



Department of Energy
Washington, DC 20585

July 2, 2012

Mr. Damon Detillion
Program Manager
Wastren-EnergX Mission Support, LLC
P.O. Box 307
Piketon, Ohio 45661

Dear Mr. Detillion:

The Office of Health, Safety and Security's Office of Security Enforcement conducted an onsite Regulatory Assistance Review of the classified information security program elements that support the Wastren EnergX Mission Support, LLC (WEMS) regulatory compliance program during the period March 13-15, 2012. Our review included an evaluation of WEMS processes for identifying, reporting and tracking classified information security noncompliances; WEMS internal tracking systems; and processes for correcting deficiencies to prevent recurrence. The Office of Security Enforcement also conducted a limited review of WEMS management and safeguards and security self-assessment programs.

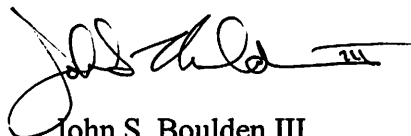
Although WEMS has not yet completed the process of fully integrating classified information security activities and 10 C.F.R. Part 824 into its existing regulatory compliance program, the Office of Security Enforcement is encouraged by the direction proposed by WEMS senior management related to implementation of its classified information security regulatory compliance program. This review, described in the enclosed report, identifies strengths, as well as recommendations for improving WEMS' security regulatory compliance program.

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



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

Sincerely,

A handwritten signature in black ink, appearing to read "John S. Boulden III". The signature is fluid and cursive, with a horizontal line extending to the right.

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

Enclosure: Regulatory Assistance Review Report

cc: Larry Kelly, OR
Rick Coriell, WEMS
Dan Longpre, WEMS

**OFFICE OF SECURITY ENFORCEMENT
REGULATORY ASSISTANCE REVIEW
WASTREN-ENERGX MISSION SUPPORT, LLC**

I. Introduction

During March 13-15, 2012, the Office of Security Enforcement, within the Office of Health, Safety and Security, conducted a regulatory assistance review of the classified information security program managed by Wastren-EnergX Mission Support, LLC (WEMS), located at the Portsmouth Gaseous Diffusion Plant (PORTS) in Piketon, Ohio. The review was conducted in a manner consistent with the guidance provided in the U.S. Department of Energy (DOE) *Enforcement Process Overview* (EPO), dated June 2009. The EPO document is located on the Office of Health, Safety and Security website at: http://www.hss.doe.gov/enforce/docs/overview/Final_EPO_June_2009_v4.pdf

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

On March 28, 2011, the United States Enrichment Corporation relinquished responsibility for site security at PORTS to DOE. WEMS was designated by DOE as the cognizant contractor security organization, effective April 2011, while Fluor, Babcock & Wilcox Portsmouth (FBP) remained responsible for protective force operations at PORTS. Both WEMS and FBP are prime contractors to DOE. As a result of this contractual structure, there have been coordination issues between the two contractors involving certain security responsibilities. To address this concern, the WEMS security manager has implemented a written protocol, approved by the DOE contracting officer representative, to formally define security roles and responsibilities. This protocol has been supported by the Portsmouth/Paducah Project Office (PPPO) line management.

At the time of this review, WEMS was in the process of fully developing its regulatory compliance program for classified information security. Most of the existing program documentation addresses the requirements of 10 C.F.R. Part 824; however, several security and regulatory procedures require updates to include these requirements. The WEMS regulatory compliance program coordinator (hereinafter referred to as the enforcement coordinator) has years of safety regulatory compliance experience, but has

only recently been assigned to integrate the security organization's regulatory compliance efforts into WEMS's existing regulatory compliance program.

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

Strengths

- There appears to be effective informal lines of communication between the WEMS Security Organization (WEMS Security), the WEMS enforcement coordinator, and PPPO.
- The WEMS enforcement coordinator has many years of safety regulatory compliance experience that should aid in the successful integration of 10 C.F.R. Part 824 regulatory requirements into WEMS regulatory compliance program.
- Management attention and commitment to the overall security program are evident, as exemplified, in part, by their development and participation in the Senior Review Board (SRB).
- Classified documents and matter appear to be adequately protected and controlled, consistent with DOE policies.
- WEMS has implemented stringent and conservative administrative controls designed to limit access to classified information, which further reduces the opportunity for noncompliances.
- WEMS personnel with information security responsibilities are trained and knowledgeable of their program responsibilities.
- WEMS has a well-established security awareness program that includes 10 C.F.R. Part 824 requirements in its initial and annual security briefings.
- WEMS uses a multi-disciplinary team approach to ensure the accuracy of initial categorization of security incidents, including consultation with the DOE Oak Ridge Office (DOE-OR) and PPPO, as appropriate.
- WEMS incidents of security concern (IOSC) program personnel are proactive in responding to security incidents, knowledgeable of program requirements, and have years of investigative experience.
- The IOSC program conducts thorough security incident inquiries and produces timely inquiry reports that are well written and can be easily understood by third-party readers.

