Doc. No. 1
MEMORANDUM FOR CAMILLE C. YUAN-SOO HOO
MANAGER
LIVERMORE SITE OFFICE

FROM: BRADLEY A. PETERSON
DIRECTOR
OFFICE OF INDEPENDENT OVERSIGHT
OFFICE OF HEALTH, SAFETY AND SECURITY


The Office of Independent Oversight, within the Office of Health, Safety and Security, will conduct an inspection of safeguards and security and cyber security topical areas at the Livermore Site Office and the Lawrence Livermore National Laboratory, during the period of March-April 2008. The inspection plan for this activity is attached.

The inspection schedule is as follows. The full team will conduct planning and onsite data collection visits from March 10-14, 2008, and March 31-April 4, 2008, respectively. Final data collection activities, performance testing, and close-out activities are scheduled for April 14-25, 2008. Please note that we will continue to refine our inspection focus areas to ensure that we adequately address those areas that are of specific interest to you and key Headquarters managers. This inspection plan includes information on the scope of the inspection, lines of inquiry for safeguards and security and cyber security topical areas, and team composition.

Should you need additional information, please contact Steve Yonkoff, Deputy Director, Office of Security Evaluations and the inspection team leader, at (301) 903-5895. Alternatively, your staff may contact John Boulden, Acting Director, Office of Cyber Security Evaluations and the cyber security team topic lead, at (301) 903-0324.

Attachment
cc:  Thomas D'Agostino, NA-1
    William Ostendorff, NA-1
    Glenn Podonsky, HS-1
    Michael Kilpatrick, HS-1
    Bradley Peterson, HS-60
    Bill Eckroade, HS-61
    John Boulden, HS-62
    Thomas Pyke, IM-1
    Rolf Mowatt-Larssen, IN-1
    William Hunteman, IM-30
    William Desmond, NA-1
    Robert Brese, NA-1
    Robert Smolen, NA-10
    Linda Wilbanks, NA-65
    Wayne Jones, NA-65
    Cheryl Stone, NA-70
    Duane Gordon, LSO
Plan for the Safeguards and Security and Cyber Security of the Livermore Site Office and the Lawrence Livermore National Laboratory

March-April 2008

U.S. Department of Energy
Office of Health, Safety and Security
Office of Independent Oversight
DEPARTMENT OF ENERGY
OFFICE OF HEALTH, SAFETY AND SECURITY
OFFICE OF INDEPENDENT OVERSIGHT
PLAN FOR THE SAFEGUARDS AND SECURITY AND
CYBER SECURITY INSPECTION OF THE
LIVERMORE SITE OFFICE AND THE LAWRENCE LIVERMORE NATIONAL
LABORATORY

March 10 – April 25, 2008

Approved by: _______________________________ Date: _______________________________
William A. Eckroade, Director
Office of Security Evaluations
Office of Independent Oversight

Approved by: _______________________________ Date: _______________________________
John S. Boulten III, Acting Director
Office of Cyber Security Evaluations
Office of Independent Oversight

Approved by: _______________________________ Date: _______________________________
Bradley A. Peterson, Director
Office of Independent Oversight
Office of Health, Safety and Security
I. INTRODUCTION

This document outlines activities currently planned by the Office of Independent Oversight, within the Office of Health, Safety and Security, for evaluating line management of safeguards and security and cyber security at the Lawrence Livermore National Laboratory (LLNL). Additionally, Independent Oversight will inspect activities at the Livermore Site Office (LSO) that directly support LLNL security programs. Inspection activities will be conducted according to the Department of Energy (DOE) Order 470.2B, Independent Oversight and Performance Assurance Program, which establishes the foundation for the evaluation of program effectiveness. While this plan outlines projected evaluation activities, it should be understood that changes to specific activities and inspection focus areas will be made in response to emerging concerns and requests from key LSO, LLNL, and Headquarters managers. Site representatives will be kept informed of significant changes in proposed activities and inspection focus areas.

II. SCHEDULE

In order to minimize impact to LLNL, emphasis is placed on limiting the onsite evaluation efforts to only those activities that cannot be accomplished at Headquarters. The Headquarters planning stage includes line management interviews, documentation review, team orientation, and performance test coordination.

The full inspection team will participate in an onsite planning visit from March 10-14, 2008, during which time initial data gathering will also occur. Primary data collection activities, to include interviews, document and record reviews, limited scope performance testing, and other performance observations, will be conducted during the periods of March 31-April 4. Other inspection activities, including large-scale force-on-force performance tests, final data collection, validating inspection results, conducting factual accuracy reviews, finalizing a draft report; and conducting close-out activities, will be conducted during the period April 14-25, 2008. At the completion of the onsite inspection a draft report will be issued and key managers and senior staff will be briefed on the inspection results consistent with Independent Oversight protocols.
III. INSPECTION TEAM RESPONSIBILITIES AND ASSIGNMENTS

Steve Yonkoff, Deputy Director, Office of Security Evaluations, will be the senior DOE official managing the evaluation activities as the inspection leader and also the senior Independent Oversight point of contact. He will be assisted by a deputy inspection team leader, technical specialists, and administrative support personnel. The inspection leader and his staff will ensure evaluation activities are conducted in accordance with approved procedures. Team members and their assigned topical disciplines are outlined below.

The evaluation team will be subdivided into subject areas. These areas will include Protection Program Management (PPM), Classified Matter Protection and Control (CMPC), Personnel Security (PS), Physical Security Systems (PSS), Protective Force (PF), Material Accountability and Control (MC&A), Classification and Information Control (CIC), and Classified and Unclassified Cyber Security. In addition, the sensitive compartmented information facility at LLNL will be inspected. This activity will be coordinated directly with the Office of Intelligence and Counterintelligence and handled separate from other inspection activities.

DOE Order 470.2B assigns responsibility to the Heads of Field Elements to assist Independent Oversight in performing an effective and valid evaluation. This responsibility includes the provision of (1) access and support, (2) points-of-contact, and (3) validation of the factual content of the inspection data and report.

IV. INSPECTION PROCESS

Independence

Independent Oversight is charged with the independent oversight of safeguards and security; cyber security; emergency management programs; and environment, safety, and health throughout the Department. Independence is assured by a direct reporting relationship to the Secretary of Energy (i.e., outside any line management reporting chain) through the Chief, Health, Safety and Security Officer. Further, Independent Oversight does not have any direct responsibility for facility operations, protection program management, information systems management, or policy formulation.

Independent Oversight exercises independence in the conduct of inspections. Scheduling of inspections is independent of line management although valid concerns of site and DOE management are accommodated, whenever possible. Evaluations are based upon performance based assessments of how sites implement the requirements established in DOE orders and directives with an emphasis on the effectiveness of the program elements. Independent Oversight also provides feedback on the effectiveness of orders and directives and whether they adequately establish effective program requirements. Consequently, Independent Oversight will employ the professional judgment of experienced inspectors to
provide an overall evaluation of safeguards and security, and cyber security program status, including the impact of orders and directives governing implementation.

**Emphasis on DOE Line Management and Self-Assessment Processes**

The primary purpose of Independent Oversight's assessment activities is to provide timely information to the Secretary of Energy and other senior Departmental Managers on the status of Departmental safeguards and security; cyber security; emergency management; and environment, safety, and health programs. This information must be presented in a manner that supports and facilitates Secretarial-level actions to address identified shortcomings. Therefore, an emphasis is placed on evaluating management performance, particularly DOE management direction and guidance for program implementation. Evaluation of the adequacy of DOE and contractor management assessment and self-assessment processes (feedback and improvement) is an important aspect of Independent Oversight's emphasis on management effectiveness, and is thus a major focus of the inspection. At the same time, the most fundamental management performance measure is the extent to which programs are effectively implemented. Thus, a central feature of Independent Oversight's inspections is the consideration of program effectiveness through performance testing, performance observations, and analysis of program documentation. While Independent Oversight's assessments provide a "snapshot in time" of performance, the analysis of inspection results will highlight program trends and provide evidence of progress or decline in overall performance, whenever such trends and evidence are discernable.

