



Department of Energy

Washington, DC 20585

November 19, 2009

Dr. Samuel Aronson
Director
Brookhaven National Laboratory
40 Brookhaven Avenue
Upton, New York 11973-5000

Dear Dr. Aronson:

The Office of Health, Safety and Security's Office of Security Enforcement conducted an onsite program review from July 14-16, 2009, of the classified information security program elements that support the Brookhaven Science Associates, LLC (BSA) regulatory compliance program. Our review included: an evaluation of processes for identifying noncompliances; reporting and tracking noncompliances in the Safeguards and Security Information Management System; internal tracking systems; and correcting deficiencies to prevent recurrence. The Office of Security Enforcement also conducted a limited review of BSA management and independent assessment programs.

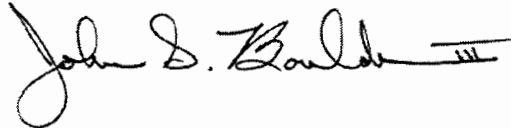
Although BSA is in the initial stages of integrating security activities and Title 10 Code of Federal Regulations (C.F.R.) Part 824 into its existing enforcement program, a number of improvement initiatives related to implementation of the security regulatory compliance program is underway. The results of this review, described in the enclosed report, identified a number of strengths and some weaknesses with the BSA security enforcement program.

The Department of Energy's Enforcement Policy (10 C.F.R. Part 824) allows for the mitigation of civil penalties for self-identification and timely reporting of noncompliance issues, as well as for effective corrective action. Thus, failure to correct the weaknesses noted in this report may result in a potential reduction or loss of mitigation for any future enforcement action against BSA. In addition, should these weaknesses persist, the Office of Enforcement would be less likely to exercise enforcement discretion for noncompliance issues that are of lesser significance.



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 Crowe, Director, Office of Security Enforcement, at (301) 903-0107.

Sincerely,

A handwritten signature in black ink that reads "John S. Boulden III". The signature is written in a cursive style with a horizontal line at the end.

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

Enclosure

cc: Charles Dimino, BSA
John Amabile, BSA

**OFFICE OF SECURITY ENFORCEMENT
PROGRAM REVIEW
BROOKHAVEN SCIENCE ASSOCIATES, LLC**

I. Introduction

During July 14-16, 2009, the Office of Security Enforcement, within the Office of Health, Safety and Security, conducted a program review of classified information security programs at Brookhaven Science Associates, LLC (BSA). Compared to other Departmental facilities possessing classified information, BSA has a relatively small amount of classified holdings and a limited number of cyber assets accredited for classified processing. The program 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 can be found on the Office of Health, Safety and Security website under the Office of Enforcement at:

http://www.hss.energy.gov/enforce/Final_EPO_June_2009_v4.pdf

This review included an evaluation of BSA processes for identifying classified information security noncompliances; reporting and tracking classified information security noncompliances in the Safeguards and Security Information Management System (SSIMS); monitoring of BSA internal deficiency tracking/trending systems; and correcting deficiencies to prevent recurrence. It also included a limited review of BSA management and internal security self-assessment programs, as well as an evaluation of the BSA security regulatory compliance program, which documents processes at BSA for identifying, reporting and correcting noncompliances in accordance with requirements defined by Title 10 Code of Federal Regulations (C.F.R.) Part 824 (10 C.F.R. Part 824), *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*, and Departmental security policies. The information in this report is based on a review of the BSA program documentation provided to the review team as well as interviews with personnel responsible for implementing the BSA compliance monitoring program.

At the time of this review, BSA had a number of ongoing improvement initiatives related to the implementation of its security regulatory compliance program. These initiatives are discussed in section VII of this report. In addition, this review identified a number of strengths and some weaknesses regarding the effectiveness of BSA's regulatory compliance program pertaining to classified information security. Each strength and weakness is discussed in further detail within the body of this report and is provided in a consolidated list as follows:

Strengths:

- A pro-active approach was used in requesting Pacific Northwest National Laboratory (PNNL) to conduct a peer review of the BSA security enforcement program prior to this program review.