- Cyber security and other subject matter experts (SMEs) are integrated into the IOSC program and are utilized as appropriate.
- Security noncompliances identified as a result of external/internal assessments are maintained in the WEMS Commitment Tracking System (CTS), which is a centralized database designed to ensure the effective management of noncompliances.
- WEMS has a causal analysis guidance procedure in place and requires training for all personnel responsible for conducting causal analysis.
- WEMS management recognizes the overall importance of having a viable self-assessment program and the ability to self-identify noncompliant conditions.
- A formal process is in place to provide timely notification to the appropriate manager and other designated personnel when noncompliances are identified during assessment activities.
- Personnel performing self-assessments are trained and possess subject matter expertise in the areas they are assessing.

Recommendations

- Ensure that applicable requirements identified in 10 C.F.R. Part 824 are formally documented in all of the WEMS local classified matter protection and control (CMPC), IOSC, and classified cyber security program training and procedures.
- Define and formally document the regulatory compliance program structure as it relates to the protection and control of classified information including: lines of authority and communication; integration of 10 C.F.R. Part 824 into the existing WEMS regulatory compliance and WEMS Security programs; and associated roles and responsibilities.
- Develop a formal regulatory screening process that takes into consideration all of the available information that addresses WEMS performance related to the protection and control of classified information. To better facilitate this process, the enforcement coordinator should receive all available information that addresses WEMS performance related to the protection and control of classified information.
- Consider coordinating with DOE-OR to begin entering self-assessment findings and programmatic issues into the self-reporting process available in SSIMS.
- Expand the data entered into the CTS to include IOSC and any other noncompliances related to the protection and control of classified information.

- Implement a trending and analysis process using data maintained in CTS. This trending data should include all information pertaining to the protection and control of classified information (IOSC, internal assessments, security surveys, and external audits, etc.).
- Add security personnel to the list of WEMS SMEs and trained causal analysis facilitators.
- Revise WEMS existing causal analysis guidance to specify when causal analysis and corrective action verification/effectiveness reviews are necessary for security and cyber security incidents. This revision will ensure that the most significant security incidents receive the appropriate rigor and attention.
- Provide additional detail in the annual self-assessment report, consistent with DOE directives, to indicate: what was assessed; how the assessment was performed; and an analysis of the results of assessment activities. The assessment should also provide a basis for management to make informed decisions regarding the WEMS information security program.
- Enhance the existing WEMS self-assessment program to include performance-based activities designed to demonstrate program effectiveness, and lessen reliance on compliance-based checklists.
- Document surveillance activities and on-the-spot corrections made throughout the year and include them in the annual self-assessment report as performance-based assessment observations.

II. General Program Implementation

The WEMS regulatory compliance program is well established, and has taken the initial steps of integrating 10 C.F.R. Part 824 requirements into its existing procedures related to the protection and control of classified information. Based on discussions with WEMS management and staff members, they are aware of the regulatory requirements associated with 10 C.F.R. Part 824; however, these requirements are not formally documented in all WEMS security and regulatory compliance procedures. The review team observed a close and effective working relationship among WEMS Security, the enforcement coordinator, and PPPO.

The WEMS enforcement coordinator is the site quality assurance (QA) manager and has extensive QA experience, having served as the safety enforcement coordinator at PORTS since 1997. The QA manager has only recently become involved in WEMS security activities and is now the security enforcement coordinator as well. The enforcement coordinator's lines of authority and communication, as well as associated roles and responsibilities, have not yet been formally defined or documented in the QA manager position description, nor formally documented in related regulatory compliance procedures.

