Department of Energy
Washington, DC 20585

June 9, 2011

Dr. Charles F. McMillan
Director, Los Alamos National Laboratory and
President and Chief Executive Officer of
Los Alamos National Security, LLC
P.O. Box 1663, A100
Los Alamos, New Mexico 87545

Dear Dr. McMillan:

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 Los Alamos National Security, LLC (LANS) regulatory compliance program during the period February 28, 2011 - March 3, 2011. Our review included an evaluation of LANS processes for identifying, reporting and tracking classified information security noncompliances; LANS internal tracking systems; and processes for correcting deficiencies to prevent recurrence. The Office of Security Enforcement also conducted a limited review of LANS management and safeguards and security self-assessment programs.

Although LANS is in the early stages of integrating security activities and 10 C.F.R. Part 824 into its existing enforcement program, the Office of Security Enforcement is encouraged by the improvement initiatives related to implementation of its security regulatory compliance program. This review, described in the enclosed report, identifies strengths, as well as recommendations for improving LANS's security enforcement 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 LANS, as described in the U.S. Department of Energy's Classified Information Security Regulation (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: Kevin Smith, NNSA/LASO
Michael Lansing, LANS
Marjorie Gavett, LANS

Enclosure

OFFICE OF SECURITY ENFORCEMENT
REGULATORY ASSISTANCE REVIEW
LOS ALAMOS NATIONAL SECURITY, LLC

I. Introduction

During February 28 – March 3, 2011, 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 Los Alamos National Security, LLC (LANS). 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 LANS processes for identifying classified information security noncompliances; reporting and tracking classified information security noncompliances in the Safeguards and Security Information Management System (SSIMS); using LANS internal deficiency tracking/trending systems; and correcting deficiencies to prevent recurrence. It also included a limited review of LANS management and safeguards and security (S&S) internal assessment programs and an evaluation of LANS efforts to integrate its classified information security enforcement 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 (PAAA) and worker safety and health (WSH) enforcement programs (hereinafter collectively referred to as the enforcement program).

The Office of Enforcement issued a security enforcement letter to LANS 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 LANS management, in coordination with the Los Alamos Site Office (LASO), addressed the issues identified in the security enforcement letter in parallel with the corrective actions that had already been identified as a result of the July 2007 LANS compliance order. Based on discussions with both LASO and LANS management, improvements have been made related to the issues identified in the security enforcement letter.

At the time of this review, LANS was in the process of implementing improvement initiatives within its enforcement program for classified information security. These initiatives are discussed throughout this report. In addition, this review identified strengths, as well as recommendations regarding the effectiveness of the LANS enforcement 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 improving the overall security program are evident, as exemplified, in part, by the appointment of two security representatives to serve as liaisons between the LANS security programs and the enforcement program. In addition, LANS management continues to support the reduction of classified storage areas (e.g., vault-type rooms), as well as reducing the number of classified holdings.

- There is an effective partnership and lines of communication between the LANS security organization (including classified cyber security), the LANS enforcement program, and LASO.

- LANS security personnel within the security incident team (SIT), classified matter protection and control (CMPC), classified cyber security, self-assessment, and corrective action management programs appeared well trained and knowledgeable of their program responsibilities and the regulatory and policy requirements.

- The LANS CMPC program conducts monthly CMPC training that is open to all employees, but mandatory for classified matter custodians. In addition, the LANS CMPC program conducts a training effectiveness evaluation 180 days after the training.

- LANS has an active security awareness program that provides timely and meaningful information and lessons learned on classified information security topics and requirements.

- The LANS security program has embedded in each Laboratory directorate security representatives, known as deployed security officers (DSO), whose responsibilities include addressing security problems and providing security support to line management.

- LANS conducts thorough security incident inquiries and produces well-documented inquiry reports.

- LANS has developed an automated tracking system, the Performance Feedback and Improvement Tracking System (PFITS), which captures S&S noncompliances identified during internal and external assessments. PFITS was designed to ensure the evaluation, resolution, closure, reporting, and trending of S&S-related issues.

