Department of Energy
Washington, DC 20585

March 5, 2010

Mr. Darrel P. Kohlhorst
President and General Manager
Babcock & Wilcox Technical Services Y-12, LLC
P.O. Box 2005
Oak Ridge, Tennessee 37831-8014

Dear Mr. Kohlhorst:

The Office of Health, Safety and Security's Office of Security Enforcement conducted an onsite program review from October 5 – 8, 2009, of the classified information security program elements that support the Babcock & Wilcox Technical Services Y-12, LLC (B&W Y-12) regulatory compliance program. Our review included: an evaluation of B&W Y-12 processes for identifying classified information security noncompliances; reporting and tracking classified information security noncompliances in the Safeguards and Security Information Management System; B&W Y-12 internal tracking systems; and correcting deficiencies to prevent recurrence. The Office of Security Enforcement also conducted a limited review of B&W Y-12 safeguards and security self-assessment program and corrective actions taken in response to the July 2009 enforcement letter.

Although B&W Y-12 is in the initial stages of integrating security activities and Title 10 Code of Federal Regulations (C.F.R.) Part 824 into its existing safety enforcement program, the Office of Enforcement is encouraged by the improvement initiatives underway related to implementation of its security regulatory compliance program. The results of this review, described in the enclosed report, identified a number of strengths and some weaknesses with B&W Y-12's security enforcement program.

Correction of the weaknesses noted in this report may allow the Office of Enforcement to consider mitigation as described in the U.S. Department of Energy Enforcement Policy (10 C.F.R. Part 824, appendix A) for any future related enforcement action against B&W Y-12.

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,

John S. Boulden III

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

Enclosure

cc: Butch Clements, B&W Y-12
Conard Stair, B&W Y-12

OFFICE OF SECURITY ENFORCEMENT
PROGRAM REVIEW
BABCOCK & WILCOX TECHNICAL SERVICES Y-12, LLC

I. Introduction

During October 5-8, 2009, the Office of Security Enforcement, within the Office of Health, Safety and Security, conducted a program review of the classified information security programs at Babcock & Wilcox Technical Services Y-12, LLC (B&W Y-12). 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 evaluated B&W Y-12 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 B&W Y-12 internal deficiency tracking/trending systems; and correcting deficiencies to prevent recurrence. It also included a limited review of B&W Y-12 internal security assessment programs and an evaluation of B&W Y-12 efforts to integrate its security regulatory compliance program – as defined by Title 10 Code of Federal Regulations (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 (PAAA)" compliance program, which includes both nuclear safety and worker safety and health enforcement (hereinafter referred to as the enforcement program). Further, this review also evaluated the corrective actions taken by B&W Y-12 in response to the enforcement letter, dated July 10, 2009, issued to B&W Y-12 communicating the Office of Enforcement's concerns about the protection of classified information at the Y-12 National Security Complex.

At the time of this review, the B&W Y-12 PAAA program manager (hereinafter referred to as the enforcement coordinator) identified a number of ongoing improvement initiatives related to 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 B&W Y-12'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:

- The B&W Y-12 Safeguards, Security & Emergency Services (SS&ES) program has developed a good relationship and effective lines of communication with the B&W Y-12 enforcement program.

- B&W Y-12 SS&ES conducts thorough security incident inquiries and completes timely, well-documented inquiry reports.

- B&W Y-12 cyber security and Classified Matter Protection and Control (CMPC) organizations have a close and effective relationship with the B&W Y-12 security incident program regarding classified information/cyber security incidents.

- Personnel in the B&W Y-12 incidents of security concern program are well trained and knowledgeable of the program requirements and responsibilities, and appropriately include subject matter experts (SMEs) and the Y-12 Site Office (YSO), in the initial categorization of security incidents.

- The security-related trending data from the incidents of security concern program is used proactively in identifying targeted opportunities to conduct focus area reviews, as well as identifying adverse trends and instituting corrective actions to prevent further occurrences.

- Safeguards and security (S&S) noncompliances identified as a result of security incidents or external/internal assessments are included in the Safeguards and Security Tracking, Analysis and Reporting System (SSTARS), which ensures the evaluation, resolution, closure, reporting, and trending of all S&S-related issues.

- The B&W Y-12 internal assessment program, specifically the topical/subtopical self-assessments, appear effective in providing meaningful feedback on performance, quality, and compliance to workers and management, as well as identifying concerns at an early stage.