**"Top-Down" Approach**

Independent Oversight's role is not to duplicate surveys and assessments of safeguards and security, cyber security, emergency management, and environment, safety, and health topics that are conducted by other organizations. Rather, Independent Oversight's role is to provide an independent review of program effectiveness, which gives line management essential feedback on program status and direction. This leads to a "top-down" approach to evaluation planning that focuses on overall program effectiveness across the breadth of the program. However, as part of this approach, Independent Oversight recognizes the need to conduct carefully targeted, in-depth reviews of particular aspects of program implementation to effectively evaluate performance. Independent Oversight inspections are designed to balance the need for breadth and depth.

**V. SCOPE OF THE EVALUATION**

The Independent Oversight inspection will evaluate performance of line management responsible for safeguards and security, and cyber security programs at LSO and LLNL.

The major focus of the safeguards and security portion of the assessment is the evaluation of measures in place for the physical protection of special nuclear materials. Independent Oversight will pay particular attention to the effectiveness of LLNL management in comprehensively and systematically addressing actions needed to correct findings identified during special reviews, surveys, self-assessments, and inspections.
As part of its overall program of protective force performance tests, Independent Oversight will conduct a series of large-scale force-on-force tests designed to generate data with respect to individual and team tactical performance, command, control, communications, and other aspects of tactical response. Independent Oversight conducts such performance tests against the terrorist adversary capability defined by the DOE Design Basis Threat (DBT). Independent Oversight recognizes that the Department is in a transitional status with respect to the DBT policy. Accordingly, force-on-force performance tests will be conducted in accordance with the applicable Design Basis Threat (DBT) Policy and Secretarial directives as documented in the Site Safeguards and Security Plan (SSSP) and approved site DBT implementation planning documentation.

The inspection will also assess the protection that LLNL provides to classified and sensitive unclassified information. As part of the safeguards and security portion of the assessment, the following topical areas will be evaluated by Independent Oversight:

- Program Protection Management
- Classified Matter Protection and Control
- Classification and Information Control
- Personnel Security
- Physical Security Systems
- Protective Force Program
- Force-on-Force Performance Testing
- Material Control and Accountability

The cyber security evaluation team will assess the overall effectiveness of classified and unclassified cyber security at LSO and LLNL. The cyber security evaluations will feature a combination of comprehensive penetration testing and a review of programmatic elements essential to an effective program. Testing will include scanning for vulnerabilities using various tools and penetration testing from within the network (representing a malicious insider or adversary that has gained access to the internal network) and external to the network (representing external attackers). All penetration testing will be coordinated and performed in accordance with a technical assessment protocol document signed by Independent Oversight and LSO authorized representatives that define the governing rules. The programmatic portion of the evaluation includes evaluation of management, operational and technical controls.

A common emphasis for the safeguards and security and cyber security evaluations will be the performance of DOE line management, both in the field and at Headquarters, and also the effectiveness of feedback and improvement mechanisms such as surveys and self-assessments and their associated corrective action mechanisms. Although the focal point for reporting results in these areas will be the Protection Program Management appendix of the inspection report, this emphasis will incorporate data collection across all topical areas.

The inspection will be conducted according to formal protocols and procedures described in the Office of Independent Oversight and Performance Assurance Appraisal Process
Protocols. This document provides the general framework for the work processes used by Independent Oversight for conducting inspections. This general framework will be further supplemented by a variety of subordinate protocol documents including office-specific appraisal process guides, Independent Oversight's Context and Protocols for Performance Testing of Protective Forces and its Composite Adversary Team Standard Operating Procedure, as well as the relevant topical inspector's guides.

This plan outlines the overall scope and conduct of the inspection. Team members will develop individual schedules of onsite activities that supplement this overall plan. Appendix C contains detailed topical area scope and lines of inquiry.

VI. EVALUATION SAFETY

Independent Oversight considers safety to be of primary importance in all inspection activities. Special emphasis is placed on the safe conduct of safeguards and security performance tests, particularly force-on-force performance testing and protective force limited scope performance tests. All performance tests will be carefully planned to minimize safety risks while achieving acceptable levels of realism. The performance test safety planning process includes a determination of potential safety hazards associated with anticipated performance tests and, where indicated, the preparation of written performance test safety plans designed to address these potential hazards. All routine evaluation activities will be conducted in accordance with LLNL safety procedures.
Livermore Site Office and the Lawrence Livermore National Laboratory
Inspection Schedule

Planning and Data Collection Visit – March 9-14, 2008

March 9, 2008
Team Members Travel

March 10, 2008
7:30 a.m. – 8:30 a.m.
Badging
8:30 a.m. – 9:30 a.m.
In-Brief (proposed)
9:30 a.m. – 10:30 a.m.
Training (proposed)
10:30 a.m. – 5:00 p.m.
Planning, Data Collection, Document Review and Interviews

March 11-13, 2008
7:30 a.m. – 5:00 p.m.
Planning, Data Collection, Document Review and Interviews
5:00 – 6:00 p.m.
Team Meeting

March 14, 2008
Team Members Travel Home

Data Collection Visit – March 31 – April 4, 2008

March 30, 2008
Team Members Travel

March 31 – April 3, 2008
7:30 a.m. – 5:00 p.m.
Planning, Data Collection, Document Review and Interviews
5:00 – 6:00 p.m.
Team Meeting

April 4, 2008
Team Members Travel Home

Performance Testing, Data Collection, Validation and Closeout Activities – April 13 - 25, 2008

April 13, 2008
Team Members Travel

April 14 - 18, 2008
7:30 a.m. – 5:00 p.m.
Data Collection, Performance Testing, Report Writing, and Validation Activities
5:00– 6:00 p.m.
Team Meeting

April 19, 2008
Report Writing
April 21, 2008
12 noon. – 5:00 p.m.

April 22, 2008
8:00 a.m. – 5:00 p.m.

April 23, 2008
8:00 a.m. – 5:00 p.m.

April 24, 2008
TBD

April 25, 2008
Team Members Travel Home

Quality Review Board

Quality Review Board

Comment Resolution

Out-brief
## CORE INSPECTION TEAM COMPOSITION

### Management Team
Steve Yonkoff, Inspection Team Leader  
D.L. Whaley, Deputy Team Leader  
Kevin Nowak

### Program Management
Chris McLaughlin, Team Leader  
Mike Henry  
Bob Schultheiss

### Protective Force
Chris Hammond, Team Leader  
Leigh Barnes  
Ken Shields  
Steve Henwood

### Performance Testing
Jeff Larosa, Team Leader  
Ken Baxter  
Larry Grocki

### Physical Security Systems
Darryl Toms, Team Leader  
Jim Hamilton  
Jeff McClure

### Personnel Security
Mike Stalcup, Team Leader  
Bill Rich  
April Stottler

### Classified Matter Protection and Control
Ralph Kurtzman, Team Leader  
Gary Koch  
Pat Schmidt

### Material Control & Accountability
Vince Devito, Team Leader  
Frank Lamb  
Dave Shisler
Note: The core inspection team will be supported by an administrative support component, a performance testing component, augmentees from other DOE and NNSA sites, and other members of the Office of Independent Oversight brought in for limited roles. These names will be provided to the site as part of normal coordination activities.
Table of Contents

OFFICE OF INDEPENDENT OVERSIGHT INSPECTION
OF SAFEGUARDS AND SECURITY AND CYBER SECURITY
OF THE LIVERMORE SITE OFFICE
AND THE LAWRENCE LIVERMORE NATIONAL LABORATORY

