



**Department of Energy**  
Washington, DC 20585

November 15, 2011

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

Dear Mr. Grossenbacher:

The Office of Health, Safety and Security's Office of Security Enforcement conducted an onsite regulatory assistance review of the classified information security program elements that support the Battelle Energy Alliance, LLC (BEA) regulatory compliance program during August 8-11, 2011. The review included an evaluation of BEA's processes for identifying, reporting and tracking of classified information security noncompliances, and processes for correcting deficiencies to prevent recurrence. The Office of Security Enforcement also conducted a limited review of BEA's management and safeguards and security self-assessment programs.

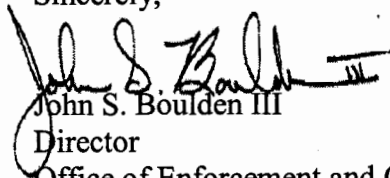
BEA is actively involved in integrating the provisions of 10 C.F.R. Part 824 with its existing regulatory compliance program and recognizes the need to re-evaluate the program structure to ensure that all classified information security programs and assets are fully considered. The Office of Security Enforcement is also encouraged by the improvement initiatives related to the implementation of BEA's security regulatory compliance program. The results of this review, described in the enclosed report, identified a number of strengths, as well as recommendations for your consideration that provide opportunities to further improve BEA's classified information security regulatory compliance program.

Program improvements, whether self-identified or through implementation of the recommendations noted in this report, may serve as a basis for mitigation for any future classified information security related enforcement action against BEA, as described in the enforcement policy statement that accompanies the U.S. Department of Energy's Classified Information Security Regulation (i.e., 10 C.F.R. Part 824, appendix A).



No reply to this letter is required. If you have any questions regarding this review, please contact me at (301) 903-2178, or your staff may contact Mr. Steven G. Crowe, Director, Office of Security Enforcement, at (301) 903-0107.

Sincerely,

Handwritten signature of John S. Boulden III in black ink.

John S. Boulden III

Director

Office of Enforcement and Oversight  
Office of Health, Safety and Security

Enclosure: Regulatory Assistance Review Report

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

**OFFICE OF SECURITY ENFORCEMENT  
REGULATORY ASSISTANCE REVIEW  
BATTELLE ENERGY ALLIANCE, LLC**

**I. Introduction**

During August 8-11, 2011, the Office of Security Enforcement, within the Office of Health, Safety and Security, conducted a regulatory assistance review of the classified information security program managed by Battelle Energy Alliance, LLC (BEA) at the Idaho National Laboratory (INL). The review was conducted in a manner consistent with the guidance provided in the U.S. Department of Energy (DOE) *Enforcement Process Overview* (EPO), dated June 2009. The EPO document is located on the Office of Health, Safety and Security website at:

[http://www.hss.doe.gov/enforce/docs/Final\\_EPO\\_June\\_2009\\_v4.pdf](http://www.hss.doe.gov/enforce/docs/Final_EPO_June_2009_v4.pdf)

This review included an evaluation of BEA's processes for identifying classified information security noncompliances; reporting and tracking classified information security noncompliances in the Safeguards and Security Information Management System (SSIMS); using BEA's internal deficiency tracking/trending systems; and correcting deficiencies to prevent recurrence. It also included a limited review of BEA's management and safeguards and security (S&S) internal assessment programs and an evaluation of BEA's efforts to integrate its classified information security regulatory compliance program – as defined by 10 C.F.R. Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*, and Departmental security policies – with its existing Price-Anderson Amendments Act and worker safety and health compliance programs (hereinafter collectively referred to as the regulatory compliance program).

This report identifies strengths, as well as recommendations intended to improve the effectiveness of the BEA regulatory compliance program for classified information security. Strengths and recommendations are listed below and are discussed in further detail in the appropriate sections of this report.