- The BSA Laboratory Protection Division (LPD) has recently developed an effective relationship and lines of communication with the BSA regulatory compliance officer (RCO).
- BSA utilizes a team concept in the initial categorization of security incidents which includes subject matter experts (SME) from BSA, Brookhaven Site Office (BHSO), and the Office of Science Chicago Office – Integrated Support Center (SC-CH). In addition, the BSA LPD has a pro-active, knowledgeable, and competent staff.
- The BSA RCO is knowledgeable of regulatory requirements and the Office of Enforcement’s guidance as described in the EPO.
- BSA utilizes a comprehensive self-assessment tool that addresses all applicable safeguards and security programs. The self-assessment involving classified matter protection and control (CMPC) is completed by knowledgeable staff, provides a thorough description of what was assessed, and the BSA CMPC program manager validates assessment results.
- Internal assessment results are broadly communicated to BSA management, BHSO, and SC-CH.
- BSA exhibits a strong “self-reporting” culture.
- BSA LPD advocates a conservative philosophy for categorizing its security incidents.
- BSA LPD conducts thorough incident inquiries and completes timely, well-documented inquiry reports. Case files are well maintained and include thorough supporting documentation.
- BSA employs conservative administrative controls regarding the use, transmission, storage, and destruction of classified matter.
- Classified matter custodians and users receive initial and annual CMPC training through the security education program and other specialized security briefings.
- BSA’s Information Technology Division (ITD) has a close and effective relationship with the LPD regarding classified cyber incidents.

Weaknesses:

- There is no requirement for BSA LPD to notify the RCO of internal assessment results.
- The BSA security education program does not ensure that all BSA personnel with classified matter responsibilities receive security enforcement (i.e., 10 C.F.R. Part 824) awareness training.
- The BSA corrective action process procedure does not clearly identify who is responsible for developing, approving, tracking, monitoring, and validating closure of security noncompliances.
- Independent verification and validation of causal analyses and corrective actions resulting from security noncompliances identified by security incidents, external audits/reviews and internal assessments are not being performed.
- Formal documentation of the BSA self-assessment program does not effectively explain the assessment methodology nor provide a detailed scope or description of how internal assessments are conducted.

- BSA self-identified noncompliances that are corrected on the spot are not formally documented or tracked in its action tracking system (ATS).
- Both the CMPC and cyber self-assessments focus on a compliance-based approach with only minimal performance-based components.
- BSA has not yet determined how it will utilize the opportunity to self-identify noncompliances through the recently provided (e.g., April 2009) SSIMS screen.

II. General Implementation

BSA recently developed a program description document¹ and a procedure² addressing its enforcement program. These documents outline the RCO responsibilities pertaining to causal analysis and corrective actions resulting from security incidents and classified information security assessments. However, this review found that while, BSA LPD procedure ADM-213, *Reporting Incidents of Security Concern* describes the role of the RCO in the notification of security incidents, there is no specific requirement that the BSA LPD notify the RCO of assessment results.

The BSA RCO is currently developing a risk significance assessment tool and corrective action process that will include elements of the security incident program into the existing BSA enforcement program.

Based on discussions with BSA RCO and BSA LPD management, there is an inclusive knowledge of regulatory requirements (i.e., 10 C.F.R. Part 824) amongst its staff. However, the general BSA population with classified matter responsibilities is not fully aware of the regulatory requirements or expectations. In addition, discussions with the BSA ITD representatives revealed that they were less aware of the regulatory requirements, compared to the LPD staff.

At the request of BSA, PNNL conducted a peer review of its security enforcement program in June 2009. The PNNL review report³ contained meaningful recommendations to improve BSA's existing security enforcement program.

Specifically, the PNNL review noted: a positive reporting culture is maintained at BSA; the security incident program is well documented and includes the requisite program elements; BSA is categorizing its security incidents appropriately; and SMEs (i.e., physical security, CMPC, cyber security) are consulted as needed during the incident notification and inquiry processes.

