Department of Energy
Washington, DC 20585

August 7, 2009

Mr. Greg Meyer
President and General Manager
Babcock & Wilcox Technical Services Pantex, LLC
P.O. Box 30020
Amarillo, Texas 79120

Dear Mr. Meyer:

The Office of Health, Safety and Security's Office of Security Enforcement conducted an onsite program review from March 24 – 26, 2009, of the classified information security program elements that support the Babcock & Wilcox Technical Services Pantex, LLC (B&W Pantex) regulatory compliance program. Our review included: an evaluation of B&W Pantex processes for identifying classified information security noncompliances; reporting and tracking classified information security noncompliances in the Safeguards and Security Information Management System; B&W Pantex internal tracking systems; and correcting deficiencies to prevent recurrence. The Office of Security Enforcement also conducted a limited review of B&W Pantex management and Safeguards and Security self-assessment programs.

Although B&W Pantex 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 its 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 B&W Pantex's 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. Recognize that 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 B&W Pantex. 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,

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

Enclosure

cc: Kathy Brack, B&W Pantex

OFFICE OF SECURITY ENFORCEMENT
PROGRAM REVIEW
BABCOCK & WILCOX TECHNICAL SERVICES PANTEX, LLC

I. Introduction

During March 24-26, 2009, the Office of Security Enforcement, within the Office of Health, Safety and Security, conducted a program review (PR) of the classified information security programs at Babcock & Wilcox Technical Services Pantex, LLC (B&W Pantex). The program review was conducted in a manner consistent with the guidance provided in the *DOE Enforcement Process Overview* (EPO), dated June 2007. Subsequent to the conduct of the B&W Pantex PR, the EPO was revised in June 2009 and 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 B&W Pantex processes for identifying classified information security noncompliances; reporting and tracking classified information security noncompliances in the Safeguards and Security Information Management System (SSIMS); use of B&W Pantex internal deficiency tracking/trending systems; and correcting deficiencies to prevent recurrence. It also included a limited review of B&W Pantex management and safeguards and security (S&S) self-assessment programs and an evaluation of B&W Pantex efforts to integrate its security enforcement (Title 10 Code of Federal Regulations (C.F.R.) Part 824) program with its existing Price-Anderson Amendments Act (PAAA) program, which includes both nuclear safety and worker safety and health enforcement (hereinafter referred to as the enforcement program).

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

<u>Strengths:</u>

- B&W Pantex exhibits a strong "self-reporting" culture.

- Causal analysis activities that support the enforcement and incidents of security concern programs are well defined and contain a structured process to ensure that appropriate actions are taken in a timely manner to minimize the potential for recurrence.

- Management attention and commitment to the overall security program are evident, as exemplified by the funding of a security position in the B&W Pantex enforcement program; weekly reviews of newly identified security incidents; monthly reviews of security incident trends; and an effective partnership between the contractor and the Pantex Site Office (PXSO).

- Identified issues/deficiencies are managed through the B&W Pantex Problem Evaluation Request System (PERS) and Electronic Suspense Tracking and Routing System (ESTARS), which are used for the reporting, documenting, tracking, correcting, and trending of identified issues/deficiencies.

- The available security-related trending data is used effectively to identify security awareness topics, and timely security messages are delivered to the workforce through the use of interactive and innovative methods.

- The security incident program personnel were knowledgeable of the program requirements and responsibilities, and when necessary included subject matter experts as well as PXSO in the initial categorization of security incidents.

Weaknesses:

- Some security incidents were miscategorized as an "IMI-5" or "near miss" which reveals the correct categorization may not be assigned in all cases.

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

- There is insufficient communication and interface between the self-assessment program and the other security functional areas (i.e., security incident program), which could result in missed opportunities to identify underlying programmatic security weaknesses.

II. General Program Implementation

In early October 2008, a management change in the B&W Pantex safeguards and security (S&S) division resulted in increased S&S involvement and integration with the B&W Pantex existing administrative programs, including the enforcement program. The new S&S management team has extensive nuclear safety experience and thus is familiar with the PAAA enforcement program function and elements. A B&W Pantex management assessment was initiated in October 2008 to determine if B&W Pantex had any gaps in the implementation of its enforcement program, to include 10 C.F.R. Part 824, as identified in the Office of Enforcement's EPO document. This analysis involved representatives from the following B&W Pantex functional areas: PAAA enforcement; integrated safety management; performance assurance; and personnel security programs.

