Department of Energy
Washington, DC 20585

September 7, 2010

Dr. George H. Miller
Director
Lawrence Livermore National Laboratory
P.O. Box 808
Livermore, California 94551-0808

Dear Dr. Miller:

The Office of Health, Safety and Security's Office of Security Enforcement conducted an onsite regulatory assistance review from May 3 – 6, 2010, of the classified information security program elements that support the Lawrence Livermore National Security, LLC (LLNS) regulatory compliance program. Our review included: an evaluation of LLNS processes for identifying, reporting and tracking classified information security noncompliances; LLNS internal tracking systems; and processes for correcting deficiencies to prevent recurrence. The Office of Security Enforcement also conducted a limited review of LLNS management and Safeguards and Security self-assessment programs.

Although LLNS 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, the Office of Enforcement is encouraged by the improvement initiatives related to implementation of its security regulatory compliance program. This review, described in the enclosed report, identified several strengths and some weaknesses with LLNS' security enforcement program.

Correction of the weaknesses noted in this report may support the Office of Enforcement in providing mitigation as described in the U.S. Department of Energy Enforcement Policy (10 C.F.R. Part 824, appendix A) for any future classified information security related enforcement action against LLNS.

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

Sincerely,

John S. Boulden III

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

Enclosure

cc: Alice Williams, NNSA/LSO
John Lewis, LLNS
Constance De Grange, LLNS

OFFICE OF SECURITY ENFORCEMENT
REGULATORY ASSISTANCE REVIEW
LAWRENCE LIVERMORE NATIONAL SECURITY, LLC

I. Introduction

During May 3-6, 2010, the Office of Security Enforcement, within the Office of Health, Safety and Security, conducted a regulatory assistance review of the classified information security programs managed by Lawrence Livermore National Security, LLC (LLNS). 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 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 LLNS processes for identifying classified information security noncompliances; reporting and tracking classified information security noncompliances in the Safeguards and Security Information Management System (SSIMS); using LLNS internal deficiency tracking/trending systems; and correcting deficiencies to prevent recurrence. It also included a limited review of LLNS management and Safeguards and Security (S&S) internal assessment programs and an evaluation of LLNS efforts to integrate its classified information security regulatory compliance assurance program – as defined by Title 10 Code of Federal Regulations (C.F.R.) Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*, and Departmental security policies – with its existing regulatory compliance assurance program, which includes both nuclear safety and worker safety and health enforcement (hereinafter referred to as the enforcement program).

Prior to this review, the Office of Enforcement issued a security enforcement letter to LLNS on May 15, 2008, that specifically addressed concerns regarding classified e-mails sent by unauthorized methods and the effectiveness of corrective actions to prevent recurrence. This regulatory assistance review found that LLNS took the enforcement letter seriously and made positive efforts to address the concerns. However, LLNS had no formal documentation or evidence files to support those efforts.

At the time of this review, LLNS had a number of ongoing improvement initiatives related to the implementation of its regulatory compliance assurance program for classified information security. These initiatives are discussed throughout this report. In addition, this review identified several strengths and some weaknesses regarding the effectiveness of the LLNS regulatory compliance assurance program for classified information security. Strengths and weaknesses 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 addition of a new staff position to the LLNS enforcement program to specifically address classified information security regulatory compliance matters.

- There is an effective partnership between the contractor and the Livermore Site Office (LSO).

- The LLNS security organization has developed a close relationship and effective lines of communication with the LLNS enforcement program.

- LLNS exhibits a strong "self-reporting" culture in which 80 percent of the security incidents are self-reported by the offending LLNS employee.

- Personnel in the security incident reporting office (SIRO) are well trained and knowledgeable of regulatory and policy requirements, and their program responsibilities.

- LLNS uses a team concept in the initial categorization of security incidents that includes LSO and subject matter experts (SMEs), as appropriate.

- LLNS conducts thorough security incident inquiries and completes timely, well-documented inquiry reports. In addition, LLNS recently (February 2010) began entering its own security incidents into SSIMS, which should improve the timeliness of security incident actions and provide greater knowledge of security incident trending data.