In addition, the PNNL peer review identified 17 areas needing improvement, along with suggested recommendations to address the program weaknesses. At the time of this review, the Office of Security Enforcement found that BSA had already addressed many

¹ Health, Safety, and Security Regulatory Compliance Validation and Noncompliance Reporting, dated June 8, 2009.

² Health, Safety and Security Regulatory Compliance Review and Reporting Procedure, dated June 24, 2009.

³ Program Peer Review, dated June 10, 2009.

of the PNNL identified areas for improvement, and was actively addressing and working towards full implementation of those recommendations. The weaknesses reflected in this report are in addition to the ones identified by the PNNL peer review.

Security incidents reported through the BSA incidents of security concern program are categorized and resolved in accordance with DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management*. The LPD and BHSO consult on the initial categorization of security incidents and then share their thoughts with SC-CH prior to entering the incident notification into SSIMS. The BSA RCO is also notified of security incidents as they occur.

Depending on the complexity of the issue or severity of the security incident, an informal root cause analysis is conducted by the inquiry official. This usually consists of one of several causal analysis tools (i.e., the “Five Whys”, a simplified barrier analysis, or a TapRoot analysis). Corrective actions resulting from security incidents are developed and tracked by the LPD manager and maintained in ATS. However, security deficiencies resulting from self-assessments, performance testing, and other assessment tools are not being communicated to the BSA RCO or tracked in ATS. Additionally, there is currently no procedure that formally identifies who is responsible for the development, approval, tracking, monitoring, and closure of corrective actions, to include verification and validation.

This review found that the BSA classified matter assets are strictly controlled by trained and knowledgeable CMPC custodians. BSA employs conservative administrative controls on its classified assets, which aids in minimizing the potential for classified matter related noncompliances. All BSA custodians and users of classified matter receive initial and annual CMPC training. In addition, SC-CH is in the process of arranging to have the DOE National Training Center provide the CMPC I training course at Brookhaven National Laboratory through a mobile training team.

Strengths:

- The BSA RCO is knowledgeable of regulatory requirements, and the Office of Enforcement expectations and protocols, as described in the EPO.
- The BSA LPD has recently developed an effective relationship and lines of communication with the BSA RCO.
- A pro-active approach was used in requesting PNNL to conduct a peer review of the BSA security enforcement program prior to this program review.
- BSA employs conservative administrative controls regarding the use, transmission, storage, and destruction of classified matter.
- Classified matter custodians and users receive initial and annual CMPC training through the security education program, and other specialized security briefings.

Weaknesses:

- There is no requirement for BSA LPD to notify the RCO of internal assessment results.
- The BSA corrective action process procedure does not clearly identify who is responsible for developing, approving, tracking, monitoring, and validating closure of security noncompliances.
- The BSA security education program does not ensure that all BSA personnel with classified matter responsibilities receive security enforcement (i.e., 10 C.F.R. Part 824) awareness training.

III. Identification and Categorization of Security Incidents

This section of the report discusses the specific activities involving the identification and categorization of reportable security incidents. At BSA, there are two primary sources of identification of reportable security incidents: (1) the incidents of security concern program, and (2) the LPD biennial self-assessment (see section VI). Both of these programs currently reside within the LPD.

BSA procedure ADM-213, *Reporting Incidents of Security Concern*, describes the requirements for BSA employees to ensure the timely identification, notification, inquiry, reporting, and follow-up of security incidents that occur at BSA. Specifically, this procedure covers the following program elements associated with reportable security incidents: identification, notification, inquiry, reporting (see section IV), determination and implementation of corrective actions (see section V), and incident closeout (see section V). In addition, BSA procedure ADM-220, *Roles and Responsibilities*, describes the roles and responsibilities of personnel who handle security incidents at BSA.

When any BSA employee observes, finds, or has knowledge of or information regarding a security incident, the procedure directs them to immediately notify their supervisor and the LPD manager or his designee. The procedure indicates that the initial notification may be made to an Occurrence Reporting and Processing System (ORPS) categorizer. The ORPS categorizer is then responsible for determining if the report falls under DOE Manual 470.4-1, change 1, section N. If so, the ORPS categorizer will contact the LPD manager, security operations manager, or his designee.