- The LANS internal assessment/review process performed by the CMPC program is comprehensive and effective in terms of performance and quality.

Recommendations

- Continue the current efforts to integrate 10 C.F.R. Part 824 into the existing LANS enforcement program and formally define and document the associated roles and responsibilities.

- Continue the current efforts to formally document the applicable requirements identified in 10 C.F.R. Part 824 in all LANS security procedures, enforcement program procedures, and local training that addresses classified information security topics.

- Evaluate current processes for determining the appropriate Impact Measurement Index (IMI) categorization. Some recent security incidents appeared to have been categorized at a lower IMI level because the possibility of a suspected or potential compromise of classified information was ruled out without documenting the requisite supporting evidence. In addition, some security incidents were categorized using a locally defined "sub-reportable" category, even though they appear to have met the established IMI categorization and reporting requirements.

- Continue the recent (i.e., February 2011) efforts on training relative to the institutionalized methods and requirements for conducting causal analyses.

- Conduct further analysis of data related to classified information security noncompliances identified during incidents of security concern and assessments would provide additional insights in identifying root causes and subsequent corrective actions to prevent recurrence.

- Provide a roll-up of all assessment activities and the associated results, conducted Laboratory-wide throughout the fiscal year (FY), should be reflected in the LANS end-of-year report as a means to meet the objective of the self-assessment requirements.

II. General Program Implementation

This review found that LANS is in the early stages of implementing its initiatives to formally integrate the security enforcement function, as defined by 10 C.F.R. Part 824, into the LANS enforcement program to include the enforcement screening of all classified information security noncompliances. Notwithstanding, the review team observed a close and effective working relationship among LANS enforcement program personnel, representatives of the S&S program, and LASO.

LANS has recently appointed two security representatives, one in physical security and another in cyber security, to serve as liaisons with the LANS enforcement program. One of their roles is to screen classified information security noncompliances. The LANS security enforcement screening tool, *Self Assessment Screening Checklist for Security*

SSIMS Reporting, and the associated procedure, *Security 10CFR824 Screening Process,* dated December 9, 2010, contain specific information for determining when noncompliances should be voluntarily entered into SSIMS. The criterion used is consistent with the thresholds established in the EPO for voluntary reporting of classified information security noncompliances. However, this tool does not provide any information on identifying noncompliances as defined in Departmental classified information security policies, including the Incidents of Security Concern (IOSC) policy, that require mandatory reporting. As a result, the tool limits security enforcement program screening to self-assessment results, rather than addressing all classified information security noncompliances, including those identified as a result of incidents of security concern or noncompliances identified by external assessments (e.g., security surveys, Independent Oversight inspections, Inspector General and General Accounting Office investigations). LANS recognizes the need to update its program implementation documents to reflect current practices, including the recent changes in its security enforcement screening process.

The review team suggested that LANS include a mechanism in both the Integrated Security Issues Tracking System (ISITS) and PFITS to identify specific noncompliances that require security enforcement screening and cite the specific Departmental policy for each identified noncompliance regardless of the source (e.g., security incidents/events, internal/external assessments, investigations). The review team has made similar suggestions during past regulatory assistance reviews at other U.S. Department of Energy (DOE)/National Nuclear Security Administration (NNSA) sites and referred LANS to other sites/locations that are further along in implementing this type of regulatory screening process.

The LANS enforcement program has established a training course relevant to all three enforcement program disciplines, including classified information security. The course, *Course #47656, PAAA, WSH, and Information Security Overview Self-Study*, is a web-based self-study course that all Laboratory managers must complete within one year of assignment to a management position. This course is in the process of being updated to address LANS's classified information security enforcement program and 10 C.F.R. Part 824 requirements. The course, *Course #18653, PAAA Facility Price-Anderson Amendments Act Coordinator Training*, has been updated to address LANS's classified information security enforcement program and 10 C.F.R. Part 824 requirements. LANS cyber security personnel indicated that the annual cyber security training also includes information relevant to 10 C.F.R. Part 824 requirements. However, the review team determined that other local security training relevant to the protection and control of classified matter (e.g., comprehensive security briefing, CMPC training, annual security refresher training) has not been updated to include 10 C.F.R Part 824 requirements.