The enforcement coordinator indicated that management supports the regulatory compliance program and there are open lines of communication with representatives of the senior management team. The enforcement coordinator participates in weekly senior management meetings to discuss corrective actions resulting from significant safety and security events, and the status and results of WEMS effectiveness reviews. In addition, the enforcement coordinator participates in SRBs that meet, when necessary, to ensure WEMS follows appropriate processes to identify, report, investigate, and screen security noncompliances; perform causal analysis; and develop corrective action plans. The enforcement coordinator also performs follow-up and close-out activities for nuclear safety, worker safety and health, and security issues.

To better facilitate a proactive and effective security regulatory compliance program, the enforcement coordinator should receive all available information that addresses WEMS performance related to the protection and control of classified information. Such information includes: security inquiry reports, internal assessment reports, trending and data analysis, protective force daily incident reports, external audit reports, DOE-OR security survey reports, Independent Oversight inspection reports, and other government agency investigations (e.g., Office of the Inspector General and Government Accountability Office). Although interviews determined that the enforcement coordinator has been actively involved in reviewing some of this information, there is currently no formal screening process that documents the regulatory considerations and/or decisions made for security noncompliances. Consideration should be given to the development of a formal regulatory screening process for IOSC and other classified information security noncompliances.

The WEMS security manager has served in his current role since 2010, and has extensive security experience at PORTS. After attending the Office of Security Enforcement's Regulatory Assistance Review security enforcement briefing at the Paducah Plant in May 2011, the WEMS security manager began building a working relationship with the WEMS enforcement coordinator. Although routine meetings are held, the roles and responsibilities between the two organizations have not yet been formally defined or documented.

The WEMS security manager indicated that WEMS senior management has been very supportive of the overall security program. In addition to attending weekly senior management meetings, he also participates in SRB meetings when significant security events occur. WEMS senior management's continued attention and commitment to the overall security program are crucial to the successful integration of its classified information security programs with the existing WEMS regulatory compliance program.

The WEMS CMPC program currently maintains three vault-type rooms (VTRs) and 16 General Services Administration approved security repositories designed for storage of classified information. The CMPC program is also responsible for approved non-conforming storage of classified matter in various locations at the plant. WEMS cyber security organization maintains one accredited stand-alone system that is located within a

VTR. The system has 15 designated users who possess security clearances commensurate with the classification level of the information being processed. WEMS stated during the review that they are planning to accredit another system in the near term.

This review found that classified documents and matter appear to be adequately protected and controlled in accordance with DOE policies, and maintained by trained and knowledgeable CMPC custodians. Most of the classified holdings at WEMS are legacy documents or classified matter that supports the gaseous diffusion process. Only on rare occasions are new classified documents developed. WEMS has developed a CMPC manual that describes and implements the CMPC program at PORTS. WEMS has implemented stringent and conservative administrative controls designed to limit access to classified information, which further reduces the opportunity for noncompliances. All WEMS custodians and employees with access to classified information are required to receive initial and annual CMPC training, and security awareness briefings. The training and briefings have recently been updated to include 10 C.F.R. Part 824.

The review team learned that although WEMS Security develops security lessons-learned updates for plant employees and uses various methods to communicate these lessons (e.g., training, e-mail, and newsletters), there is no formal WEMS security lessons-learned process.

Strengths

- There appears to be effective informal lines of communication between WEMS Security, the WEMS enforcement coordinator, and PPPO.
- The WEMS enforcement coordinator has many years of safety regulatory compliance experience that should aid in the successful integration of 10 C.F.R. Part 824 regulatory requirements into WEMS regulatory compliance program.
- Management attention and commitment to the overall security program are evident, as exemplified, in part, by their development and participation in the SRB.
- Classified documents and matter appear to be adequately protected and controlled, consistent with DOE policies.
- WEMS has implemented stringent and conservative administrative controls designed to limit access to classified information, which further reduces the opportunity for noncompliances.
- WEMS personnel with information security responsibilities are trained and knowledgeable of their program responsibilities.
- WEMS has a well-established security awareness program that includes 10 C.F.R. Part 824 requirements in its initial and annual security briefings.

Recommendations

- Ensure that applicable requirements identified in 10 C.F.R. Part 824 are formally documented in all of the WEMS local CMPC, IOSC, and classified cyber security program training and procedures.
- Define and formally document the regulatory compliance program structure as it relates to the protection and control of classified information including: lines of authority and communication; integration of 10 C.F.R. Part 824 into the existing WEMS regulatory compliance and WEMS Security programs; and associated roles and responsibilities.
- Develop a formal regulatory screening process that takes into consideration all of the available information that addresses WEMS performance related to the protection and control of classified information. To better facilitate this process, the enforcement coordinator should receive all available information that addresses WEMS performance related to the protection and control of classified information.