TOPICAL AREA INSPECTION PLANS

1.0 Protection Program Management ............................................. 2
2.0 Classified Matter Protection and Control ................................... 5
3.0 Personnel Security ................................................................. 7
4.0 Physical Security Systems ...................................................... 11
5.0 Protective Force ................................................................. 18
6.0 Material Control and Accountability ........................................ 25
7.0 Classification and Information Control .................................... 27
8.0 Cyber Security ................................................................. 31
1.0 PROTECTION PROGRAM MANAGEMENT

1.1 Scope

The inspection of Protection Program Management will include all sub-topics: Protection Program Planning, Budget and Resources, Program Direction, and Feedback and Improvement. In addition, an evaluation of the site’s progress to implement applicable DOE Policy will be performed. The primary focus under protection program planning will be the Site Safeguards and Security Plan (SSSP) and the vulnerability assessments underlying them, particularly an evaluation of the extent to which the site has successfully addressed planning issues identified in previous Independent Oversight inspections. Coupled with this review will be a review of large-scale, force-on-force performance testing conducted to confirm vulnerability assessment results. In budget and resources, the primary emphasis will be on resource utilization to meet the challenges of implementing the Design Basis Threat policy, particularly the impact on resources for full compliance with the 2003 policy. The review of program direction will focus on the implementation of current DOE directives, with primary reliance on other topic teams to critique the implementation of directives. Feedback and Improvement will primarily focus on the response to self-assessments and to other reviews, such as surveys and Independent Oversight inspections.

At LSO, the inspection of protection program management will review the leadership and oversight provided for the SSSP effort and DBT Implementation process, current involvement in budget formulation and execution, and site office effectiveness in providing safeguards and security program direction to site contractors, including the review and processing of deviation requests. The review of Feedback and Improvement will include the survey program, including the approval and monitoring of corrective actions taken at the site office and by site contractors in response to issues identified by outside reviews, surveys, and self-assessments.

The results from reviewing site specific management mechanisms during other portions of the inspection will be analyzed to determine the extent to which site management systems support the objective, guiding principles, and core functions of Integrated Safety and Security Management (ISSM).

1.2 Protection Program Planning

DOE requires the site to develop and implement protection programs tailored to address specific site characteristics and requirements, current technology, ongoing programs, operational needs, and to achieve acceptable protection levels that reduce inherent risks on a cost-effective basis. The review of the safeguards and security planning element is intended to verify that LLNL has followed this requirement.

Lines of Inquiry for Vulnerability Assessments
- Do vulnerability assessments portray a threat appropriate for the operations?
- Are there assumptions made that unreasonably limit adversary actions or capabilities?
- Do the adversary strategies and tactics evaluated reflect the best choices for the adversaries under the prevailing assumptions?
- Do strategies and tactics reflect those actually trained for and used by LLNL?
• Is the methodology used to evaluate protection effectiveness adequate to evaluate adversary and site actions and responses?
• What is the role of the Site Office in vulnerability assessments?
• What is the status of Vulnerability Assessments to support DBT Implementation Planning?

Lines of Inquiry Concerning Methodologies Used for Vulnerability Assessments
• What expertise is available at the Site Office to assist with and oversee the conduct of vulnerability analyses or to critique the results?
• What methodologies are used for the vulnerability assessments?
• Are the methodologies used correctly?
• Are these methodologies adequate to evaluate the protection system?
• How are adversary timelines and task requirements determined?
• How are site-specific features of the protection system characterized in simulations?
• How are unique adversary weapons and equipment characterized in the modeling?
• Do the conditions under which performance tests are conducted match those depicted in computer simulations closely enough to allow comparison? If so, how well do they compare?

Lines of Inquiry for Site Safeguards and Security Plan
• Have the results of the vulnerability analyses been portrayed correctly in the SSSPs?
• Does the description of the operations include all current activities?
• Does the description of the protection measures accurately reflect those implemented?
• Does the process for preparing an SSSP provide for reasonable input from all concerned parties?
• Does the Site Office play a part in the review and approval of each SSSP?
• Who has approval authority for SSSPs?
• Is each approval current?
• What is the status of identified upgrades?
• Are safeguards and security essential protection elements and systems identified for evaluation under the Performance Assurance Program?

1.3 Budget and Resources

The general thrust of this element is to ensure that safeguards and security planning is reflected in the process of identifying future needs and that current funds and other resources needed to implement safeguards and security plans and commitments are available.

Lines of Inquiry for Budget Formulation
• Are the site contractors' safeguards and security managers involved in the safeguards and security budget formulation process?
• Are the Site Office safeguards and security managers involved in the safeguards and security budget formulation process?
• What are the assumptions and guidance under which the budget was formulated?
• Are these assumptions and guidance consistent with commitments made in the SSSPs and in corrective action plans?
• What provisions have been made to continue enhanced security measures into future years?

Lines of Inquiry for Budget Execution
• What is the Site Office role in tracking and overseeing expenditures of site contractors?
• Is there a current year spending plan? How well are expenditures to date matching that plan?
• What will be the impact of enhanced security measures required during FY 2007?
• Are there identified shortfalls for FY 2008?
• Is there a particular area where lack of funding may create a protection issue?
• What means are used by the Site Office and site contractors to track safeguards and security achievements versus expenditures?

Lines of Inquiry Regarding Competency Commensurate with Responsibility
• Have responsibilities been explicitly assigned to safeguards and security personnel at the Site Office and within the site contractor organizations?
• Do these assignments frequently change?
• Has there been an analysis, formal or informal, of the job skills needed to fulfill each assigned responsibility?
• Is there evidence that site contractor and the Site Office managers are effectively ensuring that individuals gain and maintain the job skills needed to fulfill assigned responsibilities?
• Have the Program Office, Site Office, and contractor established and maintained a competency standard for personnel with oversight responsibilities?
• Are sufficient training funds available?
• Are there one or more areas in which additional training emphasis is needed?
• If all safeguards and security staff are not fully competent to discharge their assigned duties, what is the primary causal factor for this?

1.4 Program Direction

Once plans have been made and resources identified, it is necessary to provide explicit instructions that will implement the planned activities within the resources that are available. Some requirements are fixed from DOE Headquarters, such as DOE directives and any implementation instructions that may originate with Headquarters line management. Within these broad guidelines, it is expected that there will be locally derived implementing instructions that will be transmitted in a variety of forms.

Lines of Inquiry Concerning Program Direction and Implementation of DOE Directives
• Has the implementation of any DOE directive been unduly delayed?
• Are all deviations correctly characterized as variances, waivers, and exceptions?
• Have all risks associated with deviations or delay in incorporating directives into contracts been correctly analyzed and stated in decision packages? Is there supporting documentation for this analysis at the site contractor organizations and/or the Site Office?
• Have any other topic teams identified a weakness due to delay in implementing directives or inappropriate approval of deviations?
• What process is used to transmit expectations and evaluate the effectiveness of the Safeguards and Security Program?
• How much fee is "at risk" and performance-based? What is the percentage relative to funding for all site programs?

1.5 Feedback and Improvement

When the Safeguards and Security Program is fully implemented, there should be a mechanism in place to regularly measure its success, provide feedback to management concerning its success, and to make cost-effective improvements regardless of its success.

Lines of Inquiry Concerning Feedback Mechanisms
• Are surveys conducted as required?
• Are survey results consistent with the results of this Independent Oversight review?
• Are survey report narratives sufficient to support the ratings assigned?
• Have working paper files been maintained as required?
• Are self-assessments conducted as required?
• Are self-assessment results consistent with Independent Oversight reviews and surveys?
• Are self-assessment report narratives sufficient to support the ratings assigned?

Lines of Inquiry Concerning Response to Feedback
• Are corrective action plans prepared for all findings?
• Are corrective action plans supported by effective analysis?
• Do corrective action plans contain all necessary information elements?
• Are effective root cause analysis and cost-benefit analysis conducted?
• Is effective risk assessment performed?
• Are corrective actions completed on schedule?
• Are corrective actions completed in a time frame commensurate with the impact of the protection weakness?
• Is there a procedure for tracking and trending findings?