- S&S noncompliances identified as a result of security incidents or external/internal assessments are included in the LLNS Issues Tracking System (ITS), which is designed to ensure the evaluation, resolution, closure, reporting, and trending of all S&S-related issues.

- The LLNS causal analysis process is based on a well documented, graded approach and a risk-based process that determines the degree of rigor necessary to ensure timely and appropriate actions to minimize the potential for recurrence. LLNS requires training for all personnel before they are assigned as causal analysts.

- All causal analyses receive a quality review, as well as validation by the topical area SME from the security organization.

- The Lawrence Livermore National Laboratory (LLNL) internal assessment program, specifically the topical/subtopical self-assessments, appear to be comprehensive and effective in providing management with feedback on the performance, quality, and compliance of the security program. All assessors receive training designed to ensure a uniform process and final product.

- Each assessment is reviewed for quality to ensure that the scope, the assessment methodologies, and the results meet expectations and that all identified issues and deficiencies are adequately documented.
- The LLNS classified matter protection and control (CMPC) and cyber security program personnel are well trained and knowledgeable of program responsibilities and requirements, and provide SME assistance as necessary.

Weaknesses

- The applicability of 10 C.F.R. Part 824 is not included in any of the LLNS local security or cyber security training courses that address classified information topics.
- LLNS lacks any formal documentation or evidence files to support its efforts in response to the enforcement letter issued by the Office of Enforcement in May 2008.
- Some recent security incidents appear to have been categorized at a lower Impact Measurement Index (IMI) level as a result of inappropriately ruling out the possibility of a suspected or potential compromise of classified information.
- The LLNS SIRO was aware of an increased trend of security incidents in calendar year (CY) 2009 involving the mishandling and storage of classified information but had not yet analyzed the information to determine the cause(s) for this trend.
- The minimal analysis of data related to classified information security noncompliances identified during assessments and incidents of security concern has impacted LLNS's ability to specifically identify the sources and/or causes.
- The LLNS compliance codes currently used in ITS for classified information security noncompliances do not include the specific Departmental security policy citations related to the identified issues and are too broad to facilitate the level of trending analysis needed to assist in preventing recurrence.
- The fiscal year (FY) 2009 annual security organization assessment summary report does not provide the necessary details to fully describe the assessment scope, methodologies, and results in a manner that allows management, specifically LSO, to understand the issues or the overall health of the LLNS security program.
- The cyber security organization does not enter identified concerns from intrusion detection monitoring performance tests into ITS, thus limiting the effectiveness of trending capabilities.

II. General Program Implementation

LLNS initially began to integrate 10 C.F.R. Part 824 into its enforcement program in late November 2009. To prepare for this integration, the LLNS enforcement coordinator conducted a preliminary analysis of the gaps in its implementation plan. In December 2009, the gap analysis was completed, with input from the LLNS security organization, and a plan to address identified shortcomings was developed.

Based on LLNS review and analysis of its enforcement program in December 2009, the following six issues were identified as areas that needed to be addressed to ensure that 10 C.F.R. Part 824 requirements are fully integrated into their enforcement program:

1. The document that describes the LLNS regulatory compliance assurance program does not explicitly address the requirements or expectations described in 10 C.F.R. Part 824.
2. The analysis of security incidents and issues for root and apparent causes and extent of condition was not consistently performed in accordance with locally established procedures.
3. The SIRO and the Performance Analysis and Reporting Section have not had access to SSIMS to ensure accurate reporting and analysis of inputted data.
4. LLNS does not consistently track corrective actions in response to classified information security incidents in ITS and ensure that corrective actions are effective in preventing recurrence.
5. LLNS has not routinely and consistently conducted or documented performance analysis of classified information security identified issues.
6. LLNS has not yet identified the regulatory compliance assurance staff needed to support the classified information security program.