III. Identification and Reporting of Incidents of Security Concern

WEMS Procedure FSS-4330/Rev. 0, *Conduct of Inquiries into Incidents of Security Concern*, dated May 12, 2010, describes the requirements for reporting IOSC, conducting inquiries, and performing corrective/disciplinary actions. According to this procedure, all PORTS contractor and subcontractor employees are responsible for reporting any observations, findings, or information regarding a potential IOSC to WEMS Security during normal working hours, or to the plant shift superintendent after normal working hours. Any person who discovers a security interest at risk (e.g., classified matter, government property) must take reasonable and prudent steps to contain the incident, protect the scene to ensure evidence is not tampered with or destroyed, and secure classified matter.

Security incidents reported through the IOSC program are categorized and resolved in accordance with DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management*, and DOE-OR, *Implementing Instructions for Incidents of Security Concern*, dated July 2008. WEMS Security utilizes a multi-disciplinary approach for initially categorizing security incidents involving classified information by consulting DOE-OR, CMPC operations manager, and, if necessary, PPPO in determining the appropriate Impact Measurement Index (IMI) categorization.

When a security-related incident occurs, WEMS Security is responsible for notifying DOE-OR CMPC operations manager during duty hours or DOE-OR operations center after normal duty hours. If classified information is found to have been processed or stored on an unclassified information system, the cyber security staff is required to take the appropriate action to contain and sanitize all affected systems and provide support to the inquiry official, as needed.

PPPO and WEMS do not have access to a SSIMS terminal to report and track security incidents. All documentation related to security incidents is transmitted to DOE-OR for data entry into SSIMS. Due to not having access to SSIMS, WEMS Security was not aware of the self-reporting process that is available to them. Currently, WEMS Security tracks security incidents separately on a spreadsheet and does not enter them in CTS.

Discussions with personnel assigned to the IOSC program revealed that the staff is knowledgeable of program requirements and WEMS operations. Two inquiry officials have successfully completed the inquiry training at the DOE National Training Center, while three newly appointed officials have not yet attended the requisite training; however, all of the inquiry officials have many years of security and investigative training and experience. The review team examined five security incident files and determined that the IMI categorizations were accurate, and all required initial reporting and incident inquiry timelines were met. The final inquiry reports were thorough and completed in a timely manner. The reports included enough information so that third-party readers, unfamiliar with the site security configuration, could easily understand the circumstances surrounding the incident.

Cyber security personnel told the review team that when classified information has been discovered on unapproved systems, they are consulted during incident categorization and are actively involved in minimizing any further damage by isolating and sanitizing all affected systems.

Strengths

- WEMS uses a multi-disciplinary team approach to ensure the accuracy of initial categorization of security incidents, including consultation with DOE-OR and PPPO, as appropriate.
- WEMS IOSC program personnel are proactive in responding to security incidents, knowledgeable of program requirements, and have years of investigative experience.
- The IOSC program conducts thorough security incident inquiries and produces timely inquiry reports that are well written and can be easily understood by third-party readers.
- Cyber security and other SMEs are integrated into the IOSC program and are utilized as appropriate.

Recommendation

- Consider coordinating with DOE-OR to begin entering self-assessment findings and programmatic issues into the self-reporting process available in SSIMS.

IV. Issues Management and Trending

WEMS uses CTS as its designated internal issues management system. This database tracks all WEMS noncompliances and resulting corrective actions that result from internal and external reviews, assessments, security surveys, and other evaluation activities. However, CTS does not include any information associated with IOSCs. To obtain a more accurate analysis of the effectiveness of the WEMS information security program, WEMS should consider including an unclassified description of security-related issues and noncompliances resulting from IOSCs, so that they can evaluate all of the data in CTS pertaining to classified information, regardless of the source, in trending and analysis activities.