2.0 Classified Matter Protection and Control

2.1 Scope

The inspection of Classified Matter Protection and Control at LLNL will include the following sub-topical areas: Program Management, Operations Security (OPSEC); the Security Infraction Program; and Physical Protection and Control of Classified Matter. Technical Surveillance Countermeasures (TSCM) will not be included in the inspection. The TSCM program at LLNL was part of a department wide special review of TSCM that was conducted in 2007. Performance testing will be conducted in the areas of transmission, reproduction, and destruction. Also, front and back checks of matter that is in accountability, to include Classified Removable Electronic Media, will be performed. Review of the site-specific procedures and interviews of personnel responsible for the sub-topical areas will be accomplished.
2.2 Program Management

Program management of the CMPC program encompasses the traditional aspects of management.

**Lines of Inquiry for CMPC Program Management**

- Have adequate resources been provided for all aspects of the CMPC program, including personnel (plus training), equipment, and facilities?
- Have organizational and individual responsibilities (including accountability for performance) been defined?
- Have management oversight activities, such as self-assessments and surveys, been effective in identifying areas of the program that do not meet DOE policy requirements?
- Have Site Office and the various LLNL management functions ensured that corrective actions are implemented in a timely and efficient manner?

2.3 Operations Security

An OPSEC program must be in place to help ensure sensitive information is protected from compromise and secured against unauthorized disclosure. The program should be structured to provide program management with the necessary information required for sound risk management decisions concerning the protection of sensitive information.

**Lines of Inquiry Concerning OPSEC**

- Is the Critical Program Information appropriate?
- Is the associated list of indicators comprehensive and reflective of site program and facility specific concerns?
- Does the membership of the OPSEC Working Group represent appropriate programmatic and management participation?
- Do the minutes of the OPSEC Working Group indicate the group meets with appropriate frequency and is recognizing and effectively addressing significant OPSEC issues?
- Is OPSEC awareness training conducted for the site’s population?
- Is its format and content appropriate to address the assigned mission of the Site Office and LLNL entities?

2.5 Incidents of Security Concern Program

A security incident program is required for all organizations that deal with classified matter in any form.

**Lines of Inquiry Concerning the Incident Program**

- Is there evidence of timely reporting of security incidents?
- Is there complete documentation for each incident?
- Is there a documented root cause analysis process for security incidents?
- Is the completion of a root cause analysis documented for each incident?
- Are corrective actions for security incidents comprehensive?
- Are the corrective actions selected likely to prevent recurrence of similar incidents?
2.6 Physical Protection and Control of Classified Matter

Physical protection and control of classified matter (accountable and non-accountable) are required by DOE directives.

Lines of Inquiry for Physical Protection and Control of Classified Matter
- Is classified matter stored in General Services Administration-approved containers or in vault-type rooms in accordance with DOE directives?
- Are reproduction policies and equipment consistent with the sensitivity of classified matter being reproduced?
- How is destruction of matter accomplished?
- What are the policies and procedures governing transmittal of classified matter?
- Do transmittal operations reflect that policy?
- Have appropriate markings been applied to classified matter, including electronic media?
- Are accountability records accurate?
- Have the various inventories been performed?
- Do the inventories, as conducted, provide reasonable assurance that no classified matter has been lost?

3.0 Personnel Security

3.1 Scope

The inspection of the Personnel Security (PS) topic will focus on the site personnel clearance program, the human reliability program (HRP), the unclassified foreign visits and assignments programs (FV&A), and the safeguards and security awareness program (SSAP). In addition, inspection activities at LSO will be conducted to assess the effectiveness of their oversight role of the LLNL Personnel Security Program as a whole.

In addition to routine data collection activities (i.e., interviews, program document and file reviews), a number of performance assessment tools may be employed during the evaluation of the personnel security topic. A test administered to drug and breath alcohol and drug testing technicians to determine their knowledge of the critical elements of the drug and alcohol testing programs. A questionnaire will be administered to selected employees to gain insight into the effectiveness of the safeguards and security awareness program to instill a high level of awareness of individual security responsibilities of the LSO and LLNL cleared employee population.

3.2 Program Management

Program management of the PS program will focus on the ability of LSO to provide adequate oversight of the LLNL PS program, and on LLNL’s ability to provide sufficient resources to meet program objectives.
Lines of Inquiry for PS Program Management

- Assess the level to which LSO and LLNL managers are actively engaged in program administration and leadership.
- Have adequate resources been provided for all aspects of the PS program, including personnel and training?
- Are personnel security clearance processes adequate to support effective implementation?
- Is the personnel security clearance organization designed for efficient operations?
- Have the LSO and LLNL managers ensured corrective actions are implemented in a timely and efficient manner?
- Assess the overall level of staff competence, experience, and skills.
- Have organizational and individual responsibilities (including accountability for performance) been defined and properly communicated?
- Have management oversight activities (i.e., self-assessments and surveys) been effective in identifying areas of the program that do not meet DOE policy requirements; including:
  - Knowledge of current issues and concerns of LLNL PS program elements;
  - Quality and depth of federal surveys and contractor self-assessments of PS sub-topical elements; and
  - Identification of other methods and strategies by which the LSO and LLNL managers assess overall PS program performance.

3.3 Personnel Security Clearance Program

DOE strives to ensure individuals to be afforded access to classified matter or SNM meet high standards of personal conduct, trustworthiness, sound judgment, and reliability.

Lines of Inquiry for the Personnel Security Clearance Program

- Are individuals processed for a DOE access authorization only if their official duties require such access and only after the completion of pre-employment checks?
- Do pre-employment checks include all required elements, and does LLNL ensure that all derogatory information has been reported to DOE?
- Have the drug testing requirements for clearance applicants and current clearance holders contained in Secretarial memorandum, Decisions regarding drug testing for Department of Energy positions that require access authorizations (Security Clearance), dated September 14, 2007, been implemented?
- Have DOE security badges been issued only after a DOE access authorization has been granted?
- Are personnel security clearance determinations properly reflected in the Central Personnel Clearance Index?
- Is timely and efficient notification made to DOE when an access authorization is no longer required?
- Are DOE security badges retrieved and destroyed when the access authorization is no longer needed or has been suspended/terminated?
- Is timely reporting of all issues of security concern being made to DOE?
• Have the requirements associated with Homeland Security Personnel Directive (HSPD)-12 been implemented?

3.4 Human Reliability Programs

Given the high interest in mitigating the potential for misuse of SNM by insiders, it is imperative that the trustworthiness and reliability of certain identified workers are above reproach. DOE seeks to accomplish this objective by implementing an HRP that includes a system of continuous evaluation and monitoring to identify those individuals whose judgment may be impaired by physical and/or emotional problems, the use of controlled substances, or the excessive use of alcohol.

Lines of Inquiry for Human Reliability Programs

• Is there a well-defined and documented process to ensure all required positions have been identified, and have all individuals in these positions been enrolled in the HRP?
• Do program officials have sufficient training or job experience to successfully meet program requirements, and do they understand their responsibilities?
• Are any individuals allowed to assume HRP duties prior to completion of all enrollment requirements?
• Are any individuals allowed unescorted access in close proximity to SNM while temporarily removed from the HRP?
• Have the appropriate notifications and actions been taken when an HRP certified employee no longer meets security and safety suitability requirements?
• Does the re-certification process ensure that all HRP certified individuals complete all annual requirements within 12 months?
• Do drug and alcohol testing procedures ensure all HRP certified individuals are tested at least once every 12 months, and are appropriate actions taken when positive test results are achieved?
• Are drug and alcohol test personnel properly trained and certified?
• Are supervisors and HRP certified individuals properly trained and do they understand their HRP responsibilities?
• Do results of questionnaires indicate that HRP supervisors and HRP certified individuals are knowledgeable of the roles and responsibilities?
• Are there indications of adequate communications between HRP officials, site occupational medical personnel, and personnel security clearance program officials?