Upon notification of a security incident, the LPD manager and the appointed inquiry official review the known circumstances, consult with SMEs, as appropriate, and review evidence to determine the appropriate Impact Measurement Index (IMI) categorization. Interviews conducted during this review with the BSA incidents of security concern program personnel revealed that SMEs from other departments (i.e., CMPC, physical security, and ITD), as well as, BHSO and SC-CH assist in categorizing security incidents.

If a potential compromise of classified information occurs, the inquiry official takes immediate action to secure the classified information, in any form or place where it exists. In the event that classified information is processed or stored on an unclassified

system, the ITD staff and the information systems security officer staff will work to contain and sanitize the affected systems and provide support to the inquiry official.

BSA LPD management has the responsibility to notify BHSO, the BSA Laboratory Director and Assistant Laboratory Directors of the security incident occurrence and the initial IMI categorization. Additional notifications are made to the appropriate organizations (i.e., SC-CH, local Counterintelligence, the HSS Office of Security Technology and Assistance), as required.

Inquiry reports are developed, in accordance with DOE Manual 470.4-1, change 1, section N, and contain the required data collection relevant to the security incident, conduct of interviews, collection, and protection of physical evidence. The inquiry report identifies all persons associated with the incident, and a chronological sequence of events is developed to capture activities preceding and following the incident. BSA LPD then analyzes the incident to determine which systems/functions performed correctly, or failed to perform as designed, when determining the cause of the incident and subsequent corrective actions. To support the causal analysis process, BSA LPD currently uses analysis tools such as, "Five Whys," a simplified barrier analysis, or TapRoot techniques.

Discussions with personnel assigned to the incidents of security concern program revealed that the staff is knowledgeable of their designated responsibilities and BSA operations. They also have appropriate security expertise and years of security experience (e.g., one individual has 8 years of experience and another has over 23 years of experience).

During this review, the Office of Security Enforcement assessed five security incident report files and determined that the IMI categorizations were accurate, and all initial reporting and incident inquiry timelines were met. Based on discussions with BSA LPD personnel responsible for determining the IMI categorization, it is apparent that BSA employs a conservative approach when determining the initial categorization of security incidents. This practice ensures that incidents with higher security significance receive the necessary rigor when conducting the causal/root cause analysis and identifying corrective actions to prevent recurrence.

The Office of Security Enforcement reviewed the latest BSA security incident data contained in SSIMS. Inconsistencies were identified regarding the number of incidents reported in SSIMS versus the number of incidents identified by BSA. The list of security incidents provided by BSA as part of the document request for this review indicated that BSA had one open incident and two closed incidents for 2008 and 2009. However, the SSIMS data indicated that an additional two incidents remained open, one from 2007 and one from 2008. This review determined that the discrepancy arose from two incidents that were entered by SC-CH without the knowledge of BSA personnel. BSA was unaware that these two incidents remained open and were being tracked by Headquarters. Immediate corrective actions were taken by SC-CH and BSA LPD to address and resolve these open incidents.

Strengths:

- BSA utilizes a team concept in the initial categorization of security incidents which includes SMEs from BSA, BHSO, and SC-CH. In addition, the BSA LPD has a proactive, knowledgeable, and competent staff.
- BSA LPD advocates a conservative philosophy for categorizing its security incidents.
- BSA LPD conducts thorough incident inquiries and completes timely, well-documented inquiry reports. Case files are well maintained and include thorough supporting documentation.
- BSA's ITD has a close and effective relationship with the LPD regarding classified cyber incidents.

No specific weaknesses were identified under this section.