LANS and LASO management emphasized their ongoing efforts to consolidate and reduce the classified information footprint at the Laboratory. LANS has successfully reduced the number of vault-type-rooms, classified holdings, and classified accountable matter. The cyber security program has also implemented diskless workstations, as appropriate, across the Laboratory. Furthermore, this review found that LANS classified assets are controlled by trained and knowledgeable CMPC custodians. The LANS CMPC program personnel conduct a two-day CMPC training session on a monthly basis. This training is mandatory for all CMPC custodians, but any LANS employee may attend. In addition to the mandatory training for CMPC custodians, the CMPC program personnel conduct an effectiveness evaluation of each custodian 60 to 90 days after each training session. The personnel responsible for teaching this course have completed basic instructor training from DOE's National Training Center. In addition to providing training in specific security topical areas, LANS has an active security awareness program. For example, LANS includes information from assessment activities, reported security incidents, and help desk calls in its Laboratory-wide publications, such as *Security Smarts* and *Anatomy of an Incident.*

The LANS S&S directorate has embedded DSOs within each of the LANS associate directorates across the Laboratory. Although each DSO is funded by the receiving associate directorate, the S&S directorate manages the daily activities of the DSO staff for the Laboratory. The DSOs are responsible for providing security-related guidance to their associate directors, solving security problems for line management, and remaining cognizant of NNSA and Laboratory security requirements. The S&S directorate's management of the DSO staff has contributed to the consistent implementation of security requirements associated with the protection and control of classified matter across all LANS directorates. Additionally, the review team's discussions with LANS security personnel responsible for the protection and control of classified matter showed that they were all well-trained and knowledgeable of their program responsibilities and the regulatory and policy requirements. The program areas of identification and reporting of incidents of security concern, issues management and trending, and assessments are discussed in sections III-V below.

Strengths

- Management attention and commitment to improving the overall security program are evident, as exemplified, in part, by the appointment of two security representatives to serve as liaisons between the LANS security programs and the enforcement program. In addition, LANS management continues to support the reduction of classified storage areas (e.g., vault-type rooms), as well as reducing the number of classified holdings.

- There is an effective partnership and lines of communication between the LANS security organization (including classified cyber security), the LANS enforcement program, and LASO.

- LANS security personnel within the SIT, CMPC, classified cyber security, self-assessment, and corrective action management programs appeared well trained and knowledgeable of their program responsibilities and the regulatory and policy requirements.

- The LANS CMPC program conducts monthly CMPC training that is open to all employees, but mandatory for classified matter custodians. In addition, the LANS CMPC program conducts a training effectiveness evaluation 180 days after the training.

- LANS has an active security awareness program that provides timely and meaningful information and lessons learned on classified information security topics and requirements.

- The LANS security program has embedded in each Laboratory directorate security representatives, known as DSOs, whose responsibilities include addressing security problems and providing security support to line management.

Recommendations

- Continue the current efforts to integrate 10 C.F.R. Part 824 into the existing LANS enforcement program and formally define and document the associated roles and responsibilities.

- Continue the current efforts to formally document the applicable requirements identified in 10 C.F.R. Part 824 in all LANS security procedures, enforcement program procedures, and local training that addresses classified information security topics.

III. Identification and Reporting of Incidents of Security Concern

Los Alamos National Laboratory (LANL) procedure P201-3, *Reporting Known and Potential Incidents of Security Concern* (revision 0), dated June 3, 2009, establishes the requirements for Laboratory workers to report known and potential IOSCs to the SIT. Specifically, this procedure covers requirements for the identification and reporting of IOSCs that may involve classified matter, computer systems, secure communications, and physical security occurring at the Laboratory.