These six issues were entered into ITS, along with specific corrective actions to address each programmatic shortcoming. At the time of this review, issues 3 through 6 listed above still had open corrective actions, with the last action due to close on July 30, 2010. Ongoing initiatives to formalize processes and procedures are continuing to address the 10 C.F.R. Part 824 integration concerns and the regulatory compliance screening of classified information security noncompliances. LLNS is in the initial stages of formally integrating elements of its classified information security program into its enforcement program, and there appears to be a close and effective working relationship between the contractor assurance office (CAO) and the LLNS security organization.

As a result of LLNS's planning and analysis, as discussed above, an integration plan was developed, and full implementation is expected by August 2010. The integration plan proposed adding a position specifically to address classified information security within the LLNS enforcement program. Once this position is filled, the assigned individual will facilitate the process for identifying, reporting, and tracking classified information security noncompliances. The main focus of this position is to ensure prompt self-identification and correction of noncompliances so that LLNS can identify and correct problems in advance, rather than reacting to a security event or having an external oversight organization find the noncompliant condition.

The roles and responsibilities for the regulatory compliance assurance program are documented in DES-0083, *Identifying, Reporting, and Tracking Noncompliances with DOE Safety and Security Requirements, Contractor Assurance*. This procedure was recently created, effective May 1, 2010, to include the requirements of 10 C.F.R. Part 824. The procedure for managing security incidents also describes the classified information security regulatory compliance assurance program. Additional implementation processes have been integrated for consistency in a number of other procedural documents (e.g., conducting causal analysis, managing assessments, lessons learned).

LLNS personnel are trained in regulatory compliance assurance by completing two courses. The first course, *CA0100 Safety and Security Regulatory Compliance Program*, is a one-time, two-hour course for senior managers and is a prerequisite for the second course, *CA0200 Safety and Security Regulatory Compliance Evaluation*, which is a two-hour course for evaluators, functional area managers, and directorate points of contact and is required every other year. Both courses were recently updated to address the recent changes in the classified information security enforcement program. Although this training has been updated, the review team determined that other local security and cyber security training developed by LLNS to address classified information topics have not been updated to include 10 C.F.R Part 824 requirements.

This review also found that security incident trending data is provided on a monthly basis to senior management and quarterly to Directorate Security Officers (DSOs). However, prior to the current LLNS enforcement coordinator there was very little involvement with classified information security-related issues, and metrics and trending data were only provided by the LLNS security office. Nonetheless, upon full integration of 10 C.F.R. Part 824 into the LLNS existing enforcement program and the addition of a new staff position for handling classified information security issues, the expectations, as defined in DES-0083, *Identifying, Reporting, and Tracking Noncompliances with DOE Safety and Security Requirements, Contractor Assurance* should be achieved.

Strengths

- Management attention and commitment to the overall security program are evident, as exemplified, in part, by the addition of a new staff position to the LLNS enforcement program to specifically address classified information security regulatory compliance matters.

- There is an effective partnership between the contractor and LSO.

- The LLNS security organization has developed a close relationship and effective lines of communication with the LLNS enforcement program.

Weaknesses

- The applicability of 10 C.F.R. Part 824 is not included in any of the LLNS local security or cyber security training courses that address classified information topics.
- LLNS lacks any formal documentation or evidence files to support its efforts in response to the enforcement letter issued by the Office of Enforcement in May 2008.

III. Identification and Reporting of Incidents of Security Concern

LLNS procedure SOM-PRO-10-005993, *Incidents of Security Concern* (Rev. 4), dated March 3, 2010, establishes procedures for classification review and timely dissemination of security incidents to LLNL management, the National Nuclear Security Administration (NNSA), LSO, and DOE Headquarters. Specifically, this procedure covers the following program elements associated with reportable security incidents: incident identification, notification, inquiry, and reporting.