**Strengths**

- Management attention and commitment to the overall security program are evident, as exemplified, in part, by the support provided to the integration of the classified information security program with the existing regulatory compliance program, as well as the proactive approach in communicating security incidents that involve the

protection and control of classified information to senior level management. In addition, BEA has also been active in reducing its classified holdings.

- Effective partnerships and lines of communication among BEA's security organization (Laboratory Protection), the BEA enforcement coordinator, and the Department of Energy-Idaho Operations Office (DOE-ID) are apparent.
- BEA personnel with responsibilities for regulatory compliance and classified information security appear to be well trained and knowledgeable of program responsibilities.
- BEA incidents of security concern (IOSC) program personnel are knowledgeable of program requirements and have years of investigative experience.
- BEA uses a multi-disciplinary team approach to ensure the accuracy of initial categorization of security incidents that includes subject matter experts (SME), the division director for Security Programs and Services, and DOE-ID, as appropriate.
- BEA IOSC inquiry officials conduct thorough security incident inquiries.
- BEA requires training for all personnel responsible for conducting causal analysis.
- Personnel performing self-assessments are trained and have subject matter expertise in the areas they are assessing.
- Improvement in the overall structure of the BEA classified matter protection and control (CMPC) self-assessment program is evident, as exemplified, in part, by expanding assessment activities to include all BEA directorates that handle and store classified information.

### **Recommendations**

- Formally document applicable requirements identified in 10 C.F.R. Part 824 in all of BEA's local CMPC, IOSC, and classified cyber security program procedures, as well as local training that addresses classified information security topics.
- Clearly define and formally document the regulatory compliance program structure for all classified information security programs, (i.e., CMPC, IOSC, classified cyber security, special access programs (SAP), and intelligence programs) including lines of authority and associated roles and responsibilities.
- Document sufficient details in inquiry reports so that third-party readers can easily understand the circumstances surrounding the incident and the evidence that supports the incident categorization.

- Continue ongoing efforts to implement the integrated corrective action management system (ICAMS) to provide BEA with a centralized database for the effective management of all identified S&S noncompliances.
- Provide the enforcement coordinator with all available information (e.g., internal assessment reports, including classified cyber security; trending and analysis data; protective force incident reports; and external audit reports, such as those resulting from DOE-ID security surveys; external oversight inspections; and investigations by other government agencies, such as the Office of the Inspector General (IG) and the Government Accountability Office (GAO)) that addresses BEA's performance related to the protection and control of classified information. In addition, provide general performance related information (i.e., non-program specific) relative to the protection and control of classified information for BEA SAPs and intelligence programs.
- Formally define BEA's regulatory screening process for classified information security-related noncompliances and clearly identify the roles and responsibilities for both S&S personnel and the enforcement coordinator. In addition, as a part of the screening process, define the criteria for noncompliances in ICAMS that fall under the provisions of 10 C.F.R. Part 824.
- Formally define the criteria for determining types of noncompliances and/or deficiencies (e.g., finding, issue, observation, opportunity for improvement) resulting from IOSCs and internal assessments. Furthermore, formally identify who has the ultimate authority for determining whether an identified issue is categorized as a finding, observation, opportunity, etc.
- Continue current efforts to enhance BEA's trending and analyses based on data currently being maintained in various databases, spreadsheets, and ICAMS. In addition, remain proactive in refining and improving existing trending processes as additional results from IOSCs, internal assessments, and external surveys/reviews are entered into ICAMS.
- Re-evaluate the existing BEA criteria for determining when causal analysis reviews are required. In addition, maximize the opportunity to determine the underlying cause of less-severe classified information security noncompliances to prevent more severe reportable security incidents (i.e., Impact Measurement Index (IMI) -1 and -2) from occurring.
- Enhance the CMPC self-assessment methodology by increasing the frequency and broadening the scope of meaningful performance-based activities designed to demonstrate program effectiveness.
- Include assessment results from all BEA organizations that work with classified information in the S&S CMPC assessment process to ensure overall performance effectiveness.