- The B&W Y-12 CMPC and cyber security program personnel are trained and knowledgeable of program responsibilities and requirements, as evidenced by the training provided on subtopical area requirements and assistance to the division security officers (DSOs) in performing internal assessments.

Weaknesses:

- The B&W Y-12 SS&ES and enforcement program's written processes and procedures (i.e., Y19-51-007, *S&S issues management program* and Y76-001, *PAAA compliance program*) are not reflective of current or anticipated practices with respect to 10 C.F.R. 824 implementation.

- The site descriptive criterion for risk and significance determination is not well defined for 10 C.F.R. Part 824 noncompliances.

- The current enforcement screening tool does not provide detailed security-related information for identifying sources (e.g., security incidents/events, internal/external assessments, investigations) for classified information security noncompliances.

- The process for identifying, tracking, and resolving issues identified during DSO self-assessments is not always documented in SSTARS and the established B&W Y-12 issue resolution process is not followed.

II. General Program Implementation

This review identified that the security enforcement function, as defined by 10 C.F.R. Part 824, is not formally described or fully integrated into the B&W Y-12 enforcement program. Initiatives are under way to formalize processes and procedures to address integration, as well as the enforcement screening of classified information security noncompliances. Although B&W Y-12 is in the initial stages of formally integrating security into its existing enforcement program, there is a close and in the review team's view, an effective working relationship among the enforcement program personnel and representatives of the SS&ES program.

The existing enforcement screening tool contains specific safety-related information identifying primary and secondary sources for noncompliances (i.e., nuclear safety and worker safety and health). However, this tool provides limited information regarding the identification of sources for classified information security noncompliances that require enforcement screening. The screening process does not identify noncompliances as defined in Departmental classified information security policy requirements. This practice limits enforcement program screening to incidents of security concern rather than addressing all classified information security noncompliances, including those identified as a result of an internal or external assessment. B&W Y-12 recognizes the need to update program implementation documents to reflect current processes and incorporate needed changes (i.e. noncompliance screening, etc.). Work has begun on drafting these revised procedures. Furthermore, B&W Y-12 is modifying SSTARS to include specific Departmental policy citation(s) for each identified noncompliance regardless of the source (e.g., security incidents/events, internal/external assessments, investigations).

Once identified, incidents are currently categorized and reported through the security incident program and resolved in accordance with DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management*. All inquiry reports are entered and maintained in SSIMS, and causal analyses and corrective actions are developed using a risk-based/significance determination approach and entered and tracked in SSTARS, which is part of the overall B&W Y-12 contractor assurance system. Security noncompliances may also be identified through the S&S assessment program, which consist of independent assessments, management assessments, topical/subtopical self-assessments, surveillances, and other internal evaluation activities. The performance assurance program also ensures that causal analysis is conducted using a risk-based and significance-determination approach and that associated corrective actions are entered and tracked in SSTARS.

The actions taken to address the concerns identified in the enforcement letter issued to B&W Y-12 in July 2009, were also evaluated during this review. Discussions with B&W Y-12 security personnel revealed that they had also identified, through security incident trending, similar concerns involving classified e-mails sent by unapproved methods. Although B&W Y-12 began addressing the e-mail concern before receiving the enforcement letter, it was stated that the enforcement letter reinforced the need and urgency to define and implement effective corrective actions. Also before receiving the enforcement letter, the B&W Y-12 information security manager and the security incident program manager used the 10 C.F.R. Part 824 Energy Facility Contractors Group (EFCOG) peer review checklist to perform an internal assessment of its security regulatory program. As a result of this internal assessment activity and the enforcement letter, B&W Y-12 implemented or accelerated the following actions:

