1-5, and the DOE Manual 470.4 series.[5]

Severity Level I violations are defined in paragraph V.b of 10 C.F.R. Part 824, Appendix A, *General Statement of Enforcement Policy*, as "the most significant" and "reserved for

---

[1] DOE Contract No. DE-AC07-051D14517, originally awarded November 9, 2004 (BEA Contract).

[2] The Investigation Report sets forth the investigative findings that underlie the violations asserted in this Preliminary Notice of Violation (PNOV). The facts of the Investigation Report rely in substantive part on the BEA inquiry report dated May 18, 2009.

[3] A summary of the enforcement conference is enclosed with the transmittal letter to this PNOV (Enforcement Conference Summary). During the enforcement conference, Mr. John Grossenbacher, INL Laboratory Director and President of BEA, admitted to the facts stated in the Investigation Report. *See* Enforcement Conference Summary, at 1.

[4] Investigation Report, *supra* note 2, at 4.

[5] These manuals are applicable to BEA pursuant to BEA Contract Section J, Attachment G, List of applicable DOE directives (List B), Clause I.14, Laws, Regulations and DOE Directives (DEC 2002).

violations of classified information security requirements which involve actual or high potential for adverse impact on the national security." Severity Level II violations are defined in the same paragraph as "violations [that] represent a significant lack of attention or carelessness toward responsibilities of DOE contractors for the protection of classified information which could, if uncorrected, potentially lead to an adverse impact on national security." The violations are identified below.

Summary of Violations

In summary, DOE finds that BEA committed the following violations:

1. Requirement for Classification Determination. BEA failed to have project information in known classified subject areas reviewed for classification by a derivative classifier. (See Violations, section I.)

2. Requirement for Information Protection. BEA treated project information as unclassified, and failed to protect it at the highest potential classification level and category before having it reviewed for classification. (See Violations, section II.)

3. Requirement for Cyber Security Protection. BEA failed to use information systems that were certified and accredited to ensure that the appropriate security controls were in place before processing classified information. (See Violations, section III.)

4. Requirement for Self-Assessment. BEA's self-assessment processes failed to identify its noncompliance with classified information security and cyber security Departmental requirements. (See Violations, section IV.)

Violations

I. Violation of Requirement for Classification Determination

DOE Manual 470.4-4, *Information Security* (Chg. 1, June 29, 2007),[6] Attachment 1, Section A, Chapter II, ¶ 1.c. requires that "[t]he originator of any matter that may be classified, including all matter that is prepared in a classified subject area, must ensure the matter is reviewed for classification by a derivative classifier. . . . Should any question exist regarding the classification of any draft document or working paper, the originator is responsible for obtaining a classification review."

Contrary to the above requirements, prior to the security event, BEA failed to have project information in known classified subject areas reviewed for classification by a derivative classifier. Specific examples include the following:

---

[6] DOE M 470.4-4, *Information Security*, has been cancelled and replaced with DOE M 470.4-4A, *Information Security Manual* (Chg. 1, October 12, 2010). The security event occurred when DOE M 470.4-4 applied to the BEA Contract and, accordingly, the violations associated with this security event are based on the requirements of this manual.

1. Based on document reviews and interviews, the DOE security enforcement investigation team found that BEA recognized, prior to development of the subject information, the concern of potentially generating classified information, due to the classified nature of the topics.[7] In fact, the investigation found that the responsible BEA department manager and project manager placed more emphasis on meeting customer needs, than on addressing the potential classification issues and risks associated with the subject project.[8]

2. The responsible BEA department manager and project manager consulted with the BEA classification officer on two separate occasions before commencing work on the subject project.[9] On each occasion, the BEA classification officer warned that it would be difficult to create unclassified information that would be of any value in addressing the topics of the subject project. Furthermore, the BEA classification officer recommended that the BEA managers not proceed with this project.[10]

3. For approximately four months before the discovery of the security event, BEA personnel performing work on the subject project prepared information involving classified subject areas, and failed to have the information reviewed for classification by a derivative classifier.[11]

Collectively, these noncompliances constitute a Severity Level I violation.
Base Civil Penalty - $200,000[12]
Proposed Civil Penalty (as adjusted for mitigation) – $150,000

II. Violation of Requirement for Information Protection

DOE Manual 470.4-4, *Information Security* (Chg. 1, June 29, 2007), Attachment 1, Section A, ¶ 2.a. requires that "[c]lassified information and matter that is generated, received, transmitted, used, stored, reproduced, or destroyed must be protected and controlled." Chapter II, ¶ 1.b. requires that "[a]ccess to classified matter must be limited to persons who possess appropriate access authorization, any formal access approvals and who have a need-to-know for the performance of official duties; access is not obtained by position only. Controls must be established to protect, deter, and detect unauthorized access to classified matter." Chapter II, ¶ 1.c. requires in pertinent part that "[p]rior to classification review, matter which may be classified must be protected at the highest potential classification level and category."