Between October 24, 2008, and January 23, 2009, the B&W Pantex management assessment identified the integration of the security incident program into the B&W Pantex enforcement process as an area that needed improvement. Specifically, this B&W Pantex management assessment determined; "While the B&W Pantex process for reporting security incidents meets DOE requirements, it is not consistent with the DOE Office of Enforcement's expectations, as communicated in recent Office of Enforcement integrated program reviews and the EPO document". B&W Pantex identified the following three areas for improvement:

1. S&S self-assessment results are not included in the B&W Pantex noncompliance reporting process. For example, the results of S&S assessments are not routinely evaluated for reporting under 10 C.F.R. Part 824; actions taken in response to S&S assessments are not tracked in a designated system that specifically identifies issues as regulatory noncompliances; metrics provided to senior managers do not include S&S assessment results; and the S&S corrective action process does not include an independent validation to ensure effectiveness.

2. Some aspects of the S&S reporting process have not been formalized in procedures. For example, procedures do not specifically address trending of security incidents or the methodology for evaluating potential repetitive or programmatic security noncompliances, and the role of the PAAA coordinator in security incident reporting is not formally defined or documented.

3. B&W Pantex does not monitor or trend SSIMS reports for the ratio of self-identified to event-driven items as a performance metric.

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 overall B&W Pantex enforcement program. However, as a result of B&W Pantex's extensive planning and analysis, as discussed above, an integration plan was developed in collaboration with PXSO and implementation is expected by July 2009. The integration plan proposed adding a security position within the B&W Pantex enforcement program to ensure the appropriate categorization, evaluation, and resolution of reportable security incidents. Once this position is filled, the assigned individual will facilitate integration of other S&S program elements associated with security incidents, such as program management, the performance assurance program, security education/awareness, causal/root cause analysis, and corrective action management. In addition, the interface of these S&S elements will be formally defined in the B&W Pantex enforcement program documentation.

This review also found that security incidents have been discussed on a monthly basis with the B&W Pantex enforcement coordinator since 2007; however, security related issues resulting from self-assessments, performance testing, etc., have not been communicated until recently. Beginning in 2009, the B&W Pantex S&S division implemented processes to ensure that all 10 C.F.R. Part 824 reportable security issues are brought to the attention of the B&W Pantex enforcement coordinator. In addition, B&W Pantex management reviews all newly identified security program issues on a weekly basis.

Currently, incidents reported through the security incident program are categorized 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 graded approach and entered and tracked in the B&W Pantex PER/ESTAR systems, which are part of the overall B&W Pantex performance assurance program. In addition, the performance assurance program may also identify reportable security issues through self-assessments, performance testing, and other evaluation activities. The performance assurance program also ensures that causal analysis is conducted using a graded approach and that associated corrective actions are tracked.

Although self-assessment results, causal analysis, and corrective actions are entered and tracked in ESTARS, security issues identified through self-assessments, performance testing, etc., are not entered into PERS and therefore, are not included in the B&W Pantex noncompliance reporting process. Once the B&W Pantex enforcement program fully incorporates the 10 C.F.R. Part 824 requirements, the PER system will be enhanced to include all 10 C.F.R. Part 824 related issues. B&W Pantex stated that the PER system will not include security related issues identified through self-assessments, performance testing, etc., that occurred before the enhanced PER system is implemented. However, such historical data can be valuable in determining whether the security programs designed to protect classified information are effective, improving, or in need of attention. Currently, B&W Pantex plans to continue the current practices for trend analysis while establishing a baseline of determinations for evaluating noncompliances.

Strength:

- Management attention and commitment to the overall security program are evident, as exemplified by the funding of a security position to support the B&W Pantex enforcement program; weekly reviews of newly identified security incidents; monthly reviews of security incident trends; and an effective partnership between the contractor and the PXSO.

No specific weaknesses were identified under this section.

III. Identification and Categorization of Security Noncompliances

At B&W Pantex there are two primary sources of identification of reportable security incidents: the security incident program and the performance assurance program. Both programs reside within the S&S division. This section of the report discusses the specific activities involving the identification and categorization of reportable security incidents. Activities specifically associated with the performance assurance program are addressed in section VI of this report.

B&W Pantex procedure 02.02.04.09, *Process for Incidents of Security Concern* (Issue No. 2), addresses two principal functions: discovery and notification of incidents of security concern, and conduct of inquiries. 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, B&W Pantex desk aid 0393, *Incidents of Security Concern*, provides detailed instructions regarding the identification, categorization, and reporting of reportable security incidents. However, this desk aid references the use of the former incident tracking and analysis capability system versus the current system, SSIMS, for reporting incidents.