- A gap analysis on the integrated security issues identification and reporting process was conducted, and the gaps were closed.
- General managers and senior leadership were briefed on the enforcement letter and e-mail concerns, and a task team was formed to find a solution to prevent recurrence. At the writing of this report, the task team continues to research an engineered solution that uses a keyword/key phrase filter to catch classified e-mails before they are transmitted outside the firewall.
- The security incident program manager was designated a core member of the Issues Management Board (IMB) to follow up on noncompliances that may be incidents of security concern identified by the internal assessment program.
- All Impact Measurement Index's (IMIs) are included in the issues management process, and causal analysis and corrective action planning are required for all IMI-1s, -2s, and -3s, as well as certain -4s. At the writing of this report, B&W Y-12 plans to have causal analyses documented in SSTARS, and corrective actions documented in both SSTARS and the Issues Management System. In addition, the responsible S&S functional manager will track corrective actions and validate closure.
- Trending analysis includes information on both incidents of security concern and other security-related events, as well as internal assessment results in SSTARS.
- Security incident information, as well as results from CMPC field assessment checklists (e.g., classified vault/vault-type room/repository field assessments and classified copier/shredder field assessments), is being entered into SSTARS.
- Security incident trending reports are being more widely distributed to senior managers.
- The enforcement program procedure was reviewed in conjunction with the security procedure to consider the need to formally define and document the integration of roles and responsibilities. Security incident procedures have been revised to document the security incident causal analysis and CMPC causal analysis requirements associated with incidents.
- Additional consequences that are required to prevent recurrence of noncompliances have been identified. B&W Y-12 worked with senior management and human resources to reinforce employee discipline for those who do not adhere to security requirements.

- Modification of Y15-312, *Site Issues Management Procedure*, to include the S&S issues management process.
- An issues management procedure, Y19-51-007, *Safeguards & Security Issues Management Program*, was developed for SS&ES, which includes both an issue resolution process and a 10 C.F.R. Part 824 screening process that aligns with the site issues management process as defined in, Y15-312, *Site Issues Management Procedure*.

Many of these corrective actions have had a positive impact on the integration of 10 C.F.R Part 824 into both the SS&ES program and the existing enforcement program. The corrective actions will improve the S&S issues management program and expand the use of SSTARS for tracking and trending security-related noncompliances.

Strength:

- The B&W Y-12 SS&ES program has developed a good relationship and effective lines of communication with the B&W Y-12 enforcement program.

Weakness:

- The B&W Y-12 SS&ES and enforcement program's written processes and procedures (i.e., Y19-51-007, *S&S issues management program* and Y76-001, *PAAA compliance program*) are not reflective of current or anticipated practices with respect to 10 C.F.R. 824 implementation.

III. Identification and Categorization of Security Noncompliances

At B&W Y-12 there are two primary sources of identification of reportable security incidents: the security incident program and the S&S self-assessment program. Both programs reside within SS&ES. This section of the report discusses the specific activities involving the identification and categorization of reportable security incidents. Activities specifically associated with the internal assessment program are addressed in section VI of this report.

B&W Y-12 procedure Y19-51-102, *Handling Incidents of Security Concern*, implements a consistent and uniform reporting process for all incidents of security concern. Discussions with the B&W Y-12 security incident program manager indicated that when an incident is suspected to have occurred, the facts and circumstances are examined and the IMI categorization is determined within the required 24-hour reporting period. If necessary, SMEs from other security disciplines (i.e., CMPC, physical security or cyber security), as well as YSO, are involved in the IMI categorization determination process.

The six incidents of security concern inquiry reports that were evaluated during this review revealed that the conduct and results of the inquiry were documented adequately. SSIMS inquiry reports are completed for IMI-1s, -2s, and -3s, and DOE Form 5639.3, *Report of Security Incident/Infraction*, is used to document IMI-4 inquiries. The reports were found to contain necessary time-related actions (i.e., incident discovery, notifications, and incident inquiry), data pertaining to the location and a complete discussion of the facts and circumstances surrounding the incident, such as identification of personnel involved, identification of direct and contributing causes, physical evidence, and results of interviews.

The personnel assigned to the B&W Y-12 security incident program are knowledgeable of their designated responsibilities and Y-12 operations. They also have appropriate security expertise, as well as requisite inquiry training and years of investigation experience. B&W Y-12 has embedded a cyber security SME within its security incident program to handle forensics and sanitization processes. B&W Y-12 has the ability to shut-down and suspend accounts, as well as sanitize systems remotely. This capability allows the cleanup process after an incident to be accomplished within eight hours. This rapid cleanup minimizes the potential risk of compromise of information and allows assignment of a lower IMI categorization.

Strengths:

- B&W Y-12 SS&ES conducts thorough security incident inquiries and completes timely, well-documented inquiry reports.
- The B&W Y-12 cyber security and CMPC organizations have a close and effective relationship with the B&W Y-12 security incident program regarding classified information/cyber security incidents.
- Personnel in the B&W Y-12 incidents of security concern program are well trained and knowledgeable of the program requirements and responsibilities, and appropriately include SMEs and YSO in the initial categorization of security incidents.

No specific weaknesses were identified under this section.

