Department of Energy
Washington, DC 20585

August 24, 2011

Mr. Scott Smith
Program Manager
Swift & Staley Mechanical Contractors, Inc.
761 Veterans Avenue
Kevil, Kentucky 42503-9363

Dear Mr. Smith:

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 Swift & Staley Mechanical Contractors, Inc. (SST) regulatory compliance program during the period May 23, 2011 – May 26, 2011. Our review included an evaluation of SST processes for identifying, reporting and tracking classified information security noncompliances; SST internal tracking systems; and processes for correcting deficiencies to prevent recurrence. The Office of Security Enforcement also conducted a limited review of SST management and safeguards and security self-assessment programs.

Although SST is in the early stages of integrating 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 SST 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 SST's 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 SST, 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,

John S. Boulden III

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

Enclosure: Regulatory Assistance Review Report

cc: David May, Swift & Staley Mechanical Contractors, Inc.
Debora Jolly, Swift & Staley Mechanical Contractors, Inc.
Mark Duff, LATA Kentucky
William Franz, LATA Kentucky

Enclosure

OFFICE OF SECURITY ENFORCEMENT
REGULATORY ASSISTANCE REVIEW
SWIFT & STALEY MECHANICAL CONTRACTORS, INC.

I. Introduction

During May 23-26, 2011, the Office of Security Enforcement, within the Office of Health, Safety and Security, conducted a regulatory assistance review of the classified information security program managed by Swift & Staley Mechanical Contractors, Inc. (SST), located at the Paducah Gaseous Diffusion Plant (PGDP) in Paducah, Kentucky. The review was conducted in a manner consistent with the guidance provided in the *Enforcement Process Overview* (EPO), dated June 2009. The EPO document is located on the Office of Health, Safety and Security website at:
http://www.hss.doe.gov/enforce/docs/Final_EPO_June_2009_v4.pdf

This review included an evaluation of SST'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 SST's internal deficiency tracking/trending systems; and correcting deficiencies to prevent recurrence. It also included a limited review of SST's management and safeguards and security (S&S) internal assessment programs and an evaluation of SST'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).

At the time of this review, SST was in the initial stages of developing its regulatory compliance program for classified information security. Although the existing program documentation does not yet address the requirements of 10 C.F.R. Part 824, SST has recently appointed an enforcement coordinator and started the process of including the regulatory requirements into existing security procedures and training. These initiatives are discussed throughout this report. In addition, this report identifies strengths, as well as recommendations intended to improve the effectiveness of the SST regulatory compliance program for classified information security. Strengths and recommendations are listed below and are discussed in further detail in the appropriate sections of this report.

Strengths

- Management attention and commitment to the overall security program are evident, as exemplified, in part, by the significant effort to reduce the number of classified holdings since 2005, and the recent appointment of an enforcement coordinator.

- Classified documents are adequately protected, consistent with U.S. Department of Energy (DOE) requirements.

- There appears to be an effective partnership and lines of communication between the SST security organization (SST Security), the SST enforcement coordinator, and the Portsmouth/Paducah Project Office (PPPO).

- SST personnel with information security responsibilities are well trained and knowledgeable of their program responsibilities.

- SST incidents of security concern (IOSC) program personnel are proactive in responding to security incidents, knowledgeable of program requirements, and have years of investigative experience. Additionally, SST has recently increased the number of trained inquiry officials from two to five.

- SST uses a multi-disciplinary team approach to ensure the accuracy of initial categorization of security incidents that includes the Oak Ridge Office (OR) and PPPO, as appropriate.

- The IOSC program conducts thorough security incident inquiries and produces timely inquiry reports.

- S&S noncompliances identified as a result of security incidents or external/internal assessments are maintained in the SST Corrective Action Tracking System (CATS), which is a centralized database designed to ensure the effective management of all security-related noncompliances.

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

- SST management recognizes the overall importance of having a viable self-assessment program.

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

- A mechanism is in place to provide timely notification to the appropriate manager and other designated personnel when discrepancies are identified during the assessment.

Recommendations

- Ensure that applicable requirements identified in 10 C.F.R. Part 824 are formally documented in all of the SST local classified matter protection and control (CMPC), IOSC, and classified cyber security program procedures; local training that addresses classified information security training topics; and in the Site Security Plan (SSP).