- Provide more detail in CMPC self-assessment reports to indicate the scope, methodology, and an analysis of the results for all assessment activities.
- Develop an annual S&S self-assessment report that captures all data collected throughout the fiscal year (FY) relative to BEA's S&S program performance (e.g., self-assessments, IOSC, external reviews). This report is intended, in part, to provide a basis for management to make informed decisions regarding the information security program, and to provide BEA senior management and DOE-ID with a complete picture of BEA's performance in the protection and control of classified information at INL.

## II. General Program Implementation

At the time of this review, BEA was actively involved in integrating the provisions of 10 C.F.R. Part 824 with its existing regulatory compliance program. Based on discussions, BEA recognized the need to re-evaluate the program structure to ensure that all classified information security programs and assets are fully integrated, including classified cyber security, SAPs, and intelligence programs. Although some regulatory program requirements have been documented in INL PDD-13819, *Safety and Security DOE Regulatory Program*, to include enforcement screening of security incidents involving the protection and control of classified information, not all requirements have been clearly defined and formally documented. For example, the regulatory compliance program processes for all classified information security programs (i.e., CMPC, IOSC, classified cyber security, SAPs, and intelligence programs) are not fully defined or documented in the appropriate BEA local procedures or in local training that addresses classified information security topics. Nevertheless, the review team observed a close and effective working relationship among personnel from the BEA regulatory compliance program, BEA S&S program, and DOE-ID.

BEA's S&S management was found to be supportive in the implementation and integration of the S&S program with its existing regulatory compliance program. The S&S program has embedded physical security officers (PSO) within each of its facilities across the INL. The PSOs play a significant role in implementing the security program. Although the PSOs are physically located within facilities throughout the INL, the S&S program manages the daily activities of the PSOs. The PSOs are responsible for providing security-related guidance and solving security problems for the line management they support.

The review team's discussions with BEA security personnel responsible for the protection and control of classified information and the regulatory compliance program personnel revealed that they were all well-trained and knowledgeable of program responsibilities. Personnel were also found to be familiar with the regulatory and classified information security policy requirements. BEA management indicated that a concerted effort has been made to consolidate classified matter and reduce the number of areas where classified information is stored; reduce the total number of classified holdings; and limit the number of personnel with access to classified information. These

measures decrease the likelihood of classified information being lost, compromised, or mishandled. BEA has also implemented a proactive means of communicating lessons-learned on classified information security topics and requirements. For example, BEA has established mechanisms to reach the entire INL population through the use of "I-Notes" and "Flash." Both of these tools are provided electronically to the entire INL to communicate timely lessons-learned. Although the security education program is in a state of transition, the communication network already established can be used to enhance the program.

Discussions with classified cyber security representatives indicated that the cyber security program works closely with the S&S IOSC program during incident responses involving contamination of unclassified cyber systems. However, the classified cyber security program is not currently integrated with BEA's regulatory compliance program. As a result, noncompliances involving classified information security within the classified cyber security program are not shared with, or screened by, BEA's regulatory compliance program personnel.

BEA management's continued attention and commitment to the overall security program remain crucial to the continued success of integrating BEA's classified information security programs with its regulatory compliance program.

### **Strengths**

- Management attention and commitment to the overall security program are evident, as exemplified, in part, by the support provided to the integration of the classified information security program with the existing regulatory compliance program, as well as the proactive approach in communicating security incidents that involve the protection and control of classified information to senior level management. In addition, BEA has also been active in reducing its classified holdings.
- Effective partnerships and lines of communication among BEA's security organization (Laboratory Protection), the BEA enforcement coordinator, and DOE-ID are apparent.
- BEA personnel with responsibilities for regulatory compliance and classified information security appear to be well trained and knowledgeable of program responsibilities.