IV. Reporting

This review found that all security incidents categorized correctly as IMI-1, -2, or -3, as well as incidents involving foreign nationals, are documented on DOE Form 471.1, *Security Incident Notification Report,* and coordinated through YSO prior to transmission to DOE Headquarters via SSIMS. Data reporting includes: initial notification reports; incident inquiries; and infractions and incidents issue papers for all incidents of security concern (except for those categorized as IMI-4, which are entered in SSIMS). IMI-4 incidents are included in the monthly reporting of statistical counts as required by DOE Manual 470.4-1 Chg 1, *Safeguards and Security Program Planning and Management.*

No specific strengths or weaknesses were identified under this section.

V. Issues Management and Trending

The corrective actions resulting from the receipt of the enforcement letter and B&W Y-12's identification of the adverse trends associated with e-mails have led to a number of completed or ongoing improvement processes related to the S&S issues management program.

Currently, the issues management process applies to S&S issues derived from: external sources (such as surveys and inspections); incidents of security concern (IMI-1 through IMI-4); internal sources (such as independent assessments and management assessments); performance testing; and cyber security issues (both internally and externally identified). All new internal and external S&S issues are processed through the IMB, which is chartered by the Vice President, SS&ES, and serves as a mechanism for management to determine the significance of issues and assign issue owners who have the authority, responsibility, and resources for issue resolution. In addition, recommendations from the IMB for issues identified by external sources are provided to the company's Issues Management Prioritization and Risk Board (IMPRB) for final significance determination and issue assignment when external to SS&ES.

B&W Y-12 implements a site-level approach to risk management, which focuses on ensuring that associated risks are identified and controlled. Since all S&S-related issues are now being processed through the IMB or IMPRB, a risk and associated significance determination is defined for each identified issue. The risk grading quantifies risk by assessing the consequences, determining the probability of the consequences, and combining the two to identify a risk level: high (1-5), medium (6-10), low (11-15), and very low (16-20). The significance determination (level A through D) is based on the risk level (e.g., risk levels 1 through 5 equate to a significance level of A). However, neither the current risk probability criteria defined in the B&W Y-12 risk determination procedure (Y15-016) nor the criteria defined on the significance determination worksheet are clearly defined for S&S-related issues. For example, the only specific S&S criteria identified is the IMI categorization level for incidents of security concern. The lack of security specificity in the risk and significance criterion may make it difficult to make accurate risk management determinations.

B&W Y-12 has established an issue resolution process that is driven by the significance determination assigned by the IMB or IMPRB for each S&S-related issue. Discussions with B&W Y-12 security personnel indicated that issues from assessments, performance tests, and incidents of security concern are identified as a "lack of compliance and/or performance." As a result, B&W Y-12 has set expectations that S&S personnel will be assigned as a SME to advise the issue owners in the development and closure of the corrective action plan. Depending on the significance determination of the issue, an appropriate resolution path is taken. Significance level A and B issues (i.e., those with a higher level of security significance) are required to follow the corrective action plan path, which includes, as appropriate: a causal/root cause analysis; an extent–of-condition analysis; compensatory measures; development of lessons learned; a corrective action plan; enhancements; and issue closure summary. Issues identified as level C and D (i.e., those with a lower level of security significance) also follow a defined resolution path, but with fewer steps. For example, level C issues require a causal/root cause analysis and extent-of-condition analysis, but level D issues do not, unless the issue is a YSO deficiency or deemed necessary by management. SSTARS tracks progress and requires certain steps which are established by the significance determination to be completed before an issue is identified as closed.

B&W Y-12 is refining and implementing a process for enforcement screening of S&S issues. Enforcement screening is required for S&S issues from external and internal sources (i.e., assessments and performance tests), including incidents of security concern that are given a significance level of A or B. Issues given a lesser significance level (C or D) are subject to secondary screening for potential 10 C.F.R. Part 824 enforcement reporting. Responsibility for enforcement screening and coordination with the enforcement program office has been delegated to line management Price-Anderson officers (LMPOs), who are also responsible for implementing the enforcement program within their divisions. A LMPO for security screening has been designated. Screening is to occur within 15 days after the significance determination is made by the IMB or IMPRB. The Issues Management System is programmed to track, record screening dates, and provide status reports showing pending and completed enforcement screenings. In the near future, SSTARS will also have this capability to allow for detailed security-related screenings.