---

[7] Investigation Report, *supra* note 2, at 4-5.
[8] *Id.* at 4, 12.
[9] *Id.* at 5.
[10] *Id.*
[11] *Id.*
[12] Recently, several provisions of 10 C.F.R. Part 824 were amended to reflect that effective January 13, 2010, the Base Civil Penalty for Severity Level I violations has been increased to $110,000. *See* 74 Fed. Reg. 66,033 (Dec. 14, 2009). This change will not be applied to the proposed base civil penalties for BEA because the security event occurred before the effective date of the change.

Contrary to the above requirements, prior to the security event, BEA treated classified project information as unclassified and failed to protect it at the highest potential classification level and category before having it reviewed for classification. Specific examples include the following:

1. Despite the classification issues and risks associated with the topics of the subject project, BEA management accepted the project and began work in an unclassified environment.[13] As a result, BEA treated classified information as unclassified, and failed to protect and control the information at the highest possible classification level and category.[14]

2. Throughout work on the subject project, classified information was distributed and destroyed by unapproved methods, and stored outside of approved security areas.[15] BEA also downloaded classified information to various types of removable electronic media that were not appropriately protected while in use and in storage. As a result, uncleared individuals, as well as cleared individuals without the appropriate need-to-know, gained unauthorized access to classified information.[16]

Collectively, these noncompliances constitute a Severity Level I violation.
Base Civil Penalty - $200,000
Proposed Civil Penalty (as adjusted for mitigation) – $100,000

III. Violation of Requirement for Cyber Security Protection

DOE Manual 205.1-5, *Cyber Security Process Requirements Manual* (August 12, 2008), Attachment I, states that "the contractor is responsible for implementing and complying with the requirements of . . . the applicable Senior DOE Management Program Cyber Security Plan (PCSP).

The PCSP applicable to BEA is the "Department of Energy, Office of the Under Secretary of Energy, Program Cyber Security Plan, dated May 9, 2007, Version 1.0." Version 1.0 of the PCSP was transmitted to BEA on June 18, 2007. Section 6.3 of the PCSP, Certification and Accreditation (C&A), requires that DOE "establish a C&A process to ensure that adequate security controls are provided for all Department information systems." This is to ensure that classified information is processed only on certified and accredited information systems.

Prior to the security event, BEA failed to use information systems that were certified and accredited to ensure that the appropriate security controls were in place before processing classified information. In addition, the security event represented a failure by BEA to use certified and accredited information systems. Specific examples include the following:

---

[13] Investigation Report, *supra* note 2, at 5.
[14] *Id.* at 5-6.
[15] *Id.*
[16] *Id.* at 6.

1. The failure of the BEA department manager and program manager to follow warnings and guidance provided by the BEA classification officer resulted in the processing of classified information on unclassified information systems.[17]

2. Classified information associated with the subject project was provided to other BEA employees on electronic media that was uploaded to additional unclassified information systems, including personal laptops.[18] By using uncertified and unaccredited information systems, classified information was not protected by the requisite security controls.

Collectively, these noncompliances constitute a Severity Level I violation.
Base Civil Penalty - $200,000
Proposed Civil Penalty (as adjusted for mitigation) – $100,000

IV. Violation of Requirement for Self-Assessments

DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management* (Chg. 1, March 7, 2006),[19] Attachment 2, Part 1, Section G, ¶ 2.a.(6) requires that "Contractors must conduct self-assessments between periodic surveys conducted by the cognizant security authority and include all applicable facility S&S [Safeguards and Security] program elements. The self-assessment must ensure the S&S objectives are met. . . ." Section G, ¶ 1.a. provides that an objective of self-assessments is to "[p]rovide assurance to the Secretary of Energy, Departmental elements, and other government agencies (OGAs) that [S&S] interests and activities are protected at the required levels."

Contrary to the above requirements, prior to the security event, BEA's self-assessment processes failed to identify the broad classified information security and cyber security noncompliances disclosed by the security event. Specific examples include the following:

1. A review of the BEA S&S directorate information security assessment reports and subsequent interviews found that assessments conducted before the security event were limited in both frequency and scope.[20] Because these assessments were not comprehensive, BEA failed to identify the multiple classified information security deficiencies disclosed by the security event.