- Define and formally document the regulatory compliance program structure including: lines of authority and communication; integration of 10 C.F.R. Part 824 into the existing SST regulatory compliance and security programs; and associated roles and responsibilities.

- Ensure that the enforcement coordinator receives all available information that addresses SST's performance related to the protection and control of classified information in order to provide effective support to the regulatory screening process. Such information includes: internal assessment reports; trending and analysis data; protective force daily incident reports; and external audit reports, such as those resulting from OR security surveys, Independent Oversight inspections, and other government agency investigations (e.g., Office of the Inspector General (IG) and Government Accountability Office (GAO)).

- Ensure inquiry reports contain sufficient detail so that third-party readers can easily understand the circumstances surrounding the incident.

- Conduct trending and analysis using data currently maintained in CATS. This trending data should include all information pertaining to CMPC (IOSC, internal assessment results, external surveys, and reviews, etc.). There is currently sufficient information contained in CATS to establish an integrated trending and analysis process.

- Establish a standardized approach to the SST causal analysis process. This will ensure all personnel are uniformly trained on the appropriate causal analysis models and tools required to be used by SST.

- Consider re-evaluating the criteria for determining when causal analysis and corrective action verification/effectiveness reviews are necessary. The existing restrictive criteria established by the SST procedure could discourage a formal causal analysis from being conducted in cases where it would be warranted. SST should maximize the opportunity to determine the underlying cause of less-severe classified information security noncompliances, and enhance the corrective action process through the conduct of independent verification/effectiveness reviews.

- Revise the self-assessment methodology to be less compliance-based and reliant on the use of checklists. CMPC assessments could be enhanced with an increased emphasis on the quality of performance-based activities designed to demonstrate program effectiveness.

- Broaden the CMPC assessment scope to consider other topical areas (e.g., protection program management, physical security, and protective force) that contribute to the protection of classified information.

- Ensure that SST Security's assessment activities are formally documented in SST corporate assessment procedures.

- Evaluate the need to continue the practice of conducting two self-assessments per year. The evaluation should also consider whether this duplicative effort inhibits SST's ability to conduct a need-based, in-depth, and balanced assessment.

- Provide more 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 SST information security program.

II. General Program Implementation

At the time of this review, SST had not yet integrated 10 C.F.R. Part 824 requirements into its existing regulatory compliance program. Likewise, the security enforcement program requirements have not been included in the security programs designed to protect and control classified information. Based on discussions with SST Security management, staff members are aware of the regulatory requirements associated with 10 C.F.R. Part 824; however, these requirements are not formally documented in SST procedures, the SSP, nor most of the local training modules that address classified information security topics. The review team observed a close and effective working relationship among SST Security, regulatory compliance program personnel, and PPPO.

SST management indicated that since 2005, a concerted effort has been made to secure and containerize loose classified matter; reduce the number of areas where classified information is stored; reduce the total number of classified holdings; and limit the number of personnel with access to classified information. These measures have decreased the likelihood of classified information being lost, compromised, or mishandled. In addition, this review found that SST classified documents are adequately protected in accordance with DOE requirements, and are controlled by trained and knowledgeable CMPC custodians. SST also employs stringent and conservative administrative controls to limit access to classified information, which further reduces the opportunity for noncompliances. All SST custodians and employees with access to classified information are required to receive initial and annual CMPC training.

SST recently appointed an enforcement coordinator with a quality assurance (QA) background. However, due to the lack of integration of 10 C.F.R. Part 824 into the existing SST regulatory compliance program structure, the enforcement coordinator lines of authority and communication, as well as associated roles and responsibilities, have not yet been formally defined or documented, thus limiting the benefits of this appointment.

To better facilitate a proactive and effective security regulatory compliance program, the enforcement coordinator should receive all available information that addresses SST's performance related to the protection and control of classified information in order to provide effective support to the regulatory screening process. Such information includes: security inquiry reports, internal assessment reports, trending and analysis data, protective force daily incident reports, external audit reports, OR security surveys, Independent Oversight inspections, and other government agency investigations (e.g., IG and GAO investigations). SST 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 SST regulatory compliance program.