B&W Y-12 has recently instituted SSTARS, which is a software application that captures internal and external assessment issues, as well as incidents of security concern. SSTARS is accredited and approved for processing classified information and is designed to facilitate the evaluation, resolution, closure, reporting, and trending of all S&S-related issues. This system has been in operation since April 2009 and currently contains 222 records. Prior to the implementation of SSTARS, B&W Y-12 had a number of different systems that were independently used for reporting and tracking S&S issues. Because issue data was not easily retrievable, trending of identified issues had not been generally effective. An exception was the incidents of security concern program, which had a separate database that provided detailed trending information pertaining to reported incidents of security concern. In addition to the monthly metrics provided to the B&W Y-12 senior management team for trending, the security incident program also provided quarterly formal trending and analysis reports and used the trending data to identify specific areas of concern and completed assessments of those areas. A review of recently developed focus area reports found them to contain valuable information to be able to address specific security concerns.

With the implementation of SSTARS, B&W Y-12 can provide advanced trending and analysis for S&S-related issues. B&W Y-12 security personnel indicated that performance analysis and trending are important in identifying systemic/programmatic issues involving the protection of classified information and in identifying potential issues before they become significant events. The B&W Y-12 draft procedure for the

S&S issues management program indicates that performance analysis and trending will be completed on a quarterly basis using the data in SSTARS. In addition, the IMB and the S&S functional areas will use SSTARS to verify ongoing performance and identify recurring issues in a topical/subtopical area or by the responsible organization. The performance analysis and trending activities will also support the screening and reporting of issues for applicability to 10 C.F.R. Part 824. If any trending issues are determined applicable under 10 C.F.R. Part 824, they will also be entered into SSIMS with corrective actions.

Strengths:

- The security-related trending data from the incidents of security concern program is used proactively in identifying targeted opportunities to conduct focus area reviews, as well as identifying adverse trends and instituting corrective actions to prevent further occurrences.

- S&S noncompliances identified as a result of security incidents or external/internal assessments are included in the SSTARS, which ensures the evaluation, resolution, closure, reporting, and trending of all S&S-related issues.

Weaknesses:

- The site descriptive criterion for risk and significance determination is not well defined for 10 C.F.R. Part 824 noncompliances.

- The current enforcement screening tool does not provide detailed security-related information for identifying sources (e.g., security incidents/events, internal/external assessments, investigations) for classified information security noncompliances.

VI. Assessments

The B&W Y-12 SS&ES assessment program is documented in Y19-51-002, *Safeguards and Security Assessment Program*. The purpose of this program is to ensure internal monitoring of compliance and performance with S&S contractual requirements. The SS&ES assessment program consists of four general assessment categories: 1) external oversight; 2) independent assessments; 3) management assessments; and 4) topical/subtopical self-assessments, surveillances, performance testing, and other activities. Only the fourth tier (i.e., topical/subtopical assessments, surveillances) was addressed during this review.

Along with management assessments, the topical/subtopical self-assessments are the foundation of the SS&ES assessment program; they are conducted by SMEs most familiar with the work and therefore have the greatest effect on performance, quality, and compliance. The subtopical area assessors (CMPC and cyber security) are provided assessment training, which was developed by B&W Y-12. The B&W Y-12 CMPC and cyber security personnel are knowledgeable of their subtopical areas and the roles and responsibilities associated with conducting assessments. In fact, SS&ES SMEs provide training to division personnel and are directly involved in SS&ES program improvement initiatives.

B&W Y-12 SS&ES topical area managers, functional area department managers, and the assessment program manager review prior assessment results and issues when planning and scheduling future assessment activities, with specific emphasis on areas where prior issues are noted. The topical area manager determines the self-assessment frequency, but ensures that each topical area is reviewed at least annually. These assessments are performed more frequently than others, not only to provide workers and managers with feedback, but also to identify problems at an early stage. With the implementation of SSTARS, assessors can obtain data on trends to determine the performance level of programs and organizations. In addition, because previously identified issues are maintained in SSTARS, the scope of assessments includes an effectiveness review of implemented corrective actions. The results from topical/subtopical assessments, as well as other assessment activities (e.g., surveillances, performance tests, walk-downs) conducted through the fiscal year are consolidated in an annual assessment report. All S&S issues identified during these assessment activities are reviewed by the IMB and/or the IMPRB and go through the issues management process as previously described in section V above.