### **Recommendations**

- Formally document applicable requirements identified in 10 C.F.R. Part 824 in all of BEA's local CMPC, IOSC, and classified cyber security program procedures, as well as local training that addresses classified information security topics.
- Clearly define and formally document the regulatory compliance program structure for all classified information security programs (i.e., CMPC, IOSC, classified cyber

security, SAPs, and intelligence programs), including lines of authority and associated roles and responsibilities.

### III. Identification and Reporting of Incidents of Security Concern

INL policy MCP-3786, *Incidents of Security Concern*, serves as the implementation tool for the IOSC program. All employees report potential IOSCs to their PSO, the warning communication center, or the nearest protective force member. Any person discovering a security interest at risk (e.g., classified matter, government property) must take reasonable and prudent steps to contain the incident, protect the scene to ensure that evidence is not tampered with or destroyed, and appropriately secure classified matter.

Security incidents reported through the PSO are initially analyzed by the PSO to determine if the IOSC program should be involved. Although the PSOs are familiar with the IMI tables regarding what types of incidents are reportable, incidents involving the protection and control of classified information may fall under the provisions of 10 C.F.R. Part 824 and may also require the involvement of the BEA regulatory compliance program. In order to ensure the accurate reporting and involvement of appropriate personnel for incidents involving the protection and control of classified information, PSOs should ensure the involvement of the IOSC program. BEA reports IOSCs to DOE Headquarters through SSIMS.

IOSCs are categorized and resolved in accordance with DOE Manual 470.4-1, Chg. 1, Part 2, Section N, *Incidents of Security Concern*. BEA's IOSC program utilizes a multi-disciplinary approach for initially categorizing security incidents involving classified information by consulting BEA's S&S management, security program SMEs (as deemed necessary), and DOE-ID. If classified information is found to have been processed or stored on an unclassified cyber system, the process described in INL PLN-2731, *INL Classified Cyber Security Incident Response Plan*, is implemented to contain and sanitize all affected systems and provide support to the inquiry official, as needed.

The review team examined 11 security incident files and determined that the IMI categorizations were accurate, and that all requisite initial reporting and incident inquiry timelines were met. The inquiries were found to be thorough, and many of the reports were well written. However, in some instances, the inquiry narratives lacked the necessary details to allow third-party readers to easily understand the circumstances surrounding the incident, as well as the evidence supporting the categorization. In addition, improvement in timeliness of closure of less-significant IOSCs (i.e., IMI-3 and -4) would allow for more relevant sharing of lessons-learned, corrective actions, and identification of trends.

Discussions with personnel assigned to the IOSC program revealed that the staff is knowledgeable of program requirements and BEA operations. Furthermore, each inquiry official has years of investigative experience and was able to submit documentation of investigative training to obtain credit for completion by the DOE National Training Center.



## **Strengths**

- BEA IOSC program personnel are knowledgeable of program requirements and have years of investigative experience.
- BEA uses a multi-disciplinary team approach to ensure the accuracy of initial categorization of security incidents that includes SMEs, the division director for Security Programs and Services, and DOE-ID, as appropriate.
- BEA IOSC inquiry officials conduct thorough security incident inquiries.

## **Recommendation**

- Document sufficient details in inquiry reports so that third-party readers can easily understand the circumstances surrounding the incident and the evidence that supports the incident categorization.

## **IV. Issues Management and Trending**

BEA currently uses multiple systems for tracking and trending security noncompliances identified through various means, such as IOSCs, self-assessments, and external reviews. At the time of this review, BEA had initiated the process of entering all S&S noncompliance data into ICAMS. ICAMS is an unclassified database that BEA intends to use as the central location for recording all S&S noncompliances (e.g., incidents, internal and external findings, opportunities for improvement) and all associated corrective actions. The current use of multiple tracking systems has made it difficult for BEA to accurately describe its performance in protecting and controlling classified information. To date, BEA has only entered IOSCs for FY 2011 into ICAMS. All other security noncompliances continue to be tracked in separate systems and spreadsheets.