3.5 Unclassified Foreign Visits and Assignments Program

International cooperation and collaboration are important elements in the effective planning and implementation of many DOE programs. DOE and its international partners benefit from the exchange of information that results from a managed process of unclassified visits and assignments by foreign nationals. These visits and assignments must be conducted in a manner consistent with U. S. and DOE national security policies, requirements, and objectives including export control laws and regulations.
Lines of Inquiry for the Unclassified Foreign Visits and Assignments Program

- Do program officials, hosts and escorts have sufficient training or job experience to successfully meet program requirements?
- Are unclassified foreign visits and assignments structured and conducted in such a manner that prevents unauthorized transfer of sensitive information, protect counterintelligence interests, security interests, and sensitive subject information and technologies, as well as export controlled information?
- Has responsibility for approving unclassified visits and assignments been properly assigned or delegated?
- Are records on indices checks, security plans, passport and visa, biographical and personal identification data, purpose for the visit or assignment, certification of DOE mission advancement, and host reports being properly maintained?
- Are security plans sufficiently detailed to ensure the proper control of foreign nationals and sensitive information?
- Does the approval process contain and document all necessary coordination elements, (i.e., security, cyber security, OPSEC, Counter Intelligence, export control, etc.)?
- Are foreign nationals allowed off site access to LSO and LLNL computing assets, and if so, has an adequate risk assessment been completed before allowing this access?
- Is foreign national visit and assignment information being properly documented in the Foreign Access Central Tracking System (FACTS)?
- Has LSO and LLNL developed the ability to automatically upload information into FACTS?
- Is the protective force informed of any foreign nationals that have been granted access during after duty hours?
- Have there been any issues of security concerns or security infractions identified in regards to FV&A?

3.6 Safeguards and Security Awareness Program

Supporting DOE’s personnel security program, as well as the broader aspects of the overall protection program, the safeguards and security awareness program is designed to ensure all individuals are informed of their individual security responsibilities associated with DOE programs and activities. The program, which consists of a series of specially designed briefings, also alerts individuals to actual or potential threats, and motivates them to maintain a high level of individual security awareness.

Lines of Inquiry for the Safeguards and Security Awareness Program

- Have all individuals completed the initial briefing and the comprehensive security briefing prior to issuance of a site or DOE security badge, respectively?
- Are appropriate access controls and badge actions taken after an individual’s access authorization is suspended or terminated and a termination briefing is completed?
- Are the materials that support the various required briefings comprehensive, contain required information, and current?
- What is the primary method employed for delivery of required briefings and is it effective?
- Did all LSO and LLNL personnel complete the FY 2007 annual security briefing? If not, what actions were taken?
• Does LSO and LLNL have an effective process in place to ensure completion of all SSAP briefings?
• Do results of the security awareness questionnaire indicate employees understand their individual security responsibilities?

4.0 PHYSICAL SECURITY SYSTEMS

4.1 Scope

The evaluation of the Physical Security Systems (PSS) topic will be based upon the performance capabilities inherent in DOE requirements for the protection of Category I Special Nuclear Materials using the layered protection strategy. The fundamental expectation is that the contribution of physical security systems to the overall protection strategy should be equivalent to other DOE sites, with appropriate allowance made for conditions or limitations specifically acknowledged and accepted in the SSSP. The PSS topical inspection will focus upon the various alarm systems, access control and search equipment, and associated alarm monitoring and communication systems that are integral to the overall assessment and response process. Additionally, the effectiveness of the testing and maintenance activities designed to ensure the ongoing effectiveness of physical security systems would be reviewed. Activities relating to the inspection of physical security systems will include interviews with personnel responsible for physical security, performance testing of security systems, and documentation review.

4.2 Intrusion Detection and Assessment

An essential element in any protection system is the detection and timely, accurate assessment of unauthorized intrusions. A variety of physical, electronic, and human elements are employed to accomplish detection and assessment, as well as to provide adversary pathway delay to allow sufficient time for the protection system to adequately respond. Electronic Intrusion Detection Systems (IDS) are deployed throughout the DOE complex for the protection of a variety of DOE assets. Chief among those assets are nuclear weapons and SNM. Intrusion detection systems are also used for the protection of classified parts, material, and matter and for the protection of personnel and government property. The requirements and expectations for performance of electronic IDS are applied in a graded manner corresponding to the importance of the asset(s) being protected. The lines of inquiry for intrusion detection listed below are focused on the protection of Category I Special Nuclear Material and classified matter, and to a lesser extent on the protection of personnel, and government property.

Assessment of intrusion alarms and other security incidents at DOE facilities is either accomplished through Closed Circuit Television (CCTV) or visual assessment. Timely assessment and resolution of alarms is critical whether protecting SNM or other DOE assets. Detection without effective assessment provides no protection. The lines of inquiry for assessment listed below are related to the protection of SNM, classified matter, personnel, and government property, and address both visual and electronic assessment.

Lines of Inquiry for Intrusion Detection and Assessment
• Are the IDS terminals password protected?
• Are IDS user access levels appropriate for personnel roles and responsibilities?
• Is access to IDS terminals physically controlled?
• Are the procedures adequate to prevent the introduction of malicious code to IDS terminals?
• Does the site have procedures to respond to alarms, including response time; also, response procedures when multiple alarms occur simultaneously?
• Does the site have procedures to record/log alarms? Is this done within the IDS?
• Does the site have procedures to patrol perimeters and security areas and to inspect systems to ensure that protection is not degraded (e.g., verify that no ladders, scaffolds, etc., can be used to bridge/jump the exterior fences, and verify no equipment is blocking interior sensors)?
• Does the site have compensatory procedures used during failure of alarm system or components thereof?
• Does the IDS provide timely annunciation of intrusion alarms?
• Does the IDS distinguish between intrusion, tamper, and supervisory alarms?
• Is response to IDS alarms adequate? Include post-alarm testing (esp. for tamper alarms)?
• Does performance testing of interior alarms reveal any non-functioning or poorly functioning sensor?
• Are credible pathways sufficiently covered by motion detection or other alarm devices within Vault-Type-Rooms (VTR)?
• If the distance between the true floor (or true ceiling) and the false floor (or false ceiling) of a VTR is greater than six inches, is the required alarm sensor coverage provided?
• Do Vault and VTR door and wall construction meet requirements?
• Are man-size penetrations, including Heating Ventilation and Air-Conditioning ducting, covered, blocked, or alarmed? Can the integrity of seals (rebar) be confirmed on a regular basis?
• Does the site have procedures to assess intrusion alarms?
• Does the site have procedures to assess tamper and line-supervision alarms?
• Does the site have procedures to respond to alarms?
• Is response to IDS alarms adequate, to include post-alarm testing (esp. for tamper alarms)?
• Does the site utilize CCTV Cameras, and are CCTV cameras used as the primary source of assessment for any alarms?
• If primary assessment is via CCTV, can the alarm(s) be reliably assessed with the cameras as installed and configured?
• Is lighting adequate for assessment?
• Are there obstructions that interfere with assessment?
• Is maintenance and testing for the CCTV system adequate?
• Are camera fields of view and focal lengths adequate for assessment?
• Does the video capture system adequately assist assessment? Is it susceptible to deception such as alarm stacking?

4.3 Access Control and Entry/Exit Inspection

The protection scheme for DOE sites and facilities is organized around the concept of layered protection. The number and types of layers depends on the assets being protected. At each layer of the protection scheme, increasingly restrictive levels of access control and entry/exit inspection
procedures are applied to ensure that only authorized personnel are admitted and that prohibited and controlled articles are excluded from security areas. The lines of inquiry for access control and entry/exit inspection listed below are related to the protection of SNM, classified matter, personnel, and government property.