When Pantex personnel discover unsecured/unattended classified matter (including classified computer systems), the procedure directs them to immediately notify their supervisor, the operations center (OC), the cyber security and information security organizations, and/or a representative of the protective force. If the OC receives a report of such an event, the OC notifies either the cyber security or the information security organization concerning the circumstances and provides available details. Protective force personnel may be notified of unsecured/unattended classified matter, or may discover it during routine security patrols. In all cases, a cyber security or information security inquiry official (IO) is notified, and the classified matter at risk is attended by appropriately cleared personnel until it is released to the IO.

The IO initiates the preliminary inquiry by identifying the individual(s) involved, determining whether any classified matter is missing or unprotected, and ensuring that all classified matter associated with the incident is appropriately secured. The IO then categorizes the incident in accordance with DOE directives, using the current incident management index (IMI) tables. Interviews conducted during this PR with security incident program personnel revealed that subject matter experts from other departments assist in categorizing security incidents. This process was confirmed during interviews with cyber security and classified matter protection and control personnel. Once categorization is complete, the IO submits the requisite security incident notification to DOE Headquarters via SSIMS. As required, all completed inquiries and supporting information are documented and entered into SSIMS.

Discussions with personnel assigned to the security incident program revealed that they are extremely knowledgeable of their designated responsibilities and Pantex operations. They also have appropriate security expertise; one individual has over 30 years of physical protection experience, and another has over 5 years of information/cyber security experience. In addition, a third individual assigned to the cyber security department is authorized as an inquiry official and has over 12 years of experience in investigations and cyber security. However, clear lines of communication or interface between the security incident program and the B&W Pantex self-assessment program appear to be lacking. Personnel from both programs acknowledged that significant security incidents resulting in a high likelihood of risk to classified matter would be communicated, but it was not clear whether lower-level, less obvious issues identified through self-assessments or trending are shared effectively with other functional areas within the security organization.

The latest security incident data contained in SSIMS showed inconsistencies between the number of incidents reported in SSIMS and the number of incidents identified by B&W Pantex. The list of security incidents provided by B&W Pantex as part of the document request for this review was found to contain more incidents because it includes “IMI-5” incidents, a category developed by B&W Pantex to identify near misses. The Office of Security Enforcement reviewed 10 security incident report files, most of which were “IMI-5” cases (a few were identified as IMI-4). This review determined that some security incidents identified as “IMI-5” (near miss) should have been reported in SSIMS as IMI-4, and one IMI-4 security incident should have been categorized at a higher IMI level.

Although the IMI tables were designed for broad interpretation, it is important to ensure that the most accurate categorization is applied, based on the available information. Security incident categorizations at Pantex are based on information that is familiar and recognizable by B&W Pantex personnel, and thus the full details of the categorization decision are not always well documented in the security incident records. Consequently, individuals who are not familiar with Pantex operations and facilities cannot readily determine the accuracy of categorization of security incidents. For example, the records may simply identify the facility where a security incident occurred; leaving it to the reader to discover that the facility has multiple layers of physical security features and strict access controls. Individuals who are familiar with Pantex facilities would be aware of these important details, but others would need more information to determine whether the classified matter involved in the incident was at risk.

Strength:

- The security incident program personnel were knowledgeable of the program requirements and responsibilities, and when necessary included subject matter experts as well as PXSO in the initial categorization of security incidents.

Weaknesses:

- There is insufficient communication and interface between the self-assessment program and the other security functional areas (i.e., security incident program), which could result in missed opportunities to identify underlying programmatic security weaknesses.

- Some security incidents were miscategorized as an “IMI-5” or “near miss” which reveals the correct categorization may not be assigned in all cases.

IV. Reporting

Based on the significant level of trust between management and employees, it is evident that B&W Pantex has a strong and viable “self-reporting” culture. The security education/security awareness program supports this culture by communicating identified security concerns to the entire Pantex plant population in a timely and professional manner. As a result, personnel are aware of the important security issues and when/how to report occurrences when observed.

Strengths:

- B&W Pantex exhibits a strong “self-reporting” culture.
- The available security-related trending data is used effectively to identify security awareness topics, and timely security messages are delivered to the workforce through the use of interactive and innovative methods.

No specific weaknesses were identified under this section.