The SIT is the single point of contact for reporting all incidents of security concern at LANL. Any person who identifies a potential security incident must immediately notify the SIT. If the incident is identified outside of normal hours of operation, workers must immediately report it to the ADSS on-call duty officer. In addition, the worker must notify the responsible line manager or a designated alternate. The line manager ensures that the SIT has been notified and is responsible for immediately reviewing reports of IOSCs to identify and mitigate potential vulnerabilities. In addition, reporting an information security incident mobilizes an incident response by the information security operations center (iSOC). The iSOC works with various Laboratory teams that cooperate as members of the iSOC to ensure the accurate notification, response, management attention, prevention, and investigation of classified information incidents. If necessary, the iSOC can mobilize other functions, such as the computer security incident response team and the vulnerability analysis group.

Both the iSOC and the SIT are responsible for categorizing security-related incidents in accordance with the criteria established by DOE/NNSA and for reporting both internally and externally within required time frames. The SIT maintains internal procedures for categorizing and reporting for the Laboratory IOSC program in accordance with DOE Manual 470.4-1, Chg. 1, Part 2, Section N, and the iSOC maintains internal procedures for categorizing and reporting cyber-related incidents in accordance with NNSA Policy Letter (NAP)-14-B.

At the time of this review, the LANS SIT program consisted of eight inquiry officials. Discussions with SIT representatives indicated that incidents are reported by Laboratory personnel either by calling or visiting the SIT office. The inquiry official who takes the call or the report is responsible for handling the initial actions, which include, as appropriate, responding to the incident location, determining and isolating any vulnerability that may exist, initiating necessary compensatory measures, and starting the inquiry process. The SIT team lead is responsible for determining, within 24 hours, the initial IMI categorization of IOSCs, using the IMI tables contained in DOE Manual 470.4-1, Chg. 1, Part 2, Section N, as a basis. LANS has established a local incident category, "sub-reportable," to account for incidents that the SIT team lead considers not to meet the established IMI reportable categories.

The review team evaluated 20 security incident files and 14 sub-reportable security call assessment records (SCAR) from the past two years. The security incident files were well organized and the inquiry reports were well written and contained detailed information on the facts and circumstances involving the reported security incident. However, some cases lacked the evidence to support the assigned IMI category, particularly in ruling out the potential or suspected compromise of classified information. In other cases, IOSC policy requirements, specifically incident categorization requirements, were not met, nor was the required policy deviation process followed. The review team found that all 14 of the sub-reportable incidents involved noncompliance with DOE/NNSA S&S policies and procedures. Based on the information provided on the SCARs, the review team determined that seven of these sub-reportable incidents (50 percent of those reviewed) lacked the requisite supporting evidence (i.e., mitigating factors) for eliminating the potential for compromise and therefore met the IMI reporting criteria.

Strength

- LANS conducts thorough security incident inquiries and produces well-documented inquiry reports.

Recommendation

- Evaluate current processes for determining the appropriate IMI categorization. Some recent security incidents appeared to have been categorized at a lower IMI level because the possibility of a suspected or potential compromise of classified information was ruled out without documenting the requisite supporting evidence. In addition, some security incidents were categorized using a locally defined "sub-reportable" category, even though they appear to have met the established IMI categorization and reporting requirements.

IV. Issues Management and Trending

LANS uses SSIMS to report and track its security incidents. In addition to SSIMS, LANS also uses ISITS, which is the SIT IOSC unclassified database. LANS has also developed a classified version of the ISITS database to track classified security incidents and other classified noncompliances. ISITS is essential to the SIT operation as it is the foundation for all IOSC notifications and the repository for all supporting data gathered during an inquiry. SIT also uses the ISITS database to produce trending reports, many of which are produced and distributed on a routine basis. For example, an IOSC periodic update with IMI information is transmitted to DOE, NNSA, group leads, team leads, and ADSS on a monthly basis. Incident data slides and handouts are also produced for the bi-weekly security integration board (SIB) meetings. The review team found ISITS to be a robust case management tool capable of producing IOSC trending reports.