Lines of Inquiry for Entry/Exit Control and Inspection

- Does the site have documented procedures to verify access authorization by checking identifiers (e.g., names, employee numbers) against an access authorization list (hard copy or computer file)?
- Does the site have documented procedures to log non-routine entries (e.g., visitors, personnel during off-shift, and personnel not normally assigned) at security areas?
- Does the site have documented procedures to verify the identity of a visitor before issuing a badge/pass/credential?
- Does the site have documented procedures to verify the authorization and clearance of a visitor before issuing a badge/pass/credential?
- What type of personnel access control method/equipment is utilized at each layer of protection (Limited Area, Property Protection Area, VTR, etc.)?
- How often are the inspection equipment such as metal detectors and X-ray machines tested? What types of tests are performed?
- Does performance testing reveal that equipment is effective in detecting prohibited and controlled articles?
- Are entry control facilities configured to prevent bypass of the search procedures?
- Is U.S. citizenship validated before providing visitor or temporary workers site access? Does the visitor log contain penalty language for falsifying U.S. citizenship? Are visitor forms, as they relate to foreign visitors, properly filled out?

4.4 Badges, Passes, and Credentials

Badges, passes, and credentials are critical to controlling access to DOE sites and facilities. The DOE standard badge is utilized by the site’s electronic access control systems and by protective forces to ensure only authorized individuals are allowed to enter each layer of protection. Failure to protect badges passes, and credentials and the systems that create them may provide adversaries a means to circumvent whole layers of the protection, rendering other protection systems and methods useless. The lines of inquiry concerning badges, passes, and credentials listed below are related to the protection of SNM, classified matter, personnel, and government property.

Lines of Inquiry for Badges, Passes, and Credentials

- Does the site have procedures to store and account for badges and badge stock?
- Does the site have procedures to report lost badges and to notify appropriate personnel?
- Does the site have procedures to enroll personnel in an automated access control system (e.g., card reader; biometric identification device)?
- Does the site have procedures to delete personnel from an automated access control system?
- Does the site have procedures to monitor personnel as they interface with access control equipment to ensure they follow authorized procedures?
- Is access to badging system terminals controlled and restricted to only authorized individuals with the appropriate access authorization?
• Does the site have procedures for the return of expired badges, including data and procedures to audit badging records and recover badges not returned?

4.5 Barriers

Just as each layer of the protection scheme has increasingly restrictive levels of access control and search procedures, the barriers applied increase in strength and resistance to attack, as they get closer to (and as a function of) the asset being protected. The lines of inquiry for barriers listed below are related to the protection of SNM, classified matter, personnel, and government property.

Lines of Inquiry for Barriers
• What types of barriers (layers) are utilized to protect SNM and classified information?
• What types of barriers (layers) are utilized to protect personnel, government property, and sensitive unclassified information?
• Does the site have procedures to patrol and inspect exterior security area perimeter barriers (e.g., fences) to verify integrity and detect unauthorized objects (e.g., ladders) or conditions (e.g., excessive soil erosion under fence)?
• Does the site have procedures to patrol and inspect interior security area perimeter barriers (e.g., VTR walls, doors) to verify integrity and detect penetration?
• Does the site have procedures to lock down/secure the facility or area in response to a security condition?

4.6 Communications

Systems utilized by the DOE for security communication include protective force radios, duress alarms, public address systems and standard telephone lines. These systems must be available and effective for normal and emergency communication. Prudent measures must be taken to protect communications from loss of service or exploitation by potential adversaries. As part of the overall command and control infrastructure, loss or compromise of these systems can have a large impact on the effectiveness of protective force response to adversarial events. The lines of inquiry concerning communications listed below are related to the protection of SNM, classified matter, personnel, and government property.

Lines of Inquiry for Communications
• Are communications adequate for routine and emergency conditions?
• Are security radios continuously recorded over all channels?
• Are communications tested on all frequencies and at key locations?
• Is radio battery power and sensitivity adequate?
• Are investigation/response procedures implemented if a protective force member does not respond to a periodic radio check?
• Are there procedures to switch to different frequencies during specified conditions (e.g., tactical response)?
• Does the site have procedures to communicate a duress situation when a duress switch cannot be activated, such as use of code words?
• Does the site have procedures to respond to a duress condition?
• Can duress alarms be quickly and inconspicuously activated?
• If the site utilizes an encrypted radio frequency signal for communication, is the encryption key appropriately protected and routinely changed?

4.7 Testing and Maintenance

Systems employed for the protection of DOE sites and facilities must be tested and maintained to ensure their effectiveness. Maintenance activities are either corrective (upon failure) or preventive in nature. The corrective maintenance organization must have the resources to fix identified deficiencies in a timely manner. Preventive Maintenance (PM) must be performed at a minimum to manufacturer’s specifications. However, false and nuisance alarm rate data, failure, and out of service data must be considered when planning and performing preventive maintenance activities which includes upgrades and replacement of equipment. Operational and performance testing should be an integral part of any maintenance organization to ensure components are operating effectively. The lines of inquiry for maintenance and testing listed below are related to the protection of SNM, classified matter, personnel, and government property.

Lines of Inquiry for Testing and Maintenance
• Is the maintenance and testing program documented, including frequency and content of preventive maintenance and of testing?
• Has a list of critical system elements been developed and is it current? What is the basis for the items on the critical system elements list?
• Does an inspection of past year’s maintenance records reveal any problems, such as:
  o Has the 24/72-hour requirement been met?
  o Are personnel signing maintenance records appropriately cleared?
  o Is the PM schedule on track?
  o Does the maintenance organization have enough personnel and resources to adequately perform it functions?
  o Have the manufacturer’s recommendations and specifications for PM been compiled and incorporated into the security maintenance program?
• Does the maintenance and testing documentation indicate if the sensor anomaly may be the result of inadequate PM or testing?
• Does the past year’s test data contain appropriate content, results, and periodicity?
• Does the site have procedures to maintain/calibrate security-related hardware?
• Does the site have procedures to initiate repair/replacement of degraded equipment?
• Does the site record and maintain maintenance results?
• Does the site analyze maintenance results for trends or for prioritization of future maintenance items?
• Does the site have procedures to verify test results?
• Does the site have procedures to verify proper maintenance (e.g., functional tests by a second person)?
• Does the site have procedures to verify or inspect work by offsite vendors?
• Does the site have procedures to verify integrity of system-following software modifications?
4.8 Support Systems

Support systems, which interface with security systems and subsystems, are employed to ensure the reliable operation of security components. The main and emergency power supply subsystems must not be vulnerable to sabotage. Support systems such as uninterruptible power supplies (UPS) and diesel generators must be able to operate in the event of a catastrophic loss of main power. Preventive maintenance and performance testing should verify their operability. The lines of inquiry for support systems listed below are related to the protection of SNM, classified matter, personnel, and government property.

Lines of Inquiry for Support Systems

- What security-related components are supplied auxiliary power by batteries, an UPS, or other means?
- What is the length of time each UPS will maintain operation at full load?
- Which security-related components are supplied auxiliary power by diesel generators?
- What are the frequency and methods for testing and maintaining diesel generators (e.g., full load tests, test of switching devices)?
- What is the frequency and methods for testing and maintaining system batteries or the UPS?
- What is the frequency and methods for testing and maintaining batteries that power individual components (e.g., sensors and data gathering panels)?
- What is the replacement frequency for non-rechargeable batteries?
- What indications are received in Central Alarm System/Secondary Alarm Station when normal or auxiliary power fails?
- What is the source of offsite electric power, including number of feeds?
- How are the systems tested (i.e., are they turned on, brought up to speed and then the load switched, or does the test actually simulate power loss)?

4.9 Systems Management

Program management of the physical security system program encompasses the traditional aspects of management, program direction, and oversight.