V. Issues Management and Trending

Once security incidents are identified and categorized by B&W Pantex, a notification report is issued, an inquiry is conducted to determine the circumstances surrounding the incident, the extent of condition and the risk to classified matter are determined, and the resolution of the incident to prevent recurrence is implemented. As noted in section III, the ten final inquiry reports that were reviewed were found to have been evaluated thoroughly and to contain appropriate (but not always sufficiently detailed) documentation. Written statements by those involved were structured and succinct, and contained relevant information. All areas of concern were evaluated with an equal level of rigor, and all areas of the inquiry process were present. Overall, the inquiry reports were reasonably well documented and contained all report elements required by Departmental policies.

One of the most significant strengths of the B&W Pantex security program is the emphasis on managing identified incidents/deficiencies, and maximizing the lessons learned to prevent recurrence. The Office of Security Enforcement reviewed several key documents associated with issues management and trending during this review: desk aid 0325, *Guidelines for Conducting Extent of Condition Reviews*; desk aid 0461, *Causal Analysis Graded Approach*; work instruction procedure 02.03.14.04.06, *How to Develop Safeguards and Security Corrective Actions*; work instruction procedure 02.03.14.04.11, *How to Manage Closure of S&S Corrective Actions*; and work instruction procedure 02.03.04.01.01, *Performing Causal Analysis and Developing Corrective Action Plans*. The review team was also briefed on the high reliability operations (HRO) program and how it is being incorporated into the causal analysis process to ensure continuous program improvements.

The causal analysis program at B&W Pantex is extremely robust and, based on the information gathered during this review, highly effective. Causal analysis is applied using a graded approach and conducted by trained facilitators. The selected analysis methodology depends on the type of problem that is identified. For example, for less-significant deficiencies, a less rigorous model is used (i.e., the phoenix model or apparent cause analysis). More significant problems or deficiencies may require more strenuous methodologies, such as barrier analysis or causal factor analysis. In some cases, a problem or deficiency may be extensively analyzed, regardless of its significance, because of the amount of information that is expected to be derived by determining its most fundamental cause (including contributing and direct causes). These cases are known as "information-rich" incidents and are analyzed with an exceptional level of rigor due to the level of potential insight.

Regardless of the source of identified issues, (reportable enforcement occurrences, security incidents, etc.) all discrepancies requiring corrective actions are captured and posted on PER/ESTARS. As noted in section II, the PER system presently does not include current or past security issues identified as a result of self-assessments, performance testing, etc., and will not, until security activities are fully incorporated into the B&W Pantex enforcement program. However, causal analysis and corrective actions are being tracked through ESTARS, which readily provides necessary information to B&W Pantex management and other organizations responsible for correcting the identified deficiency.

Once 10 C.F.R. Part 824 is fully integrated with the B&W Pantex enforcement program, all identified issues, including security issues, will have a PER report generated to track and document completion of planned actions to establish compliance. According to the expected process, the initiator of the PER gathers information about the issue and completes the appropriate data fields, including the individual responsible for correcting the deficiency. Once the initiator submits the PER, the division point of contact (DPOC) receives an ESTARS task to verify and validate the issue, the responsible individual, and the assigned division. Upon verification of the issue by the DPOC, the responsible individual receives an ESTARS task, determines whether a full causal analysis is required, and then completes all the appropriate data entry fields for the PER.
Before the causal analysis is initiated, an ESTARS task is sent for an enforcement screening. (Currently, security-related issues are annotated as "not applicable" for the enforcement screening. Once security activities are integrated into the enforcement program, an enforcement screening will be required.)

To continue the expected process, upon completion of the causal analysis, the responsible individual receives an ESTARS task for review of the causal analysis and corrective action plan. If corrective actions are required, the responsible individual initiates ESTARS corrective action tasks. Corrective action assignees receive an ESTARS task and complete the assigned actions. Once corrective actions are completed, an ESTARS task is sent for review of corrective action closure documentation and verification of accuracy and completeness. This process is completed for each action identified within a corrective action plan. When all corrective actions are completed, issues management personnel perform a final quality review of the PER that addresses the completeness of the causal analysis documentation and closure of each corrective action.

Currently, the B&W Pantex enforcement program independently validates the completion and effectiveness of nuclear safety and worker safety and health corrective action plans. Under this process, the enforcement program has no responsibility for validating the completion or effectiveness of corrective actions resulting from security incidents, internal assessments, or external audits/inspections. When corrective action plans are developed in response to a security incident, the security incident program is responsible for reviewing the plan for completeness and providing concurrence. Once the corrective action plan is approved, it is the responsibility of the assigned department or division to monitor and complete the actions, and to close the actions when they believe they are complete. Neither the security incident program nor the performance assurance program is required to provide independent validation of corrective actions to ensure completion and effectiveness to prevent recurrence. B&W Pantex has identified this issue and will address it appropriately as part of the upcoming integration of security activities into the enforcement program as discussed in section II.