The WEMS corrective action program, to include CTS, is managed and administered by the QA organization. Noncompliances are entered and tracked through closure in accordance with WEMS Procedure FSS-2607/Rev. 0, *Issues Management Program*, dated March 9, 2010, which addresses the processes for reporting, evaluating, and managing resulting actions. Issues are derived from multiple sources including but not limited to: incidents, deliverables, assessments, general correspondence, and management decisions identified in the normal course of work. When an issue is identified, WEMS line management and QA are notified. The issue is evaluated to determine if it requires reporting under the WEMS *Nuclear, Worker Safety and Health, and Security* procedure, and an incident report is generated. The incident report is evaluated to determine if a critique and/or SRB meeting is required to perform causal analysis, develop corrective actions, identify the issue owner, assign due dates, and determine if an effectiveness review is required. The CTS coordinator is responsible for entering issues into CTS and assigning the functional manager ownership of the resulting corrective actions.

WEMS Procedure FSS-2608/Rev. 0, *Causal Analysis*, dated March 9, 2010, defines the methods for performing causal analysis in accordance with DOE Guide 231.1-2, *DOE Occurrence Reporting Causal Analysis Guide*. The purpose of the procedure is to assist personnel in determining the apparent cause and/or root cause of reportable occurrences. The WEMS policy requires the issue owner to determine if the assistance of a SME, a trained causal facilitator, and/or other individuals having skills, training, or experience related to the issue are needed, and assemble a causal analysis team. The current list of WEMS SMEs and trained causal facilitators does not include anyone from the security organization.

The procedure identified a number of causal analysis methodologies and tools available for use, and also described the rigor of causal analysis to be applied, based on the significance of the event. However, this procedure was developed without taking security incidents into consideration. Interviews with WEMS staff responsible for conducting causal analysis confirmed that the procedure is unclear when causal analysis is required for security and cyber security incidents or which causal analysis tool should be applied. WEMS staff also acknowledged the need to revise this procedure to address specific security situations/events that may require causal analysis.

Strengths

- Security noncompliances identified as a result of external/internal assessments are maintained in the WEMS CTS, which is a centralized database designed to ensure the effective management of noncompliances.
- WEMS has a causal analysis guidance procedure in place and requires training for all personnel responsible for conducting causal analysis.

Recommendations

- Expand the data entered into the CTS to include IOSC and any other noncompliances related to the protection and control of classified information.
- Implement a trending and analysis process using data maintained in CTS. This trending data should include all information pertaining to the protection and control of classified information (IOSC, internal assessments, security I surveys, and external audits, etc.).
- Add security personnel to the list of WEMS SMEs and trained causal analysis facilitators.
- Revise WEMS existing causal analysis guidance to specify when causal analysis and corrective action verification/effectiveness reviews are necessary for security and cyber security incidents. This revision will ensure that the most significant security incidents receive the appropriate rigor and attention.

V. Assessments

WEMS Procedure FSS-2602, *Oversight Activity – Management Conformity Assessment*, dated October 5, 2011, describes the process for conducting oversight activities called management conformity assessments (MCAs). Types of MCAs include but are not limited to walkthroughs, walk-downs, inspections, surveillances, reviews, examinations, and evaluations where programs, processes, products, services, and facilities are checked for conformance to requirements.

If a potential occurrence, incident, noncompliance, or nuclear, worker safety and health, or security issue is identified, it is immediately communicated to the WEMS line manager and the QA manager.

The WEMS security manager is responsible for implementation of the safeguards and security self-assessment program, in coordination with the QA manager. Interviews with these managers indicated their strong desire to implement an effective assessment program, and both were well aware of the importance of this program in preventing a significant security event from occurring.

The cyber security organization also conducts a self-assessment on the stand-alone classified computer systems operated by WEMS, which is due annually in August. Information and cyber security assessments are conducted by experienced personnel with sufficient training to assess assigned security topics. Noncompliances identified during the assessments are entered into CTS and tracked to closure.

The review team analyzed the *WEMS Safeguards and Security Self-Assessment Report at the Portsmouth Gaseous Diffusion Plant*, dated January 4, 2011, and the *Safeguards and Security Self-Assessment Report at the Portsmouth Gaseous Diffusion Plant*, dated January 23, 2012. The review validated that the WEMS assessment methodology includes document reviews, interviews, observations, and a few performance-based activities. The assessment approach was found to be almost exclusively compliance-based and driven by the security survey and self-assessment toolkit checklists. The information security section of these reports (section 8) provided a very brief description of requirements, a discussion of required training, and the assigned rating of satisfactory. Actual details of what was assessed, how the assessment was performed, and the results of the assessment were not included in the annual report. The review team found that the report provided limited value to management as a basis to make programmatic decisions about the WEMS information security program.