Strengths

- Management attention and commitment to the overall security program are evident, as exemplified, in part, by the significant effort to reduce the number of classified holdings since 2005, and the recent appointment of an enforcement coordinator.

- Classified documents are adequately protected, consistent with DOE requirements.

- There appears to be an effective partnership and lines of communication between the SST Security staff, the SST enforcement coordinator, and PPPO.

- SST personnel with information security responsibilities are well trained and knowledgeable of their program responsibilities.

Recommendations

- Ensure that applicable requirements identified in 10 C.F.R. Part 824 are formally documented in all of the SST local CMPC, IOSC, and classified cyber security program procedures; local training that addresses classified information security training topics; and in the SSP.

- Define and formally document the regulatory compliance program structure including: lines of authority and communication; integration of 10 C.F.R. Part 824 into the existing SST regulatory compliance and security programs; and associated roles and responsibilities.

- Ensure that the enforcement coordinator receives all available information that addresses SST's performance related to the protection and control of classified information in order to provide effective support to the regulatory screening process. Such information includes: internal assessment reports; trending and analysis data; protective force daily incident reports; and external audit reports, such as those resulting from OR security surveys, Independent Oversight inspections, and other government agency investigations (e.g., IG and GAO).

III. Identification and Reporting of Incidents of Security Concern

SST Procedure PGDP 1.3.9/R4, *Conduct of Inquiries into Incidents of Security Concern*, dated February 14, 2011, describes the requirements for reporting IOSC, conducting inquiries, and performing corrective/disciplinary actions. According to this procedure, all Paducah DOE contractors and subcontractors are responsible for reporting any observations, findings, or information regarding a potential IOSC to SST Security during normal working hours, or to the plant shift superintendent after normal working hours. Any person discovering a security interest at risk (e.g., classified matter, government property, etc.) 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, Chg. 1, Part 2, Section N, *Incidents of Security Concern*, and DOE OR, *Implementing Instructions for Incidents of Security Concern*, dated July 2008. SST Security utilizes a multi-disciplinary approach for initially categorizing security incidents involving classified information by consulting OR and PPPO in determining the appropriate Impact Measurement Index (IMI) categorization.

SST Security is responsible for notifying (via secure phone) the OR IOSC program manager during duty hours, or the Oak Ridge Operations Center after normal duty hours, of all security-related incidents. 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.

During this review, the review team examined eight security incident files and determined that the IMI categorizations were accurate, and all requisite initial reporting and incident inquiry timelines were met. The final inquiry reports were thorough and completed in a timely manner. However, inquiry narratives could be improved by ensuring that enough information is provided so that third-party readers can easily understand the circumstances surrounding the incident.

Discussions with personnel assigned to the IOSC program revealed that the staff is knowledgeable of program requirements and SST operations. Furthermore, each inquiry official has attended the inquiry training at the DOE National Training Center, as well as having years of investigative experience.

Strengths

- SST IOSC program personnel are proactive in responding to security incidents, knowledgeable of program requirements, and have years of investigative experience. Additionally, SST has recently increased the number of trained inquiry officials from two to five.

- SST uses a multi-disciplinary team approach to ensure the accuracy of initial categorization of security incidents that includes OR and PPPO, as appropriate.

- The IOSC program conducts thorough security incident inquiries and produces timely inquiry reports.

Recommendation

- Ensure inquiry reports contain sufficient detail so that third-party readers can easily understand the circumstances surrounding the incident.

IV. Issues Management and Trending

PPPO and SST do not currently have access to a SSIMS terminal to report and track security incidents. All documentation related to security incidents is transmitted to OR, who enters the information into SSIMS. All SSIMS data related to IOSC are compiled by OR, and trending documentation is provided to SST upon request. The review team examined two trending reports recently provided by OR: one for all IOSC in 2010, and the other for IOSC reported during calendar year 2011 (through April). Trending data was limited to number counts with some breakdown by IMI levels and subject areas. In some cases, the trending data (i.e., "IOSC by Nature of Event") combined information from both the Paducah and Portsmouth facilities, making it difficult to discern which facility the incident originated from. SST uses CATS as its designated internal issues management system. This database tracks all SST issues/noncompliances, including IOSC and noncompliances resulting from internal and external reviews, assessments, surveys, and other evaluation activities. CATS also contains the associated corrective actions being implemented to address noncompliances.