IV. Reporting

Based on the significant level of trust between management and employees, it is evident that BSA has a strong and viable "self-reporting" culture. The BSA LPD supports this culture by communicating identified security concerns to the entire BSA population through initial awareness briefings for all personnel and continuing refresher training for personnel with classified matter responsibilities. The LPD has also demonstrated extensive outreach by addressing employee reporting responsibilities in security education briefings and by posting reporting requirements on the BSA employee website. As a result, personnel are aware of the important security issues and when/how to report occurrences when observed.

Strength:

- BSA exhibits a strong "self-reporting" culture.

No specific weaknesses were identified in this section.

V. Issues Management and Trending

Currently, BSA LPD management and staff review the BSA ATS and its internal tracking system (i.e., excel spreadsheets) to ensure security incidents are addressed in a timely manner. Because of the low frequency of security incidents occurring at BNL (e.g., an average of two incidents of security concern per year), no formal trending analysis of security incidents is necessary. Once 10 C.F.R. Part 824 is fully integrated with the BSA enforcement program, all identified issues, including security issues and noncompliances will be included in ATS.

The BSA causal analysis program, as it relates to security incidents, is not yet formally defined. Causal analysis is covered briefly in BSA procedure ADM-213, *Reporting Incidents of Security Concern*, which states: "LPD uses root cause analysis models to determine root causes and contributing factors. In most cases, brainstorming and the

“Five Whys” technique are used. If more complex incidents are involved, the Inquiry Official coordinates root cause analysis with the BSA RCO. IMI-1 and IMI-2 synopses are sent to the Laboratory’s Lessons Learned Coordinator as classification permits.” This review determined that causal analyses are being conducted using a graded approach; however, the structure and methodology has not been formally defined and, therefore, is not always applied effectively or in a consistent manner.

The BSA existing causal analysis program, as it relates to nuclear safety and worker health and safety, is applied using a graded approach to ensure that corrective actions are commensurate with the impact of the event/issue and to effectively prevent recurrence. The analysis is conducted by BSA staff assigned to determine the causes of events/issues. BSA has developed a risk significance matrix to assist in the selection of the appropriate analysis methodology. At the time of this review, this process was not applicable to security incidents. Notwithstanding, BSA recognizes this shortcoming and is currently working to develop an equivalent causal analysis process to support its security program.

Corrective actions taken in response to security incidents must be documented in accordance with Departmental policy. To comply with this requirement, BSA enters each resulting corrective action into ATS. Presently, the BSA enforcement program independently validates the completion and effectiveness of nuclear safety and worker safety and health corrective action plans. However, this independent validation process does not currently involve corrective actions resulting from security incidents, external audits/security inspections, or other internal security assessment activities conducted by BSA LPD.

When corrective action plans are developed in response to a security incident, the incidents of security concern program is responsible for reviewing the plan for completeness and providing concurrence. Once the corrective action plan is approved, the assigned department or division is responsible for monitoring and completing the actions and for closeout activities. Neither the incidents of security concern program nor the self-assessment programs are required to provide independent validation of corrective actions to ensure completion and effectiveness to prevent recurrence. BSA has identified this issue and will address it during the upcoming integration of security activities into its enforcement program, as discussed in section II.

No specific strengths were identified in this section.

Weakness:

- Independent verification and validation of causal analyses and corrective actions resulting from security noncompliances identified by security incidents, external audits/reviews, and internal assessments are not being performed.

VI. Assessments

The classified information security internal assessments are conducted by BSA LPD biennially. The self-identified noncompliances are not currently being formally tracked in ATS. BSA recognizes this issue and is still working through this integration/implementation process.

The security enforcement team reviewed the BSA report entitled, *Laboratory Protection Division FY 2008 Self-Assessment Report*. This report consists of a brief narrative describing the conduct of the self-assessment and a summary of findings, followed by a detailed description of each topical and sub topical area assessed, and the findings resulting from these assessments. The report listed a total of 10 findings related to the protection of classified matter during fiscal year 2008. BSA security self-assessments are conducted by knowledgeable and trained staff, with the assistance of SMEs when needed. The results of the internal assessment are validated by the BSA CMPC manager. In addition, the results are broadly communicated to BSA management, BHSO, and SC-CH.