In addition to the CMPC subtopical assessments conducted by SMEs, the DSOs are responsible for performing an annual CMPC self-assessment in accordance with the checklists provided by the B&W Y-12 CMPC program. A DSO represents a division or organizational manager/director concerning Y-12 CMPC program issues and is not typically a CMPC SME. The DSO self-assessments were found to be checklist–based and limited in scope, which consequently does not provide a comprehensive compliance and performance based review, unlike the subtopical area assessments conducted by the SMEs. In addition, noncompliances identified as a result of a DSO self-assessment are not always entered into SSTARS or any other formalized tracking system. According to the B&W Y-12 CMPC program manager, a new self-assessment approach is being undertaken for fiscal year 2010 whereby the CMPC program personnel will conduct subtopical area self-assessments and surveillances for half of the B&W Y-12 organizations, and the DSOs (shadowed by CMPC personnel) will conduct self-assessments for the remaining half. While proactive measures are being taken to ensure effective and consistent evaluations (providing comprehensive checklists, shadowing DSOs to ensure that they use appropriate evaluation methods, etc.), the DSO self-assessment results are not handled with the same level of detail and rigor as other assessments (i.e., self-assessments and surveillance for those B&W Y-12 organizations being assessed by CMPC program personnel). In addition, because the identified deficiencies are not entered in SSTARS and the established issue resolution process is not followed, the effectiveness of the DSO assessments to ensure adequate causal analysis, extent of condition, corrective action plan, and closure verification is limited. Since half of the CMPC self-assessment activities scheduled for fiscal year 2010 will rely on the DSO self-assessment process, a common approach to conducting these assessments would ensure that security interests and activities are protected at the required levels, and that documented results would provide a comprehensive compliance and performance based evaluation of the CMPC program.

Strengths:

- The B&W Y-12 internal assessment program, specifically the topical/subtopical self-assessments, appear effective in providing meaningful feedback on performance, quality, and compliance to workers and management, as well as identifying concerns at an early stage.

- The B&W Y-12 CMPC and cyber security program personnel are trained and knowledgeable of program responsibilities and requirements, as evidenced by the training provided on subtopical area requirements and assistance to DSOs in performing internal assessments.

Weakness:

- The process for identifying, tracking, and resolving issues identified during DSO self-assessments is not always documented in SSTARS and the established B&W Y-12 issue resolution process is not followed.

VII. Ongoing Initiatives

At the time of this review, B&W Y-12 SS&ES and the enforcement program personnel were in the initial stages of evaluating how to effectively integrate the 10 C.F.R. Part 824 regulatory requirements into the existing safety enforcement program. With the recent implementation of SSTARS and the intent to improve the existing enforcement screening process for classified information security issues, B&W Y-12 should be successful in integrating security regulatory activities in a manner consistent with the guidance provided in the EPO document, as well as the requirements of 10 C.F.R. Part 824.

VIII. Conclusions

Although B&W Y-12 is in the initial stages of integrating security activities and 10 C.F.R. Part 824 requirements into its existing safety enforcement program, the B&W Y-12 enforcement coordinator and staff have developed a good working relationship with the B&W Y-12 security organization and have been given access to security incident data and trending results. However, the roles and responsibilities of the enforcement coordinator, as they relate to security enforcement, have not been formally defined and documented. In addition, it is imperative that the descriptive criterion for risk and significance determination be more clearly defined for 10 C.F.R. Part 824 noncompliances. If the risk and significance criterion is not corrected, the level of rigor applied in addressing noncompliant conditions may be less effective and may result in recurrent issues.

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, inquiry, causal analysis, and corrective action processes for security incidents. The implementation of SSTARS for tracking all security-related issues should improve the oversight of identified program security weaknesses and the effectiveness of implemented corrective actions to prevent the likelihood of recurrence. Overall, the Office of Security Enforcement is encouraged by the direction B&W Y-12 is headed, not only with respect to the integration of security into the existing safety enforcement program, but also with the level of rigor applied to the identification and correction of security noncompliances and the planned enhancements for tracking and trending those noncompliances in SSTARS. Management's continued attention and commitment to the security program are crucial to the successful integration of security into the B&W Y-12 enforcement program, specifically the planned enhancements of SSTARS for tracking, trending, and enforcement screening of all S&S-related issues.

By addressing the weaknesses identified during this review, B&W Y-12 can facilitate the Office of Security Enforcement's exercise of discretion for noncompliant conditions that are of lower significance; 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 YSO and the Chief Defense Nuclear Security (NA-70).