Given the compliance-based nature associated with checklists, more emphasis could be placed on the quality of performance-based activities conducted during CMPC assessments. For example, employees could be asked to demonstrate important information security tasks required of their positions. Increasing the frequency and broadening the scope of meaningful performance-based activities designed to demonstrate program effectiveness could enhance the WEMS self-assessment program.

The review team interviewed the individual responsible for conducting most of WEMS Security assessments and determined that this individual has extensive security experience and expertise in the areas he is assessing. He acknowledged that most of the WEMS Security assessment activities are compliance-based and recognizes the importance of observing employee performance. He further elaborated that he had conducted a number of surveillances throughout the year involving demolition and decommissioning activities taking place at PORTS that resulted in on-the-spot corrective actions. However, neither these surveillance activities nor the on-the-spot corrective actions were documented and included in the annual self-assessment report.

Strengths

- WEMS management recognizes the overall importance of having a viable self-assessment program and the ability to self-identify noncompliant conditions.
- A formal process is in place to provide timely notification to the appropriate manager and other designated personnel when noncompliances are identified during assessment activities.

- Personnel performing self-assessments are trained and possess subject matter expertise in the areas they are assessing.

Recommendations

- Provide additional detail in the annual self-assessment report, consistent with DOE directives, to indicate: what was assessed; how the assessment was performed; and an analysis of the results of assessment activities. The assessment should also provide a basis for management to make informed decisions regarding the WEMS information security program.
- Enhance the existing WEMS self-assessment program to include performance-based activities designed to demonstrate program effectiveness, and lessen reliance on compliance-based checklists.
- Document surveillance activities and on-the-spot corrections made throughout the year and include them in the annual self-assessment report as performance-based assessment observations.

VI. Summary

This review identified many existing attributes that indicate WEMS is in the process of establishing a comprehensive security regulatory compliance program. The enforcement coordinator has a wealth of site operational experience, a strong QA background, and has the respect of management and operations personnel. This strength can also be extended to others in the WEMS Security organization who also displayed a high level of technical competence and dedication to their professions. WEMS has a well-established IOSC program that provides for the accurate categorization of security incidents and the conduct of comprehensive inquiries.

Although WEMS has been actively involved with integrating 10 C.F.R. Part 824 requirements into its existing regulatory compliance program, these requirements have not been fully defined or documented in the appropriate WEMS security procedures or training that specifically address classified information security topics. Additionally, the security role of the enforcement coordinator still needs to be formally defined. A number of recommendations have been identified throughout this report to provide opportunities to further improve the WEMS classified information security regulatory compliance program.

By appropriately addressing the recommendations identified during this review, WEMS should expect to realize improved performance in the ability to avoid or reduce the severity of classified information security noncompliances; facilitate the Office of Security Enforcement's exercise of discretion for noncompliant conditions that are considered to be less significant; support mitigation consideration in any future enforcement action; and ensure that classified information security shortcomings receive appropriate recognition and corrective actions. Any actions taken to address these

recommendations should be appropriately coordinated with the DOE Office of Environmental Management and PPPO.

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

- Benchmarking with other DOE sites regarding the integration and coordination of the site security organization with the existing regulatory compliance program.
- Contacting other sites (e.g., the Y-12 National Security Complex and the Paducah Plant) to determine whether 10 C.F.R. Part 824 enforcement program integration activities (including tracking, trending, and analysis systems) that have been implemented at those sites would be useful to improve WEMS' existing regulatory compliance program.
- Ensuring more timely reporting and tracking of IOSC and self-reporting of programmatic issues resulting from self-assessments by installing a SSIMS terminal at PPPO and/or at WEMS.

List of Acronyms

CMPC	Classified Matter Protection and Control
CTS	Commitment Tracking System
DOE	U.S. Department of Energy
DOE-OR	DOE Oak Ridge Office
EPO	Enforcement Process Overview
FBP	Fluor, Babcock & Wilcox Portsmouth
IMI	Impact Measurement Index
IOSC	Incidents of Security Concern
MCA	Management Conformity Assessment
PORTS	Portsmouth Gaseous Diffusion Plant
PPPO	Portsmouth/Paducah Project Office
QA	Quality Assurance
SME	Subject Matter Expert
SRB	Senior Review Board
SSIMS	Safeguards and Security Information Management System
VTR	Vault-Type Room
WEMS	Wastren-EnergX Mission Support, LLC
WEMS Security	WEMS Security Organization