BEA's proactive approach in refining and improving its trending processes remains essential to accurately identify performance indicators, especially as additional data resulting from IOSCs, internal assessments, and external surveys is entered into ICAMS. If successful, all performance-related data will be maintained in an integrated system that provides timely and meaningful trending information. Although ICAMS is currently being populated with limited S&S-related information, it is scheduled to become fully operational for all S&S data in FY 2012. The goal is for all BEA organizations to provide S&S input into ICAMS. In fact, the BEA S&S assessment activities will be linked to ICAMS, which will provide a "bigger picture" of BEA's ability to protect and control classified information. However, it is critical to the success of this program that this information be readily available and shared between the S&S organization and the regulatory compliance program. Access to all available information related to the protection and control of classified information would allow the enforcement coordinator to better understand BEA's performance related to the protection and control of classified information. This information would include IOSCs, internal assessment reports (including classified cyber security, SAPs, and intelligence programs), trending and

analysis data, protective force incident reports, and external audit reports, such as DOE-ID security surveys, external oversight inspections, and other government agency investigations (e.g., IG, GAO).

Because ICAMS is not yet fully operational in tracking and trending all S&S-related information, BEA is unsure of the system's ability to capture enough detailed information to effectively identify adverse trends. One potential shortcoming is that ICAMS is an unclassified system; therefore, the S&S-related information that can be entered is severely limited. BEA could benefit by benchmarking with other DOE/National Nuclear Security Administration organizations that have a mature process in addressing these types of issues (see section VI). In addition, incorporating all S&S information into ICAMS, regardless of the identifying organization, would permit more effective tracking and trending, as well as providing centrally located data for use by the S&S organization and the regulatory compliance program. Given the sensitivity of some information, at a minimum, a placeholder could be provided in ICAMS to ensure that critical information is not neglected when determining BEA's overall performance in protecting and controlling classified information. If information is segregated or "stovepiped," it will be difficult to obtain the "bigger picture" of BEA's performance, which management should have in order to make informed decisions regarding the status of BEA's S&S program.

The review team also discussed with BEA management the possibility of BEA using SSIMS to self-report applicable 10 C.F.R. Part 824 programmatic, repetitive, or willful/intentional noncompliances identified during internal inspections, assessments, and trending activities. SSIMS provides a classified platform that allows contractor organizations to securely self-report noncompliant conditions that do not meet the established mandatory reporting criteria. Such reporting is purely voluntary, and BEA management may use this capability at its discretion.

BEA's issues management process for both IOSCs and self-assessment noncompliances involves several steps: identifying the issue; completing an issue worksheet; entering the issue into ICAMS; having the screening committee review the issue; determining whether the noncompliance is a deficiency, an issue, an opportunity for improvement, etc.; and identifying the appropriate corrective action(s). In reviewing various procedures on the management of issues, several terms were used to describe noncompliances. Some of these terms (e.g., finding, issue, recommendation, observation, opportunity for improvement) appeared to be used interchangeably and not formally defined in local procedures. In addition, the procedures do not identify who has the ultimate authority for determining which term is used when categorizing identified issues. Furthermore, during discussions with BEA personnel concerning BEA policies and procedures related to the issues management process, the review team noted a lack of clarity regarding the regulatory screening of security noncompliances, as well as identifying who is specifically responsible for conducting the regulatory screening process.