SST personnel reported that trending and analysis activities are not performed due to having a low number of IOSC involving CMPC, and that OR provides trending data on IOSC when such information is requested by SST. However, the current trending data provided by OR does not take into consideration all noncompliances relating to CMPC, such as external reviews or self-assessments. The lack of a fully integrated trending process could lead to faulty conclusions about performance effectiveness and prevent the early detection of noncompliant conditions. To obtain a more accurate analysis of the effectiveness of the SST information security program, SST should consider evaluating all data in CATS pertaining to classified information, regardless of the source, in its trending and analysis activities.

The SST corrective action program (CAP), to include CATS, is managed and administered by the QA functional organization. Noncompliances are entered and tracked through closure in accordance with SST Procedure 5.4.2/R2, *Corrective Action Program,* dated March 16, 2010, which addresses the documentation, tracking, corrective actions, and trending of noncompliances, including those involving classified information. According to this procedure, when an issue (noncompliance) is identified, regardless of its source (e.g., self-assessments, security incidents, security surveys, inspections, investigations), the responsible functional manager is required to determine the extent of the problem, identify the problem significance category, and report the issue to the QA manager. The QA manager enters the issue into CATS and assigns the functional manager ownership of corrective actions. Whether or not a causal analysis is performed depends on the significance category of the issue/noncompliance. The functional manager will perform a root cause analysis if the issue is a significance category 1 or a recurring problem, or will perform an apparent cause analysis if the problem is a significance category 2. Significance categories 3 and 4 issues do not require causal analysis. The SST CAP procedure states, "that all persons performing causal analysis must be trained." However, SST has not formally established a standardized causal analysis process to ensure that all causal analysts are uniformly trained on the appropriate causal analysis models and tools used by SST.

The SST CAP procedure also requires that a corrective action plan be developed based on the results of the root or apparent cause analysis, along with an estimated completion date. Corrective actions and associated milestones are entered into CATS by the QA manager. The procedure further states: "Corrective actions are directly linked to the root cause, apparent cause, and/or causal factors, depending on the depth of the causal analysis." As indicated above, only the most egregious of noncompliances receive root or apparent cause analysis (i.e., significance category 1 or 2). The procedure is unclear in describing how corrective actions associated with category 3 and 4 noncompliances can be directly linked to any form of causal analysis. (Note: In reviewing the definitions of the significance categories, the examples provided are more specifically related to safety issues, with vague, generic references that may be applied to security, i.e., "procedural violation" or "finding.") The restrictive criteria established by SST for a formal causal analysis could preclude rigorously reviewing classified information events that do not meet the significance category or determining the root cause of recurring trends involving less severe classified information security findings.

When the corrective actions are complete, the responsible manager notifies the QA manager of the date the action was completed. Verification and validation of the corrective actions is dependent on the significance category of the issue. Only significance category 1 and 2 issues, and recurring problems, receive corrective action verifications and effectiveness reviews conducted by someone appointed by the functional manager. Significance category 3 and 4 issues do not receive corrective action verifications and effectiveness reviews. However, the CAP procedure universally mandates independent effectiveness reviews and states that such reviews "may" be conducted by an organization independent of the problem. Given that no documented criteria is included that describes when an independent effectiveness review would be appropriate, the use of this review appears to be arbitrary.

Strengths

- S&S noncompliances identified as a result of security incidents or external/internal assessments are maintained in the SST CATS, which is a centralized database designed to ensure the effective management of all security-related noncompliances.
- SST requires training for all personnel responsible for conducting causal analysis.

Recommendations

- Conduct trending and analysis using data currently maintained in CATS. This trending data should include all information pertaining to CMPC (IOSC, internal assessment results, external surveys, and reviews, etc.). There is currently sufficient information contained in CATS to establish an integrated trending and analysis process.
- Establish a standardized approach to the SST causal analysis process. This will ensure all personnel are uniformly trained on the appropriate causal analysis models and tools required to be used by SST.
- Consider re-evaluating the criteria for determining when causal analysis and corrective action verification/effectiveness reviews are necessary. The existing restrictive criteria established by the SST procedure could discourage a formal causal analysis from being conducted in cases where it would be warranted. SST should maximize the opportunity to determine the underlying cause of less-severe classified information security noncompliances, and enhance the corrective action process through the conduct of independent validation/effectiveness reviews.