The SIRO is the single point of contact for reporting incidents of security concern at LLNL. Any person who identifies a potential security incident immediately notifies his/her line management, the program security representative (PSR), or the security duty officer and takes appropriate action to ensure that security-related information is appropriately secured. If the potential incident involves cyber security, the person who identifies it may notify the cognizant organizational information systems security officer (OISSO) or information systems security officer (ISSO). Line management, the PSR, the DSO, or the OISSO/ISSO notifies the SIRO as soon as the potential security incident is reported. When an incident involves cyber security, the SIRO contacts the OISSO/ISSO. Based on discussions with SIRO personnel and a review of the SIRO monthly performance review statistics for FY 2009 and the first half of FY 2010, approximately 80 percent of the reportable incidents are self-reported by LLNS employees, indicating a strong reporting culture.

The SIRO, consisting of a group leader and two inquiry officers, is assigned to the Office of Investigative Services, which is part of the LLNS security organization. SIRO personnel are knowledgeable of their assigned responsibilities and have years of investigative experience.

LLNS uses the IMI tables from DOE Manual 470.4-1 Chg. 1, Part 2, Section N, as a basis for identifying reportable security incidents. The SIRO is responsible for initially determining the IMI categorization. However, the SIRO has instituted a collaborative approach in which it consults with LLNS management, cyber security and CMPC SMEs, LSO, and the NNSA Office of Defense Nuclear Security (NA-70) as needed when categorizing incidents. Also as needed, the SIRO works with the LLNS computer security organization concerning incident identification, incident isolation, and incident sanitization. The SIRO issues a final inquiry report when the investigation and analysis of the security incident have been completed, causes identified and finalized, corrective actions determined, and lessons-learned identified. Based on the results of the inquiry and the totality of the circumstances surrounding the incident, the SIRO, when appropriate, issues an infraction to the responsible individual or individuals. The SIRO has a memorandum of understanding with the special access program (SAP) and sensitive compartmented information (SCI) facility coordinators to ensure that all reporting and inquiry requirements are appropriately met for related incidents.

Before the onsite portion of this regulatory assistance review, the review team specifically identified nine security incidents that LLNS reported to SSIMS for which the categorization appeared to be questionable. The review team examined the files for these security incidents during the onsite visit. Four of the nine incident files contained additional information that mitigated the categorization concern. However, for the remaining five incident files, the review team concluded that the categorization determinations made by LLNS did not accurately reflect the potential for compromise of classified information. Because LLNS has appropriately instituted a graded approach to the level of rigor applied to causal/root cause analysis and the resulting corrective actions/verification and validation based on the IMI level, it is important that the categorization be correct and a conservative approach applied (i.e., if the incident overlaps two categories, the more stringent one is applied). Correct and conservative categorization should help better define root causes, corrective actions, and lessons learned, thereby preventing recurrence. The review team found the inquiry reports to be timely and well documented. In addition, LLNS has recently (February 2010) started to enter its own security incidents into SSIMS, potentially allowing LLNS to formally close out security incidents sooner and gain real-time security incident trending data.

Strengths

- LLNS exhibits a strong "self-reporting" culture in which 80 percent of the security incidents are self-reported by the offending LLNS employee.

- Personnel in the SIRO are well trained and knowledgeable of regulatory and policy requirements, and their program responsibilities.

- LLNS uses a team concept in the initial categorization of security incidents that includes LSO and SMEs, as appropriate.

- LLNS conducts thorough security incident inquiries and completes timely, well-documented inquiry reports. In addition, LLNS recently (February 2010) began entering its own security incidents into SSIMS, which should improve the timeliness of security incident actions and provide greater knowledge of security incident trending data.

Weakness

- Some recent security incidents appear to have been categorized at a lower IMI level as a result of inappropriately ruling out the possibility of a suspected or potential compromise of classified information.

IV. Issues Management and Trending

SSIMS is used to report and track security incidents and more significant classified information security noncompliances resulting from assessments. Principal directorates (PDs) also use ITS for reporting and tracking all classified information security noncompliances. Noncompliances are entered and tracked through closure in accordance with PRO-0042, *Issues and Corrective Action Management.* This procedure and ITS are used to implement a comprehensive, integrated, transparent, and structured issues and corrective action management process that focuses on critical issues and uses a risk management methodology/graded approach for resolving issues.