LANL procedure P322-4, *Laboratory Performance Feedback and Improvement Process,* (revision 6), dated June 4, 2010, was designed to provide flexibility by defining alternative approaches to collect, evaluate, and address positive and negative performance feedback. This process defines four improvement approaches: (1) issues and corrective action management (ICAM), used for high-risk issues that do not meet documented requirements and result in a significant risk to performance; (2) performance improvement action tracker, used for tracking issues to closure that do not require the level of rigor of ICAM; (3) other improvement actions, used to document issues that are being handled by the Laboratory's improvement processes; and (4) management action, used to track issues requiring the lowest level of rigor where action tracking does not add value or the actions are being tracked in another system. Each LANS organization has an established management review board (MRB) that reviews and approves resolution of performance feedback. Performance feedback of cross-cutting institutional significance is managed by the institutional management review board. The MRB reviews performance feedback and selects the appropriate performance improvement approach based on the identified risk level. The ICAM process is used for risk level 1 and 2 (i.e., feedback that meets the criteria for an issue). Based on discussions with LANS security personnel, most classified information security issues are identified as risk level 2. The ICAM process for risk level 2 requires a causal analysis, corrective actions, effectiveness evaluation, and MRB review for issue closure.

LANS also uses PFITS, which manages Laboratory performance feedback and is an integral part of the contractor assurance system. PFITS is used, in part, to track noncompliances that result in a risk to performance, findings and deficiencies from internal/external assessments or audits, and management observations/verifications. Opportunities for improvement (OFI), noteworthy practices, and recommendations are not required to be entered into PFITS. However, management may enter them to track associated corrective actions or for trending purposes. PFITS cannot be used for classified information, so LANS uses the classified ISITS for any noncompliances that contain classified information, with a place holder in PFITS pointing to ISITS. PFITS appears to be an effective tool for the evaluation, resolution, closure, reporting, and trending of S&S-related issues.

LANL procedure P322-1, *Causal Analysis and Corrective Action Development,* (revision 2) dated November 30, 2010, establishes a systematic and disciplined approach to conducting a causal analysis and developing an associated corrective action plan (CAP). The procedure provides managers and causal analysts with a structured approach for determining the level of rigor to be applied to an analysis, developing corrective actions, and documenting the analysis and actions. The LANS process for determining the level of rigor (i.e., high, moderate, or low) requires information about three variables: probability, consequences, and complexity. For classified information security noncompliances, the highest level of rigor is applied to IMI-1 security incidents, risk level 1 issues in PFITS, and significant findings from external oversight reviews. A moderate level of rigor is typically applied to IMI-2 security incidents and risk level 2 issues in PFITS. Other noncompliances and events receive a causal analysis, but with less-extensive dedicated resources and time. The procedure contains a list of many different tools and techniques that causal analysts may apply. However, although LANS has established a graded approach for determining the risk associated with an issue and the level of rigor to be applied to analysis and corrective action based on that risk, LANS has not established a method for selecting the appropriate causal analysis tool for use in a specific case. Discussions with corrective action management personnel indicated that LANS recognizes this concern and is developing a standardized approach for conducting causal analyses and training causal analysts.

The review team identified an increasing trend in the overall number of classified information security incidents in calendar year 2010, possibly because LANS SIT personnel began entering IMI-4 security incidents in SSIMS during FY 2010. (Departmental policy does not require IMI-4 security incidents to be entered into SSIMS as individual incidents, but does not prohibit it). The review team encouraged the continued use of SSIMS for reporting all classified information security incidents as a means of transparency. The review team found that the SIT and other ADSS organizations track and distribute statistical data reports regarding security incidents and other security noncompliances. In addition, LANS management has established the SIB that meets on a monthly basis to share security-related information and issues and to discuss security performance metrics. Although valuable performance information is discussed and shared at these meetings, only a minimal amount of analysis is performed to identify the sources or root causes of deficiencies and noncompliant conditions. For example, classified information security incidents may be more prevalent in a single LANS directorate, or many incidents may deal with a particular classification guide. In addition, analysis may identify a need for engineered solutions that could improve performance and prevent recurrence better than administrative controls.