A review of the self-assessment processes found that the tool used to conduct the internal assessment is comprehensive, but it focused mainly on compliance with applicable Departmental policies and employed only a minimal number of performance-based components. In addition, minor corrections that are made on the spot are currently not formally documented or tracked. This review also found that the BSA assessment report lacks specific details, in that it does not fully describe the methodology or the complete scope of assessment activities. For example, BSA LPD reviewed 100 percent of its classified matter holdings during its most recent assessment; however, this review is not discussed in the assessment report.

In order to fully meet the objectives of an internal assessment program to provide a basis for contract organizations to make informed decisions regarding implementation of security program activities, results should be supported by both compliance and performance-based components. In addition, the identification of all security program weaknesses found is necessary to develop and complete the appropriate corrective actions that will improve the overall security program and prevent recurrence.

The Office of Security Enforcement's review and discussions with BSA concerning its use of the newly available screen in SSIMS for reporting self-identified classified information noncompliances found that BSA has not yet developed a process for taking advantage of this feature.

Strengths:

- BSA utilizes a comprehensive self-assessment tool that addresses all applicable safeguards and security programs. The self-assessment involving CMPC is completed by knowledgeable staff, provides a thorough description of what was assessed, and the BSA CMPC program manager validates assessment results.

- Internal assessment results are broadly communicated to BSA management, BHSO, and SC-CH.

Weaknesses:

- Formal documentation of the BSA self-assessment program does not effectively explain the assessment methodology nor provide a detailed scope or description of how internal assessments are conducted.
- BSA self-identified noncompliances that are corrected on the spot are not formally documented or tracked in its ATS.
- Both the CMPC and cyber self-assessments focus on a compliance-based approach with only minimal performance-based components.
- BSA has not yet determined how it will utilize the opportunity to self-identify noncompliances through the recently provided (i.e., April 2009) SSIMS screen.

VII. Ongoing Initiatives

The planned installation of a SSIMS terminal at Brookhaven National Laboratory will allow BSA to self-report noncompliances discovered as a result of its self-assessment activities. In addition, BSA will be able to monitor the status of reported security incidents, which will alleviate any future concerns regarding BSAs awareness of its open security incidents.

The BSA RCO has recently developed a risk significance matrix to be applied to security incidents. The involvement of BSA security and cyber security SMEs in the development efforts will ensure that the determination process is logical and appropriate for the assessment of risks associated with security incidents and other identified classified information security noncompliances. This process can also be an effective tool to improve causal analysis and extent-of-condition activities.

The BSA RCO has developed enforcement training that has been provided to many personnel with classified matter responsibilities and is further reinforced through its website. However, this training has not yet reached all stakeholders (i.e., ITD staff). The continued outreach efforts by BSA LPD and the RCO are important to the success of the BSA security regulatory compliance program.

VIII. Conclusions

BSA is in the initial stages of integrating security activities and 10 C.F.R. Part 824 requirements into its existing enforcement program. The roles and responsibilities of the BSA RCO, as they relate to security enforcement, have not yet been formally defined and documented. Management's continued attention and commitment to the security program is crucial to the success of the integration of security into the BSA enforcement program.

Notable strengths include the overall robust security incident program, particularly the conduct of comprehensive inquiries by knowledgeable and trained staff and the inclusion of SMEs in the categorization of security incidents, inquiry, causal analysis, and corrective actions processes for security incidents.

The future implementation of ATS for tracking all security-related issues should improve the existing oversight of identified security program weaknesses and the effectiveness of implemented corrective actions to prevent the likelihood of recurrence. However, there is currently no independent verification or validation performed to ensure that corrective actions are implemented in a timely or effective manner.

By addressing the weaknesses identified during this review, BSA can facilitate the Office of Security Enforcement's exercise of discretion for noncompliant conditions that are less significant, support mitigation consideration in any future enforcement action, and ensure that classified information security shortcomings receive appropriate recognition and corrective actions. Any actions taken to address these weaknesses should be appropriately coordinated with BHSO and SC-CH.