Once an incident is reported to DOE, the SIRO notifies the appropriate DSO, enters the incident into the ITS, and assigns the causal analysis and resulting corrective actions to the appropriate DSO. The SIRO also identifies the incident as a noncompliance with DOE classified information security requirements by selecting the appropriate LLNS compliance code. The regulatory assistance review team found that the LLNS compliance codes used do not include the specific Departmental security policy citations related to the identified issues. This lack of specificity may make it more difficult for LLNS to understand its trending data needed to assist in preventing recurrence.

Line management within each PD is responsible for ensuring that sufficient personnel are trained in the identification, reporting, and causal analysis of security incidents. All personnel conducting causal analyses must complete the following required training: CA-0014, *Causal Analysis Methods and Techniques*; CA-2011, *Apparent Cause Analysis*; and CA-0007, *Incident/Root Cause Analysis.*

For all reportable classified information security noncompliances, a causal analysis, extent-of-condition evaluation, and effectiveness review are performed in consultation with the CAO and the SIRO. For classified information security noncompliances resulting from a reportable incident (IMI-1through IMI-4), causal analysis requirements are described in the SIRO procedure SOM-PRO-10-005993, *Incidents of Security Concern, Attachment A, Site-Specific Reportable Incidents of Security Concern by Group.* LLNS uses a graded approach to its causal analysis, based on the severity of the incident (i.e., apparent cause, management root cause, or independent root cause). LLNS has predefined, as a guide, what type of causal analysis is required for each of the IMI categories/subcategories. For example, IMI-1 security incidents typically require a more rigorous causal analysis (i.e., independent root cause), whereas IMI-3 and -4 require the least rigorous analysis (i.e., apparent cause). However, the SIRO can mandate a more in-depth analysis based on the circumstances of any incident. The assigned DSO is responsible for completing the requisite causal analysis and the security organization topical area lead validates the completion of the causal analysis. All completed causal analyses are required to receive a quality review by the CAO.

If an independent root cause analysis is required, an extent-of-condition evaluation and corrective action effectiveness review are also required. For all noncompliances resulting from assessment activities that involve classified information security, a root cause analysis, extent-of-condition evaluation, and corrective action effectiveness review are required. The effectiveness reviews are overseen by the security organization in cooperation with the CAO. When required, the corrective action plan includes an action for completing an effectiveness review no sooner than six months, and no later than 18 months, after completion of all other corrective actions.

Classified information security-related incidents are also entered into the SIRO database, which provides statistics detailing the overall numbers and types of incidents, as well as PD-specific statistics. The SIRO distributes monthly statistics, which include performance review statistics for senior management; trend reports; notable incidents; data on stolen badges, prohibited articles, unsecured repositories, documents, and alarm stations; and others if requested.

The regulatory assistance review team identified an increasing trend in the overall number of classified information security incidents from CY 2008 through CY 2009 and the first half of CY 2010. LLNS management and security incident personnel noted that they were aware of the increasing trend of security incidents involving the handling and storage of classified information, but they were unable to explain the cause(s) for this negative trend. Although the SIRO tracks and distributes statistical data reports regarding security incidents and the security director is briefed weekly on classified information security issues identified during assessments, only a minimal amount of analysis is performed to identify the sources or causes of identified deficiencies.

Strengths

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

- The LLNS causal analysis process is based on a well documented, graded approach and a risk-based process that determines the degree of rigor necessary to ensure timely and appropriate actions to minimize the potential for recurrence. LLNS requires training for all personnel before they are assigned as causal analysts.

- All causal analyses receive a quality review, as well as validation by the topical area SME from the security organization.

Weaknesses

- The LLNS SIRO was aware of an increased trend of security incidents in CY 2009 involving the mishandling and storage of classified information but had not yet analyzed the information to determine the cause(s) for this trend.