Strengths:

- Causal analysis activities that support the enforcement and incidents of security concern programs are well defined and contain a structured process to ensure that appropriate actions are taken in a timely manner to minimize the potential for recurrence.

- Identified issues/deficiencies are managed through the B&W Pantex PER/ESTARS automated systems, which are used for the reporting, documenting, , tracking, correcting and trending of identified issues/deficiencies.

Weakness:

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

VI. Assessments

The B&W Pantex performance assurance program is documented in two B&W Pantex work instructions. The first instruction, 02.03.14.04.03, *How to Develop Safeguards and Security Annual Assessment and Performance Assurance Program Plans*, defines procedures for developing the S&S annual assessment and performance assurance program plans for approval by the National Nuclear Security Administration (NNSA) Pantex Site Office. The second instruction, 02.03.14.04.04, *Conduct Safeguards and Security Assessments, Performance Assurance Tests, and Internal Review and Assessments*, defines the procedure for conducting a security assessment, performance assurance test, and internal review and assessment.

The performance assurance program is intended to assure that all topical and subtopical areas are incorporated into the S&S annual assessment and performance assurance plans as outlined in DOE Form 470.8. B&W Pantex department/section managers are provided the previous year's security assessment (SA), performance assurance test (PAT), and internal review and assessment survey (IRAS) schedule for review and revision. The performance assurance program staff, in conjunction with the department/section managers, determines the scope of the assessments by using the B&W Pantex risk assessment analysis table to determine the comprehensiveness of individual SAs, PATs, and IRASs.

The security enforcement team reviewed the B&W Pantex report entitled *Performance Assurance/Assessments FY-2008 Results Roll-Up*. This report consists of a brief narrative followed by a series of tables that identifies each topical and subtopical area assessment conducted, and the findings resulting from those assessments. The report shows that 15 findings in fiscal year (FY) 2008 were related to the protection of classified matter.

The Office of Independent Oversight's February 2008 inspection of the B&W Pantex S&S program identified a finding concerning the self-assessment program. Specifically, the inspection found that the internal assessment program does not meet DOE expectations for format, content, and reporting. This finding was still open at the time of this review. B&W Pantex has a corrective action plan in place and is in the process of modifying the performance assurance/assessment program approach to address this deficiency.

No specific strengths or weaknesses were identified under this section.

VII. Ongoing Initiatives

B&W Pantex is still evaluating how to integrate the 10 C.F.R. Part 824 regulatory requirements into its existing enforcement program most effectively. However, B&W Pantex plans to hire an additional individual to serve as the security representative to the B&W Pantex enforcement program. The security representative will ensure the monitoring of security incidents, as well as noncompliances identified through the security performance assurance program. With the dedicated security representative in place and the application of the monitoring capabilities of PER/ESTARS, B&W Pantex should be able to successfully complete the integration of security activities into its existing enforcement program. This approach is consistent with the Office of Enforcement's expectations, as defined in the EPO document, and the requirements of 10 C.F.R. Part 824.

The recent introduction of the HRO philosophy to improve quality performance efforts and identify security performance indicators may be able to minimize the number and impact of reportable security incidents. This system approach may also significantly reduce the risk of a major security event at the Pantex plant.

VIII. Conclusions

B&W Pantex is in the initial stages of integrating security activities and 10 C.F.R. Part 824 requirements into its existing enforcement program. The B&W Pantex enforcement coordinator has access to security incident data and trending results listed in PER/ESTARS, and regularly scheduled meetings are being held with B&W Pantex S&S management to discuss the data. However, the roles and responsibilities of the enforcement coordinator, as they relate to security enforcement, have not 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 B&W Pantex enforcement program, specifically the plan to hire a security professional to support the B&W Pantex 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 subject matter experts in the categorization, inquiry, causal analysis, and corrective actions processes for security incidents. The future implementation of PER/ESTARS for tracking all security-related issues should improve the existing oversight of identified program security 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. The ongoing integration of security into the B&W Pantex enforcement program should alleviate the current lack of communication/interface between the self-assessment program and the other security functional areas (i.e., security incident program).

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