INL policy MCP-298, *Safeguards and Security Assurance Program*, describes the corrective action program for noncompliances related to the protection and control of classified information. Currently, this procedure does not address the use of ICAMS and

BEA recognizes that this procedure will need to be revised once ICAMS is fully implemented. In addition, this procedure states that the responsible manager and lead assessor will determine the priority/significance of an issue (i.e., high, medium or low). The significance category of an issue also drives the type of causal analysis to be performed. There are three levels of causal analysis: Level I (formal); Level II (defined in LWP 13845, principally an apparent cause analysis); and Level III (apparent cause). However, only IMI-1 or a serious IMI-2 (if management indicates) security incidents require a formal causal analysis. This restrictive criteria formally established by the BEA procedure could discourage a formal causal analysis from being conducted in cases where it would be warranted (e.g., IMI-3.3). Furthermore, this procedure does not address causal analysis activities for less severe classified information security noncompliances. Determining the underlying causes of less-severe noncompliances (i.e., IMI-3 and -4) that involve the protection and control of classified information could prevent the reoccurrence of these noncompliances and prevent the more severe (i.e., IMI-1 and -2) noncompliances from occurring.

BEA requires anyone responsible for conducting causal analysis to receive the appropriate training for the level of analysis they are authorized to perform. Due to the rigor of the Level 1 causal analysis training, only three Q-cleared personnel at BEA have the requisite training to do formal causal analysis. The BEA enforcement coordinator has completed this training and has conducted formal causal analyses for S&S-related incidents. However, the enforcement coordinator is not informed of other causal analyses being preformed as a result of incidents or noncompliances identified during S&S assessment activities.

### **Strength**

- BEA requires training for all personnel responsible for conducting causal analysis.

### **Recommendations**

- Continue ongoing efforts to implement ICAMS to provide BEA with a centralized database for the effective management of all identified S&S noncompliances.
- Provide the enforcement coordinator with all available information (e.g., internal assessment reports, including classified cyber security; trending and analysis data; protective force incident reports; and external audit reports, such as those resulting from DOE-ID security surveys; external oversight inspections; and investigations by other government agencies, such as the IG and the GAO) that addresses BEA's performance related to the protection and control of classified information. In addition, provide general performance related information (i.e., non-program specific) relative to the protection and control of classified information for BEA SAPs and intelligence programs.
- Formally define BEA's regulatory screening process for classified information security-related noncompliances and clearly identify the roles and responsibilities of

both S&S personnel and the enforcement coordinator. In addition, as a part of the screening process, define the criteria for noncompliances in ICAMS that fall under the provisions of 10 C.F.R. Part 824.

- Formally define the criteria for determining types of noncompliances and/or deficiencies (e.g., finding, issue, observation, opportunity for improvement) resulting from IOSCs and internal assessments. Furthermore, formally identify who has the ultimate authority for determining whether an identified issue is categorized as a finding, observation, opportunity, etc.
- Continue current efforts to enhance BEA's trending and analyses based on data currently being maintained in various databases, spreadsheets, and ICAMS. In addition, remain proactive in refining and improving existing trending processes as additional results from IOSC, internal assessments, and external surveys/reviews are entered into ICAMS.
- Re-evaluate the existing BEA criteria for determining when causal analysis reviews are required. In addition, maximize the opportunity to determine the underlying cause of less-severe classified information security noncompliances to prevent more severe reportable security incidents (i.e., IMI-1 and -2) from occurring.

## V. Assessments

BEA has established a CMPC self-assessment program to ensure that classified information assets are protected at appropriate levels; facilitate improvement by self-identifying noncompliant conditions; and enter the results into an issues management system. The CMPC self-assessment program is part of the overall S&S assurance program, which is contained within the asset protection management system. Each BEA management system (like the asset protection management system) has a "portfolio" that describes how performance assurance is achieved. BEA is in the process of using the "portfolio" information to determine the scope and frequency of CMPC self-assessments.

There are two basic levels of evaluation activity: (1) inspection/surveillance (hereinafter referred to as self-assessment) and (2) management and independent assessments. Self-assessments are the least "intrusive" form of evaluation, according to BEA's assurance program personnel. These assessments focus on compliance with DOE and BEA requirements and are considered the most "basic" form of assessments. Interviews with the managers of the CMPC and S&S assurance program indicated the desire to implement an effective assessment program, and both managers were aware of the importance of this program in preventing a significant security event from occurring at INL.