- The minimal analysis of data related to classified information security noncompliances identified during assessments and incidents of security concern has impacted LLNS's ability to specifically identify the sources and/or causes.

- The LLNS compliance codes currently used in ITS for classified information security noncompliances do not include the specific Departmental security policy citations related to the identified issues and are too broad to facilitate the level of trending analysis needed to assist in preventing recurrence.

V. Assessments

LLNS procedure SOM-PRO-09-005473, *Security Organization Assessment Program Procedure* (Rev. 1), dated September 21, 2009, addresses the internal self-assessments performed under the direction of the security organization to meet regulatory and contractual S&S requirements. These assessments include management self-assessments – functional areas (MSA-FAs) such as, physical security, information security, cyber security, etc., and management self-assessments – line (MSA-line assessments), including LLNS directorates.

The security organization topical area managers and directorate managers/DSOs determine what S&S topical areas will be assessed and the type of assessment that will be performed as part of its annual S&S assessment based on a graded approach and criteria. The items, services, activities, processes, systems, or programs that pose the greatest potential consequences for S&S performance, quality, and mission success within each organization are given the highest priority.

MSA-FAs are formal self-assessments, proposed by the functional area manager, to review the compliance and effectiveness of the institutional systems and processes within that functional area. The security organization topical area managers plan and schedule these assessments using a graded approach, ensuring that all applicable areas are assessed and tailoring the rigor and frequency of the assessments to meet operational needs commensurate with the level of risk to the organization. The security organization topical area managers conduct or support the assessments, ensure the preparation of assessment reports, and submit a copy of completed reports to the security organization assessment manager. The MSA-FAs are performed by an individual or a team of individuals. Assessment personnel can range from the topical area manager to members working in that topical area or other SMEs. The security organization topical area managers are responsible for entering all assessment data into ITS.

MSA-line assessments are formal self-assessments that are planned and conducted by the principal directorates (PDs). The MSA-line assessments are essentially identical to the security organization MSA-FAs in terms of planning, conduct, reporting, and tracking. Each year the security organization director specifies the number of MSA-line assessments that the PDs are required to conduct. The security organization typically specifies the subject of one or more of the assessments, and the PDs choose the subjects of the remaining assessments. The PDs may also increase the number of assessments based on perceived risk and need.

The security organization assessment manager coordinates with the security organization topical area managers and the DSOs to develop the annual assessment schedule. The schedule identifies the type of assessments, assessment scope, S&S topical area assessed, assessment tracking number, responsible individual, and frequency of the assessments to be conducted by each organization during the fiscal year. The directorate managers and the security organization topical area managers are responsible for assuring that the assessments are performed and completed as scheduled.

The security organization topical area managers and directorate managers review and approve completed assessment reports to assure that they meet the requirements of the security organization and LLNL assessment programs. Assessments are also reviewed for the appropriate depth and breadth. If the security organization assessment manager determines that the assessment report does not meet applicable requirements, it is returned to the preparing organization for improvement or referred to security organization management for other disposition.

Consistent with LLNS procedure, both the security organization and directorate personnel assigned to perform S&S assessments must possess experience, knowledge, and training commensurate with their responsibilities. The security organization assessment manager or designee schedules and conducts the security organization's assessment training course (SC-9710). To ensure that both the directorates and the security organization personnel are trained to perform S&S assessments, individuals must complete this course or work under the close supervision of personnel who are trained. Assessment reports summarize assessment activities and results, including any identified deficiencies, observations, and strengths. In addition, all deficiencies, observations, and strengths are documented in a separate "results" section of the assessment report. The security organization topical area manager or directorate manager is responsible for entering assessment results in ITS and determining the significance level of each deficiency for appropriate corrective action. However, LLNS cyber security personnel indicated that concerns resulting from intrusion detection monitoring are not captured in ITS, thus limiting the opportunity of available information when determining performance effectiveness.