Strength

- LANS has developed an automated tracking system, PFITS, which captures S&S noncompliances identified during internal and external assessments. PFITS was designed to ensure the evaluation, resolution, closure, reporting, and trending of S&S-related issues.

Recommendations

- Continue the recent (i.e., February 2011) efforts on training relative to the institutionalized methods and requirements for conducting causal analyses.

- Conduct further analysis of data related to classified information security noncompliances identified during incidents of security concern and assessments would provide additional insights in identifying root causes and subsequent corrective actions to prevent recurrence.

V. Assessments

LANL desktop procedure, *Security & Safeguards Directorate's Self Assessment and Resolution of Findings* (version 7.0), dated June 1, 2008, establishes a consistent methodology for the self-assessment team to conduct topical and subtopical security assessments within ADSS. According to this procedure, its implementation by ADSS meets the Department's self-assessment criteria as set forth in DOE Manual 470.4-1, Chg. 1. This procedure provides a detailed process for the robust review of all applicable DOE Form 470.8 topical and subtopical areas. Cyber security and counterintelligence program responsibilities are not within the direct control of ADSS, so those organizations conduct their own self-assessments and submit copies to ADSS for inclusion in the LANS annual assessment report.

Before October 1 of each calendar year, the self-assessment team leader coordinates the development of the self-assessment schedule in conjunction with the self-assessment team members and the responsible topical/subtopical area group leaders/subject matter experts (SME). The ADSS managers assign a self-assessment team lead for each of the self-assessments under their purview and ensure that the team lead is familiar with and works in accordance with the procedure. The accuracy and completeness of the self-assessment depend on the preparation before the self-assessment begins (e.g., review of previous audits/surveys/assessments, including previous findings, OFIs, CAPs, and trending data). The associate director and/or the MRB routinely direct effectiveness evaluations to be conducted for certain closed CAPs to ensure program effectiveness. SMEs lead the self-assessment process with the assistance and observation of the self-assessment team lead. Data is collected through document reviews, interviews, performance testing, and direct observation of operations. The team develops the self-assessment report and issues findings, OFIs, and best management practices. The self-assessment team lead is responsible for ensuring that the self-assessment data is reviewed for any potential enforcement issues. LASO is invited to participate in any part of the self-assessment process.

The self-assessment procedure identifies a finding as an issue in which identified deficiencies in the performance of ADSS responsibilities results in noncompliance or inadequate performance relative to DOE directives and/or LANL policies/procedures that may cause a severe risk to national security. OFIs are less-severe issues that do not warrant a finding or require a formal CAP. OFIs are also items that do not violate a requirement but are provided for management consideration as program enhancements. Best management practices, as stated in the procedure, should be identified and documented for the benefit of other ADSS entities.

The review team looked at the topical and subtopical area assessments conducted by ADSS in FY 2010 that included classified matter protection and control. The S&S self-assessment program FY 2010 end-of-year report was also reviewed. This particular report contains a brief executive summary, short summaries/synopses of each applicable topical and subtopical area reviewed, and a listing of findings and OFIs. The report is provided to LASO to meet the requirement to conduct an annual S&S self-assessment pertaining to the overall health of the Laboratory's S&S program. Discussions with LANS assessment personnel showed that the topical area and FY end-of-year reports reflect the S&S activities only within the ADSS; they do not address S&S activities within the other Laboratory directorates. Consequently, the LANS FY end-of-year reports do not provide the necessary details to fully describe the assessment scope, methodologies, and results in a manner that allows management, including LASO, to understand Laboratory-wide issues or the overall health of LANS's security program.