2. The responsible BEA directorate's internal assessments also failed to identify and mitigate vulnerabilities, identify programmatic weaknesses, develop a complete process improvement program, or improve the overall S&S program performance

---

[17] Investigation Report, *supra* note 2, at 5-6.
[18] *Id.*
[19] DOE M 470.4-1 (Chg. 1, March 7, 2006) has been cancelled and replaced with DOE Manual 470.4-1 (Chg. 2, October 20, 2010). The security event occurred when DOE Manual 470.4-1 (Chg. 1, March 7, 2006) applied to the BEA Contract and, accordingly, the violations associated with this security event are based on the requirements of this manual.
[20] Investigation Report, *supra* note 2, at 6-7.

within the directorate.[21] The assessment program provided neither a basis for line management to make decisions regarding the effective implementation of S&S activities, nor adequate assurance that S&S interests were appropriately protected and controlled.

Collectively, these noncompliances constitute a Severity Level II violation.
Base Civil Penalty - $100,000
Proposed Civil Penalty (as adjusted for mitigation) – $75,000

V. Assessment of Civil Penalties

The significance or gravity of a security breach is a primary factor in DOE's determination of an appropriate civil penalty. DOE proposes the assessment of civil penalties for the violations identified above, in consideration of the gravity of numerous security breaches that were ongoing for many months, and that could have been avoided if BEA project managers had adequately defined the work scope, or used a formal project management process to identify and mitigate security risks associated with a project involving classified subject areas.[22]

A. Severity of the Violations

Both the DOE investigation and the BEA final inquiry report concluded that a compromise of classified information occurred, resulting in unauthorized access by uncleared individuals, as well as cleared individuals without the need-to-know and/or required access approval.[23] The BEA department manager and project manager failed to adhere to warnings and guidance provided by the BEA classification officer when developing project information in a classified subject area in an unclassified manner.[24] The BEA classification officer warned the managers on two separate occasions about the potential classification concerns in proceeding with the subject project.[25] In addition, the results of DOE's investigation support the conclusion that BEA personnel placed more emphasis on meeting customer demands than anticipating and planning for security risks and mitigations associated with performing classified work in a secure manner.[26]

The failure of BEA project managers to adhere to warnings and guidance provided by the BEA classification officer resulted in the development of classified information that was not reviewed for classification by a derivative classifier, nor was it protected and controlled as classified when generated, used, stored, disseminated, or destroyed.[27] In addition, the information was processed and stored on information systems not certified and accredited for classified information.[28]

---

[21] *Id.* at 7.
[22] *Id.* at 12.
[23] *Id.*at 4.
[24] *Id.* at 5, 12.
[25] *Id.*
[26] *Id.* at 4, 12
[27] *Id.* at 5-6.
[28] *Id.* at 6.

The Investigation Report also concluded that the BEA self-assessments of the protection and control of classified information "were limited in scope, and lacked the rigor and comprehensiveness necessary to identify noncompliant conditions associated with the protection and control of classified information."[29]

DOE holds its contractors' accountable for the acts of their employees who fail to observe classified information security requirements, and who fail to perform adequate self-assessments in accordance with Departmental requirements and applicable contractual requirements. The DOE investigation and BEA's final inquiry disclosed the security deficiencies described above. The security event resulted from, and reflected BEA's failure, over many months, to understand and manage the subject project to prevent the development of classified information, and the failure to adhere to Departmental policies governing the identification, protection, and control of classified information.

B. Mitigation of Penalties

DOE provides strong incentives, through opportunity for mitigation, for its contractors' timely self-identification and reporting of security noncompliances before a more significant event or consequence arises. BEA security program weaknesses, as well as the unauthorized actions of the BEA employees, were identifiable and, if properly addressed, could have averted the security event. Classified information was introduced into unauthorized information systems, and disclosed to unauthorized persons for over four months.[30] BEA only became aware of the problem and took action when the BEA classification officer was asked to review the project information.[31] Consequently, the Office of Enforcement finds that BEA is not entitled to mitigation for self-identification and reporting.

Another mitigating factor considered by the Office of Enforcement is the timeliness and effectiveness of contractor corrective actions. After the security event, BEA immediately instituted corrective measures and took actions to minimize additional risk to classified information associated with the security event.[32]

In addition to the immediate containment, BEA initiated a stand-down of all project activities within the responsible directorate in order to assess all projects regarding implementation of Departmental and company-level security requirements and project-specific risk mitigations.[33] During the stand-down, BEA prepared and issued criteria to assess each project for identification and mitigation of security risks in preparation to restart work.[34] Each project was evaluated to identify those projects with a potential for

---

[29] *Id.* at 7.
[30] *Id.* at 5-6.
[31] *Id.* at 3.
[32] *Id.* at 7-8.
[33] *Id.* at 7.
[34] *Id.* at 7-8.