Lines of Inquiry for Systems Management

- Does site management develop plans that include goals, objectives, and responsibilities for major aspects of physical protection?
- Does physical security systems management provide adequate resources to include personnel (plus training), equipment, and facilities to meet the requirements contained in the procedures and policies?
- Does physical security systems management define organizational and individual responsibilities (including accountability for performance)?
- Does management monitor the status of the physical security system program and policy implementation?
- Does management assure that all areas of systems anomalies or non-compliance are corrected in a timely and efficient manner?
- How does the physical security systems program budgeting process function?
• Does management perform oversight activities of the physical security system program such as self-assessments to identify areas that do not meet DOE policy requirements or are not performing adequately?
• Are self-assessments and surveys designed and conducted in a manner that is successful in identifying program problem areas?

4.10 Locks and Keys

Management of security keys is a vital function. Controlling and accounting for security keys must be conducted in a manner that assures managers that physical protection is not jeopardized due to lost security keys. The lines of inquiry for locks and keys listed below are related to the protection of SNM, classified matter, personnel, and government property.

Lines of Inquiry for Locks and Keys

• Is classified matter stored in a General Services Administration (GSA)-approved security container? If not, is the storage method appropriate?
• Has criteria been established for changing the safe combination?
• Have procedures been established for properly repairing the GSA safe?
• Does the site have procedures to issue keys, store keys, change locks and lock cores, issue combinations, and change combinations?
• Does the site have a documented lock and key program and are the requirements applied in a graded fashion?
• Does the lock and key program have a documented inventory system and frequency in which the inventory is to be conducted?
• Does the site have protection measures in place for the storage of security keys, key blanks, key cutting codes and combinations, and are they protected at the same level of the asset under protection?
• Does the site have a centralized location with one organization identified and responsible for control and management of the lock and key program?
• Does the site have documentation that defines the difference between security locks and keys from administrative locks and keys?
• Does the site have procedures in place for changing out keyways and cores, replacing damaged or broken keys and changing combinations to spin dial locks?
• Does the site ensure that security key rings are protected in a manner that prevents security keys from being added or removed from the key ring?
• Does the site have procedures that require key rings be marked with a unique number for inventory and accountability purposes?
• Does the site have procedures to report lost, missing, or damaged keys and is there a mechanism in place to ensure reporting through the security incident system for proper categorization and up through the chain of command?
• Does the site have a database for locks and keys for accountability purposes?
• Does the site have procedures in place to prevent security keys from being removed from security areas? Are the keys properly protected when in the possession of the user?
• Does the site maintain the minimum number of security keys necessary for operational purposes and is there a procedure for the destruction of security keys no longer required?
• Does the sites survey and self-assessment program address all facets of the lock and key program? Are they comprehensive?

4.11 Explosive Detection

Explosive detection is a vital function. Detection of explosives must occur at security area boundaries. Either canine or explosive detection system must be used to assist in the detection of explosives that could be introduced into the facility. The lines of inquiry for the explosive detection program are listed below.

Lines of Inquiry for Explosive Detection
Has the site conducted and documented a threat analysis to determine the type and quantity of explosive that poses a risk?
• Has the site conducted and documented an analysis of the benefits of using explosive detection systems in lieu of canine?
• Has the site documented who and what is inspected for explosives?
• How does the site calibrate the explosive detection equipment? How often and by whom?
• What training has been provided to the explosive detection system operator?
• Has the explosive detection system training been documented?
• How often is the operator trained on the proper operation of the explosive detection system?
• Does the site have procedures developed to address actions to be taken when the explosive detection system indicates an alarm?
• How does the site validate the explosive detection alarm?

5.0 PROTECTIVE FORCE

5.1 Protective Force Management

• Has protective force management developed specific plans to address adversary intrusion/attack, emergency evacuation, and protective force work stoppages?
• Has protective force management identified/modified protective force mission requirements?
• Is the protective force organized in a manner that fosters effective mission performance?
• Do protective force managers have the necessary experience/skills to effectively manage all aspects of protective force operations?
• Has protective force management allocated the necessary resources (personnel and equipment) for the protective force to be successful in achieving its assigned mission?
• Has protective force management developed plans, orders, and procedures that provide specific direction to enable the protective force to successfully perform routine and emergency duties and address potential security emergencies? Are these plans, orders, and procedures periodically reviewed to ensure that they are comprehensive and accurately aligned with the Site Safeguards and Security Plan and site operations?
  o Do plans, orders, and procedures adequately document protective force use of force and rules of engagement policy?
  o Are plans, orders, and procedures available to field personnel?
• Does protective force management ensure that personnel meet established qualification requirements?
• Has protective force management established an equitable system for classifying positions to serve as a basis for assignment and promotion?
• Are individual job descriptions developed, kept current, and based on task analysis?
• Has protective force management established an equitable policy outlining the scheduling of personnel?
• How does protective force management measure the effectiveness/performance level of its shift supervisors?
• Does management have a method to monitor/assess levels of morale and discipline?
• Are adequate numbers of supervisors assigned for each shift to the extent required to ensure proper and adequate performance of duties?
• Are the responsibilities of supervisors adequately delineated in respective job descriptions?
• Do supervisors possess the necessary experience/skills?
• Are supervisors trained in shift operations leadership (including tactical leadership) and management techniques?
• What are the selection criteria that serve as a basis for promotion to the supervisory level?
• Do supervisors adequately inspect protective force personnel prior to posting to determine fitness for duty?
• Do supervisors adequately inspect personnel on post/patrol to ensure that personnel are knowledgeable of the duties they are to perform, are proficient in the use of duty equipment, that the post/patrol equipment is functioning properly, and that the orders/procedures at the post/patrol are current and complete?
• How do supervisors measure the effectiveness/performance level of personnel on post/patrol?
• Is there a mechanism in place to evaluate a shift supervisor’s ability to conduct shift post limited scope performance testing?
• How do supervisors ensure that subordinate personnel are appropriately rewarded for superior performance, counseled/re-trained for inadequate performance, and disciplined for dereliction of duty/gross violations of orders?
• Is an equitable disciplinary policy for protective force personnel established?
  • If so, has that policy been consistently administered?
• Has a grievance policy/procedure been established?
• What is the role of the bargaining unit (if applicable) regarding the disciplinary policy and the grievance process?
• Does protective force management trend disciplinary actions and grievances to determine if there are any patterns of racism, profiling, sexual harassment, or preferential treatment?
• Is there a mechanism for corporate oversight of the protective force disciplinary program?

5.2 Training

• Is the training mission oriented?
• Are protective force Training Approval Program certifications current?
• Has the protective force Special Response Team (SRT) program been certified/recertified annually as required?
• Is there an established training program that is:
  o Based on a valid and complete set of tasks and competencies?
  o Establishing training objectives which take into account the learning characteristics and competencies of trainees?
  o Designed to ensure that training activities enable trainees to achieve the level of competency required to adequately perform routine and emergency duties?
• How does the training manager integrate feedback information into the training curriculum?
• Are sufficient resources (qualified personnel and sufficient equipment) allocated to training to ensure program effectiveness?
  o Is training designed so that activities make optimum use of available resources and are accomplished on a timely basis?
• Are supervisors provided training in tactical leadership and how to perform their supervisory duties?
• Are supervisors qualified to conduct formal training activities/limited scope performance tests on-shift?
• Are the results of training/testing monitored by both operations and training program managers?
• Do protective force personnel receive SNM recognition training regarding the various forms and configurations of nuclear weapons, nuclear weapons components, and SNM being protected, including the normal location and movements of these safeguards and security interests at and/or through the duty post?
• Do SRT personnel receive adequate training regarding mechanical and explosive breaching, consistent with the Tactics, Techniques and Procedures (TTP)?
• Do protective force personnel receive adequate training regarding the DBT and potential adversaries’ characteristics, tactics, and motives; and actions required of first responders to Weapons of Mass Destruction (WMD) incidents?
• Are Central Alarm System (CAS) Operator and Security Police Officer (SPO) II refresher training and SPO III maintenance training administered as required?
• Do protective force instructors attend at least one professional development course every three years? Is Instructor refresher training administered as required?
• Is there an established process for administering site-specific response plan training?