CMPC self-assessment activities are primarily compliance-based evaluations that use checklists as the basis for the assessment. They are conducted throughout INL in all organizations working with classified information, with the exception of the classified assets associated with the Specific Manufacturing Capability (SMC) and some

intelligence programs; historically, the SMC and intelligence programs have been outside the scope of the traditional BEA CMPC assessment. As a result, these assessment activities and the related results are not shared with BEA's S&S CMPC program, which prevents BEA from having a complete view of its performance related to the protection and control of classified information. However, as an indicator of the increased emphasis on CMPC assessment activities, CMPC assessment personnel have been recently requested, by intelligence program personnel, to assist in conducting assessments within BEA's intelligence programs.

Currently, BEA's CMPC self-assessment program is principally aimed at document storage locations (i.e., repositories and vault-type-rooms). The CMPC SMEs independently determine the schedule and scope of all CMPC self-assessments. A report is completed for each assessment (i.e., storage location). As mentioned, these assessments are compliance-based, and the CMPC self-assessment checklist (Form 471.13) is the principal evaluation tool. Assessment reports also contain a narrative that provides additional detail, such as how the assessment was conducted, specific locations where the assessment occurred, and the assessment results. CMPC assessments are conducted by experienced personnel with sufficient training to assess the assigned security topics. Interviews with personnel responsible for conducting assessments indicated that a mechanism is in place to provide timely notification to the appropriate managers and other designated personnel when deficiencies are identified.

The review team analyzed 57 CMPC self-assessment reports that were conducted during FY 2010 through March 2011. The review validated that BEA's CMPC assessment methodology includes document reviews, interviews, and observations, but there was limited evidence of any performance testing. Although the assessment approach was found to be primarily compliance-based and driven by the CMPC self-assessment checklist, there was evidence that numerous other evaluation activities were performed, but not documented in the assessment report.

This review found that the scope of the CMPC assessment encompassed all areas of the CMPC program. However, in reviewing the assessment reports, it was not immediately clear which specific locations were evaluated during the assessment activities. Although this information is provided mid-way through the assessment report, it would be helpful to the reader if this information were to be included in the title page of the report. Since each individual report addresses a given area/repository, it is critical that an annual composite report be developed to achieve the Department's objective for the self-assessment program – namely, to provide a basis for management to make programmatic decisions about the classified information security program.

Given the compliance-based nature of the current checklists, additional emphasis could be placed on the quality of performance-based activities conducted during CMPC assessments. For example, employees could be asked to demonstrate important classified information security tasks required by the position.

Management assessments and independent assessments are higher-level assessments that vary slightly in approach. Management assessments perform a “rollup” function by combining the results of several inspections to provide a more complete evaluation of the area being assessed. Management assessments in the area of CMPC take an INL-wide approach to assess the implementation of BEA’s CMPC program. The focus of both the management and independent assessments is to measure and determine BEA’s performance effectiveness across INL-wide activities. An independent or management assessment of the security regulatory compliance program across the INL would provide BEA an evaluation of the processes for identifying classified information security noncompliances; reporting and tracking classified information security noncompliances in SSIMS; using internal deficiency tracking/trending systems; and correcting deficiencies to prevent recurrence.

### **Strengths**

- Personnel performing self-assessments are trained and have subject matter expertise in the areas they are assessing.
- Improvement in the overall structure of the BEA CMPC self-assessment program is evident, as exemplified, in part, by expanding assessment activities to include all BEA directorates that handle and store classified information.