The LANS cyber security program is not part of the ADSS organizational structure and thus is not included in the formal S&S self-assessment program. Based on discussions with cyber security program management, the review team noted that the cyber security self-assessment program has been in a continuous improvement mode for the past few years. Review of recent cyber security self-assessment reports found that these assessments were more comprehensive than in the past, and included the review of all applicable Laboratory directorates. Although this recent assessment process is in the early stages of development, cyber assessment personnel have been appropriately trained and are aware of the areas needing improvement.

The review team also found that the CMPC program conducts reviews/evaluations of CMPC program implementation across the Laboratory. Although LANS has not considered these CMPC assessments to be part of the LANS S&S self-assessment program, they are based on LANL procedure PS1-GP-022, *Classified Matter Protection and Control Team, Self-Assessment Procedure and Process Documentation* (version 6), dated July 13, 2010. The CMPC assessment reports were found to be comprehensive and effective in performance and quality. Further discussions with LANS personnel found that LANS had recognized the need to include these assessments and associated results in future FY end-of-year assessment reports.

Strength

- The LANS internal assessment/review process performed by the CMPC program is comprehensive and effective in terms of performance and quality.

Recommendation

- Provide a roll-up of all assessment activities and the associated results, conducted Laboratory-wide throughout the FY, should be reflected in the LANS end-of-year report as a means to meet the objective of the self-assessment requirements.

VI. Summary

LANS continues to further integrate security activities and 10 C.F.R. Part 824 requirements into its existing enforcement program. The LANS enforcement program personnel have access to security incident trending data and self-assessment results. In addition, LANS has appointed two security representatives to serve as a conduit between the security program and the enforcement program. However, the enforcement and security program implementation documents do not reflect these current practices, including the recent changes in the screening process. Management's continued attention and commitment to the security program are crucial to successfully completing the ongoing integration of security into the LANS existing enforcement program.

Notable strengths include the overall robust security incident program, particularly the conduct of comprehensive inquiries by knowledgeable and trained staff. The use of ISITS and PFITS for tracking security-related issues and the oversight provided for corrective actions associated with identified program security weaknesses are effective in minimizing the likelihood of recurrence. However, LANS'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 or root causes of all identified deficiencies. Due to the limited scope of the S&S self-assessment program, the FY 2010 end-of-year report does not provide the necessary details to fully describe the assessment scope, methodologies, and results in a manner that allows management, including LASO, to understand Laboratory-wide issues and the overall health of the LANS security program.

By appropriately addressing the recommendations identified during this review, LANS 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 NNSA.

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

- Include OFIs and on-the-spot corrections that are identified during assessments in the overall tracking and trending process.

- Use the available process in SSIMS for reporting self-identified issues as described in the EPO, specifically programmatic and repetitive concerns.

- Incorporate CMPC and cyber security assessment activities as part of the overall LANS S&S self-assessment program.

- Improve timeliness in closing all security incidents to ensure that valuable lessons-learned data is not lost.

- Include a mechanism in ISITS and PFITS to identify which noncompliances require security enforcement screening, and provide the policy citations for each noncompliance to aid in trending and analysis.

List of Acronyms

ADSS	Associate Directorate for Safeguards and Security
CAP	Corrective Action Plan
CMPC	Classified Matter Protection and Control
DOE	U.S. Department of Energy
DSO	Deployed Security Officer
EPO	Enforcement Process Overview
FY	Fiscal Year
ICAM	Issues and Corrective Action Management
IMI	Impact Measurement Index
IOSC	Incident of Security Concern
ISITS	Integrated Security Issues Tracking System
iSOC	Information Security Operations Center
LANL	Los Alamos National Laboratory
LANS	Los Alamos National Security, LLC
LASO	Los Alamos Site Office
MRB	Management Review Board
NNSA	National Nuclear Security Administration
OFI	Opportunity for Improvement
PAAA	Price-Anderson Amendments Act
PFITS	Performance Feedback and Improvement Tracking System
S&S	Safeguards and Security
SCAR	Security Call Assessment Record
SIB	Security Integration Board
SIT	Security Incident Team
SME	Subject Matter Expert
SSIMS	Safeguards and Security Information Management System
WSH	Worker Safety and Health