V. Assessments

The purpose of the SST self-assessment program is to provide assurance that security assets are protected at appropriate levels and to facilitate improvement and correction of the overall S&S program. These goals are accomplished by self-identifying noncompliant conditions during assessment activities. SST self-assessment processes are documented in SST Procedure 5.2.1/R2, *SST Integrated Assessment Program*, dated March 16, 2010. The SST QA manager is responsible for implementing the self-assessment program. The functional manager (in this case, the security manager) is responsible for assisting the QA manager in developing the assessment schedule, implementing assessments, and assigning assessors appropriate to the topic. Interviews with these managers indicated their desire to implement an effective assessment program, and both were aware of the importance of this program in preventing a significant security event.

The *SST Integrated Assessment Program* procedure defines guidelines and responsibilities for planning and executing self-assessments in accordance with DOE requirements. The procedure also defines guidelines and responsibilities for independent (internal) assessments. While this procedure sufficiently addresses both subject areas, neither procedure accurately or completely describes the assessment activities being performed by SST Security.

Currently, SST Security performs two self-assessments per year: the Security Programmatic Annual Self-Assessment and the Annual Comprehensive Self-Assessment. The Programmatic Self-Assessment utilizes checklists in the DOE S&S Survey and Self-Assessment Toolkit. A limited number of checklist items are selected (by various means, for example, one team member picks items for another team member, or a team member self-selects) to encompass all security program areas. The Annual Comprehensive Self-Assessment again uses the Toolkit checklists; however, all checklist items are selected and answered (hence the use of the term "Comprehensive"). Cyber Security also conducts a self-assessment on the two stand-alone classified computer systems operated by SST. Information and cyber security assessments are conducted by experienced personnel with sufficient training to assess their assigned security topics. Interviews with personnel responsible for conducting assessments indicated that a mechanism is in place to provide timely notification to the appropriate manager and other designated personnel when any discrepancies are identified during the assessment.

The review team analyzed the *2010 Self-Assessment Program Report for the Swift and Staley Security Organization at the Paducah Site*, dated March 23, 2011. The review validated that the SST assessment methodology includes document reviews, interviews, observations, and some performance tests. Although the assessment approach was found to be primarily compliance-based and driven by the Survey and Self-Assessment Toolkit checklists, there was some evidence of the adequacy and effectiveness of some program activities. This review found that the scope of the CMPC assessment was extremely broad and that the evaluation depth could have been more extensive in some areas. The Information Security section of the report (section 4) provided a very brief synopsis of inspection activities and results (i.e., the CMPC section of the report contained only three sentences, excluding sentences identifying the rating). Actual details of what was assessed, how the assessment was performed, and the results of the assessment were found to be contained in the support materials, but were not included in the annual report. The report provides limited value to management as a basis to make programmatic decisions about the information security program. The overall benefit of SST personnel conducting two self-assessments within the same program areas each year should be reviewed, as the current periodicity may actually have a negative impact on the quality of evaluation activities, as well as the assessment report.

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 CMPC assessments.

Strengths

- SST management recognizes the overall importance of having a viable self-assessment program.
- Personnel performing self-assessments are trained and have extensive subject matter expertise in the areas they are assessing.
- A mechanism is in place to provide timely notification to the appropriate manager and other designated personnel when discrepancies are identified during the assessment.

Recommendations

- Revise the self-assessment methodology to be less compliance-based and reliant on the use of checklists. CMPC assessments could be enhanced with an increased emphasis on the quality of performance-based activities designed to demonstrate program effectiveness.
- Broaden the CMPC assessment scope to consider other topical areas (e.g., protection program management, physical security, and protective force) that contribute to the protection of classified information.
- Ensure that SST Security's assessment activities are formally documented in SST corporate assessment procedures.
- Evaluate the need to continue the practice of conducting two self-assessments per year. The evaluation should also consider whether this duplicative effort inhibits SST's ability to conduct a need-based, in-depth, and balanced assessment.
- Provide more 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 SST information security program.