### **Recommendations**

- Enhance the CMPC self-assessment methodology by increasing the frequency and broadening the scope of meaningful performance-based activities designed to demonstrate program effectiveness.
- Include assessment results from all BEA organizations working with classified information in the S&S CMPC assessment process to ensure overall performance effectiveness.
- Provide more detail in CMPC self-assessment reports to indicate the scope, methodology, and an analysis of the results for all assessment activities.
- Develop an annual S&S self-assessment report that captures all data collected throughout the FY relative to BEA’s S&S program performance (e.g., self-assessments, IOSC, external reviews). This report is intended, in part, to provide a basis for management to make informed decisions regarding the information security program, and to provide BEA senior management and DOE-ID with a complete picture of BEA’s performance in the protection and control of classified information at INL.

## VI. Summary

BEA has established a strong foundation for its classified information security regulatory compliance program and has established the framework in its regulatory compliance program documentation. This review identified many attributes that point to BEA's ability to continue its efforts in establishing an effective classified information security regulatory compliance program. The enforcement coordinator has a wealth of site operational experience, a solid quality assurance background, and the respect of management and operations personnel. The review team also recognized others within the S&S organization that displayed a high level of technical competence and dedication to their professions. BEA has a well-established IOSC program that provides for the accurate categorization of security incidents and the conduct of comprehensive inquiries by knowledgeable and trained staff. In addition, BEA has established a sound foundation for an effective CMPC self-assessment program that ensures that classified information is protected at appropriate levels.

Although BEA has been actively involved with integrating classified information security into its existing regulatory compliance program, the processes for all classified information security programs (i.e., CMPC, IOSC, classified cyber security, SAPs, and intelligence programs) are not fully defined or documented in the appropriate BEA local procedures or local training that addresses classified information security topics. A number of recommendations have been identified throughout this report to provide opportunities to further improve BEA's classified information security regulatory compliance program.

By appropriately addressing the recommendations identified during this review, it is expected that BEA would realize improved performance in its ability to avoid or reduce the severity of classified information security noncompliances; subsequently facilitate the Office of Security Enforcement's exercise of discretion for noncompliant conditions that are considered to be less significant; support mitigation consideration in any future enforcement action; and ensure that classified information security protection shortcomings receive appropriate recognition and corrective actions. Any actions taken to address these recommendations should be appropriately coordinated with the DOE Office of Nuclear Energy and DOE-ID.

In addition to the recommendations identified throughout this report, the following suggestions are also provided. The review team encourages BEA to consider these suggestions as a means of strengthening BEA's classified information security and regulatory compliance programs:

- Benchmarking with other DOE sites regarding the integration and coordination of the security organization with the existing regulatory compliance program.
- Contacting other sites (e.g., the Y-12 National Security Complex) to determine whether its regulatory compliance program activities (including the tracking, trending, and analysis systems) could improve BEA's existing processes.

- Addressing timeliness in closure of less-significant IOSCs (i.e., IMI-3 and -4) to allow sharing of lessons-learned, timely corrective actions, and identification of trends.
- Consulting the recently identified risk-ranking criteria contained in the assurance portfolio for asset protection management systems when developing the FY S&S self-assessment schedule.
- Including additional human performance indicators in the IOSC and causal analysis processes, and documenting the methods used and the correlating results.
- Recognizing and addressing communication short-comings amongst the various facilities, security program topics, and organizations in sharing lessons-learned and addressing issues involving the protection and control of classified information at INL.



**List of Acronyms**

BEA	Battelle Energy Alliance, LLC
C.F.R.	Code of Federal Regulation
CMPC	Classified Matter Protection and Control
DOE	U.S. Department of Energy
DOE-ID	DOE Idaho Operations Office
EPO	Enforcement Process Overview
FY	Fiscal Year
GAO	Government Accountability Office
ICAMS	Integrated Corrective Action Management System
IG	Office of the Inspector General
IMI	Impact Measurement Index
INL	Idaho National Laboratory
IOSC	Incident of Security Concern
PSO	Physical Security Officer
SAP	Special Access Program
SMC	Specific Manufacturing Capability
SME	Subject Matter Expert
S&S	Safeguards and Security
SSIMS	Safeguards and Security Information Management System