information to easily migrate from an unclassified environment to a classified environment, and to ensure that appropriate practices and mitigating factors were in place to manage and protect against such information migration.[35] All specific project security plans were reviewed, and the plan requirements were briefed to project teams.[36] BEA also developed a comprehensive corrective action plan resulting from the security event's causal analysis report, the human performance improvement assessment of security incidents for the responsible directorate, and the management self-assessment implementation plan for classified information protection and control.[37] The corrective action plan contained 22 separate action items.[38]

Furthermore, BEA took specific corrective actions to address additional training, performance oversight, and accountability for individual employees. These actions included relieving the department manager and project manager responsible for the subject project from their duties.[39]

In August 2010, the DOE Idaho Operations Office (DOE-ID) security division performed a validation review of the 22 corrective actions.[40] DOE-ID validated the closure of 21 of the 22 corrective actions, with the remaining action requiring additional time to achieve closure.[41] During that review, DOE-ID found that BEA management demonstrated a renewed focus on compliance with Departmental classified information security requirement, and adopted stricter accountability standards for managers and employees who fail to adhere to these requirements. Further, DOE-ID determined that BEA management has implemented processes, procedures, and practices to address noncompliant conditions that resulted in the security event.[42]

C. Civil Penalties

The Office of Enforcement concludes that a substantial penalty is fully warranted in this case. While civil penalties assessed under 10 C.F.R. Part 824 should not be unduly confiscatory, they should nonetheless be commensurate with the gravity of the violations at issue. In this regard, DOE considered the nature, number and severity of the violations found here, as well as the circumstances of the case.

In light of these considerations, DOE proposes the imposition of a civil penalty of $700,000 for the three Severity Level I violations, and one Severity Level II violation, less 50 percent mitigation for corrective actions associated with the classified information protection and cyber security violations cited in the PNOV, and less 25 percent mitigation

---

[35] *Id.* at 8.
[36] *Id.*
[37] *Id.*
[38] Enforcement Conference Summary, *supra* note 3, at 2.
[39] Investigation Report, *supra* note 2, at 8. During the enforcement conference BEA officials described corrective actions taken in response to the security event. *See generally* Enforcement Conference Summary.
[40] Validation Review Report on Closure of the BEA Corrective Action Plan, dated August 2010, at 3.
[41] *Id.* at 5.
[42] *Id.* at 4.

for corrective actions relating to the classification and self-assessment violations cited in the PNOV. DOE-ID considered BEA's new processes and procedures for project planning and control of classified work to be a noteworthy practice; however, the implementation of these processes and procedures was found to be inconsistently applied.[43] In addition, BEA plans to increase the frequency of its internal assessments and implement risk-based assurance activities.

Pursuant to 10 C.F.R. § 824.4, DOE may propose a civil penalty for each continuing violation on a per-day basis. In consideration of the mitigating factors, DOE elected to cite each violation for two separate days, resulting in a total proposed civil penalty of $425,000.

Opportunity to Reply

Pursuant to the provisions of 10 C.F.R. § 824.6, BEA may submit a written reply to this PNOV within 30 calendar days of receipt of the PNOV. The reply should be clearly marked as, "Reply to the Preliminary Notice of Violation."

Please mail the reply by overnight carrier to the following address:

Director, Office of Enforcement
Attention: Office of the Docketing Clerk, HS-40
U.S. Department of Energy
19901 Germantown Road
Germantown, MD 20874-1290

A copy of the reply should also be sent to the Assistant Secretary for Nuclear Energy in Washington, D.C., the Manager of the DOE Idaho Operations Office, and to my office.

Pursuant to 10 C.F.R. § 824.6(b), the reply should include the following information for each alleged violation: (1) any facts, explanations, and arguments which support a denial of the violation; (2) information that demonstrates any extenuating circumstances or other reasons why the proposed remedy should not be imposed or should be reduced; (3) relevant authorities which support the position asserted, including rulings, regulations, interpretations, and previous decisions issued by DOE; and (4) copies of all relevant documents. Information provided should include corrective actions that have been or will be taken to avoid further violations, with target and completion dates added to DOE's Safeguards and Security Information Management System.

Pursuant to 10 C.F.R. § 824.6(c), if BEA fails to submit a written reply within 30 calendar days of receipt of the PNOV: (1) BEA will relinquish any right to appeal any matter in the PNOV, and (2) the PNOV, including any remedies therein, constitutes a final order.

---

[43] *Id.* at 22.

If BEA agrees to comply with the proposed remedy and waives any right to contest the PNOV, the total proposed civil penalty of $425,000 must be paid within 30 calendar days of 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 above. BEA 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).

John S. Boulden III
Acting Director
Office of Enforcement
Office of Health, Safety and Security

Washington, D.C.
this 25th day of February 2011