VI. Summary

SST is in the initial stages of developing its security regulatory compliance program. The program documentation developed to date has not integrated 10 C.F.R. Part 824 into the overall program. As a result, the security role of the enforcement coordinator has not been formally defined, nor have security enforcement program requirements been integrated into the operations of SST Security. Although recommendations for program improvement were identified, many attributes point to the ability of SST to establish a solid regulatory compliance program, as evidenced by the person recently appointed as the enforcement coordinator. This person has a wealth of site operational experience, a solid QA background, and has the respect of management and operations personnel. This strength can also be extended to others in SST Security who display a high level of technical competence and are dedicated to their professions.

SST has a well-established IOSC program that provides for the accurate categorization of security incidents and the conduct of comprehensive inquiries by knowledgeable and trained staff. The use of subject matter experts in the categorization and review of inquiry results also contributes significantly to the success of the program. However, neither SST nor PPPO have access to a SSIMS terminal, and must send hard copy security incident inquiry reports to OR for entry into SSIMS.

Although SST Security personnel have expertise in conducting self-assessments and SST has established processes and practices for an integrated assessment program, the assessments performed by SST Security do not adhere to the *SST Integrated Assessment Program* procedure. The structure of the SST Security self-assessment program, along with program processes and practices, are not formally documented. SST currently conducts all assessments using the checklists provided in the DOE S&S Survey and Self-Assessment Toolkit. This strategy results in a more compliance-based assessment with a broad scope and questionable in-depth evaluation. Additionally, SST conducts two security self-assessments per year covering the same basic subject areas based on the checklists. The value of this practice is uncertain, and it may actually have some negative impact by over-burdening limited resources. It may be more beneficial to conduct one comprehensive assessment with an increased emphasis on quality, and include additional performance-based activities that are designed to demonstrate program effectiveness.

The Information Security portion of the *2010 Self-Assessment Program Report for the Security Organization* did not contain a significant level of detail, and is of limited value to SST in managing its information security program. SST should consider expanding its criteria for determining when a formal causal analysis is required so that more classified information security events, as well as recurring trends involving less-severe noncompliances, are afforded a more rigorous analysis process. Since all CMPC related noncompliances are tracked in CATS, SST should consider performing its own, in-depth, comprehensive trending and analysis, using all available information in the CATS database.

By appropriately addressing the recommendations identified during this review, SST should expect to realize improved performance in the ability to avoid or reduce the severity of classified information security noncompliances; subsequently facilitate the Office of Security Enforcement's exercise of discretion for noncompliant conditions that are considered to be less significant; support mitigation consideration in any future enforcement action; and ensure that classified information security 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 SST to consider these suggestions as a means of strengthening SST's classified information security and regulatory compliance programs:

- Benchmarking with other DOE sites regarding the integration and coordination of the security organization with the existing regulatory compliance program.
- Contacting other sites (e.g., the Y-12 National Security Complex) to determine whether their 10 C.F.R. Part 824 enforcement program integration activities (including the Y-12 tracking, trending, and analysis systems) could improve SST processes.
- Evaluating the effectiveness of inspections upon exit from the limited area and security interest areas to act as a deterrent to the unauthorized removal of classified matter. This evaluation should consider the frequency of these inspections, as well as ensuring the inspection techniques are capable of detecting the classified assets being protected.
- Installing a local SSIMS terminal to allow SST to enter initial notifications of IOSCs, inquiry reports, and infraction forms, rather than relying on OR. It would also allow SST to monitor the status of reported security incidents, and to self-report noncompliances discovered as a result of its self-assessment activities.

List of Acronyms

CAP	Corrective Action Program
CATS	Corrective Action Tracking System
CMPC	Classified Matter Protection and Control
DOE	U.S. Department of Energy
EPO	Enforcement Process Overview
GAO	Government Accountability Office
IG	Office of the Inspector General
IMI	Impact Measurement Index
IOSC	Incidents of Security Concern
OR	Oak Ridge Office
PGDP	Paducah Gaseous Diffusion Plant
PPPO	Portsmouth/Paducah Program Office
QA	Quality Assurance
S&S	Safeguards & Security
SSIMS	Safeguards and Security Information Management System
SSP	Site Security Plan
SST	Swift and Staley Team
SST Security	SST Security Organization