The security organization topical area manager or directorate manager is responsible for tracking deficiencies to closure. When corrective actions have been completed, the security organization topical area manager or directorate manager is responsible for verifying that the deficiency has been appropriately resolved. Deficiencies that cannot be corrected by the organization that was assessed are reviewed by the security organization operations review board.

The performance management office prepares an annual report documenting the status of the LLNS S&S program. The report is prepared on a fiscal year basis or other schedule determined by LSO. In order for LSO to understand the issues or the overall health of the LLNS security program, the annual report should describe the scope/methodologies and include a narrative for all topical and/or subtopical areas. Based on discussions with LSO and a review of the FY 2009 annual report by the regulatory assistance review team, it was determined that the annual report lacked the necessary details.

Strengths

- The LLNL internal assessment program, specifically the topical/subtopical self-assessments, appear to be comprehensive and effective in providing management with feedback on the performance, quality, and compliance of the security program. All assessors receive training designed to ensure a uniform process and final product.

- Each assessment is reviewed for quality to ensure that the scope, the assessment methodologies, and the results meet expectations and that all identified issues and deficiencies are adequately documented.

- The LLNS CMPC and cyber security program personnel are well trained and knowledgeable of program responsibilities and requirements, and provide SME assistance as necessary.

Weaknesses

- The FY 2009 annual security organization assessment summary report does not provide the necessary details to fully describe the assessment scope, methodologies, and results in a manner that allows management, specifically LSO, to understand the issues or the overall health of the LLNS security program.

- The cyber security organization does not enter identified concerns from intrusion detection monitoring performance tests into ITS, thus limiting the effectiveness of trending capabilities.

VI. Conclusions

LLNS is in the initial stages of integrating security activities and 10 C.F.R. Part 824 requirements into its existing enforcement program. The LLNS enforcement coordinator has access to security incident trending data and assessment results contained in ITS and holds regularly scheduled meetings with LLNS security organization management to discuss this information. However, the roles and responsibilities of the enforcement coordinator, as they relate to security enforcement, are not yet fully formulated or formally defined and documented. Management's continued attention and commitment to the security program is crucial to successful integration of security into the LLNS existing enforcement program.

Notable strengths include the overall robust security incident program, particularly the conduct of comprehensive inquiries by knowledgeable and trained staff and the inclusion of SMEs in the categorization, inquiry, causal analysis, and corrective actions processes for security incidents. The recent use of ITS for tracking all security-related issues should improve the oversight of how identified program security weaknesses are addressed and whether implemented corrective actions are effective in minimizing the likelihood of recurrence. However, LLNS's minimal analysis of data related to classified information security noncompliances resulting from assessments and incidents of security concern hinders its ability to identify the sources and causes of recent recurring security incidents and noncompliances. In addition, the LLNS compliance codes currently used in ITS for classified information security noncompliances could be refined to specifically identify the Departmental security policy citations related to identified issues, which should also aid in reducing the likelihood of recurrence.

By addressing the weaknesses identified during this review, LLNS can 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 weaknesses should be appropriately coordinated with NNSA.

List of Acronyms

CAO	Contractor Assurance Office
C.F.R.	Code of Federal Regulations
CMPC	Classified Matter Protection and Control
CY	Calendar Year
DOE	U.S. Department of Energy
DSO	Directorate Security Officer
EPO	Enforcement Process Overview
FY	Fiscal Year
IMI	Impact Measurement Index
ISSO	Information Systems Security Officer
ITS	Issues Tracking System
LLNL	Lawrence Livermore National Laboratory
LLNS	Lawrence Livermore National Security, LLC
LSO	Livermore Site Office
MSA-FA	Management Self-Assessment – Functional Area
MSA-Line	Management Self-Assessment – Line
NNSA	National Nuclear Security Administration
OISSO	Organizational Information Systems Security Officer
PD	Principal Directorate
PSR	Program Security Representative
SAP	Special Access Program
SCI	Sensitive Compartmented Information
S&S	Safeguards and Security
SIRO	Security Incident Reporting Office
SME	Subject Matter Expert
SSIMS	Safeguards and Security Information Management System