5.3 Equipment and Facilities

• Is the protective force equipped to effectively, efficiently, and safely perform routine and emergency duties?
  o Do protective force uniforms enhance performance of both routine and emergency duties and promote a professional image?
  o Is each Security Officer (SO) equipped with a portable radio with carrier and a flashlight with carrier?
  o Is each SPO I and II assigned a handgun and ammunition, a holster (of a secure type), an ammunition carrying device of sufficient capacity, a portable radio with carrier, handcuffs (with case) or other restraining devices, an intermediate force weapon (with case, if applicable), and a flashlight with carrier?
  o Is each SPO III assigned a rifle, handgun and ammunition, a holster (of a tactical type), an ammunition carrying device of sufficient capacity, fire-resistant hood and gloves, a
flashlight with carrier, goggles/eye protection, tactical boots, a chemical/biological weapons mask with carrier, handcuffs with case and/or other restraining devices?

- Is Level IIIA and III personal protective armor readily available (carried or worn on duty) for SPO II and III personnel respectively?
  - Are records maintained to ensure personnel protective armor is not deployed beyond its lifecycle and that it is rotated out for new equipment when appropriate? **A review of applicable documentation will be conducted.**

- Are binoculars available for use to permit observation and detection of unauthorized activity and to aid in the conduct of response operations?

- Are Night Vision Devices readily available for protective force responders deployed at facilities possessing Category I and II SNM?

- Are all armed protective force personnel issued equipment that provides an intermediate force capability (e.g., side-handle or collapsible baton or chemical agents)?
  - Are intermediate force chemical agents kept in active inventory past their expiration dates?
  - Is there a formal process to dispose of and document replacement of these equipment items? **A review of these records will be conducted.**

- Are protective masks available for SPO I, II, and III personnel, and Federal Agents (i.e., they must be carried by personnel or be stationed or positioned in such a manner to be quickly donned in support of response requirements without impact to response times)?
  - Are protective masks capable of providing adequate protection in a radiological/biological/chemical environment?
  - Does the SSSP document the rationale for chemical protective equipment selection, deployment, and use of such equipment to address detection and response?
  - Are protective force procedures for the use of chemical protective equipment approved by the DOE cognizant security authority?

- Are corrective eyeglass lenses worn by protective force personnel made of Z87.1 American National Standards Institute safety glass?

- Are personnel required to wear corrective lenses issued an extra pair to carry while on duty?
  - Are personnel required to wear corrective lenses also issued protective mask inserts?

- Is individually and post issued equipment stored and/or carried so that is readily available in a manner that supports timely and effective response?
  - Is secure storage available for individually assigned equipment belonging to off-duty personnel (e.g., lockers)?
  - Are there adequate stocks of expendable supplies and equipment on hand to support the protective force mission?
  - Has the protective force established protocols and procedures that facilitate control and accountability of surplus equipment items?

- Does the protective force have a process/procedure for issuing, relinquishing, and destroying protective force shields/credentials?
  - Are adequate supplies of unissued shields maintained to support staffing requirements?
  - Are unissued shields stored in a manner that assures their protection from loss, theft, or unauthorized use?

- Does the protective force have sufficient appropriate vehicles to perform its patrol and response missions?
o Are protective force vehicles distinctly marked and equipped with necessary emergency equipment (e.g., external warning lights, sirens, radios, and spotlights)?

o Are protective force vehicles maintained in serviceable condition, with preventive maintenance performed at intervals that meet or exceed the manufacturer recommendations? **A review or maintenance records will be conducted.**

o If armored vehicles are deployed at the site, do they offer assurance of continued operation and a safe level of protection to occupants under small arms fire, up to and including North Atlantic Treaty Organization 7.62 millimeter full-metal jacket?

- Does the protective force have adequate and sufficient special equipment and radios to perform its mission?
  
o Do protective force radios provide a multi-channel capability?
  
o Do protective force radios provide clear and reliable communications for response personnel?
  
o Are SRT personnel equipped with digital encryption two-way radios?
  
o Are protective force radios equipped with a duress alarm capability?
    - If equipped with duress capabilities, the duress system must be tested weekly. **A review of duress alarm check documentation will be conducted.**

o Does the protective force possess an effective backup communications capability (e.g., cellular telephones, public address, intercom systems, text messaging pagers, telephone bridge system, etc.)?

o Does the protective force employ equipment and/or procedures to communicate and identify friendly forces in order to mitigate fratricide?
  - Are these equipment items/procedures able to facilitate SIMPLE and RAPID identification of friendly forces during daylight operations under near and far conditions, and lowlight operations under near and far conditions?

- Does the protective force have sufficient suppressive fire weapons and weapons that facilitate neutralization of armored threats?
  
o Does the protective force have adequate quantities of appropriate types of ammunition (i.e., armor penetrating, high explosive, high explosive/dual purpose, etc.) to defeat the threat?

  
o Are protective force weapons and ammunition procured from approved vendors (i.e., American-based weapons manufacturers and/or are listed on the DOE standardized ammunition contract)? **A review of procurement records will be conducted.**

- Has the site established appropriate inventory and accountability protocols for the protective force armory/weapons?
  
o Does the protocol require the inventory (by number count) of all issued weapons at the beginning of each shift, of all weapons in storage (by number count) weekly, and all protective force weapons (by type, manufacturer, and serial number) monthly? **A 100% weapons inventory will be conducted.**

  
o If a weapon is missing, do the protocols require an immediate investigation and reporting to site management and the cognizant DOE office?

  
o Are all unissued or post issued firearms battle sight zero tested and verified semiannually? **A review or firearms maintenance records will be conducted.**

  
o Has the site established appropriate procedures for the repair and serviceability of weapons by qualified, Q-cleared/HRP certified armorer?

  
o Has the site established an adequate surplus (10%) of each type of firearm deployed?
• Does the protective force have sufficient updated specialized equipment such as x-ray machines, chemical/biological detectors, explosive detection, and metal detectors?
• How does the protective force mitigate the introduction of explosives to security areas?
  o Limited scope performance tests (LSPTs) will be conducted to test all explosive detection capabilities.
  o If electronic explosives detection equipment is used, does it function effectively and are operators skilled in the employment of such equipment?
  o If canine patrols are deployed at the site, are they able to effectively identify explosive threats?
    ▪ Are canine patrol shift durations and working conditions established in a manner that fosters effective performance of duties?
    ▪ Are kennel procedures, facilities, and resources adequate to facilitate a safe and healthy work environment?
    ▪ Do protective force canine patrols receive training in accordance with limits and recommendations established by the U.S. Police Canine Association (16 hours per month or 4 hours per week)? The past year’s training records will be reviewed.
    ▪ Are site canine explosive detection performance testing and training procedures adequate to mitigate the unauthorized introduction of explosive materials?
    ▪ Does the site also employ an operational test/training methodology, which requires canine teams to identify explosive odors in the actual environment where these tasks are likely to be performed?
    ▪ Has the protective force developed adequate procedures for handling and storing explosive testing sources/training aids?
    ▪ Are explosive testing sources/training aids stored in a manner which precludes cross contamination of test source odors? Specifically, are TNT, dynamite, and ANFO stored in separate/isolated storage bunkers/containers?
    ▪ Are testing sources/training aids routinely replaced with fresh sources?
    ▪ Are explosives test sources stored in approved repositories for the appropriate class of pyrotechnics/explosives?
• Are sufficient fixed posts and hardened fighting positions available in appropriate locations?
  o Do fixed posts provide occupants with protection from weather and temperature conditions and facilities to meet personal hygiene needs?
  o Do fixed posts/hardened fighting positions facilitate observation/engagement along likely routes of adversary ingress/egress?
  o Are protective force fixed posts/hardened fighting positions configured to facilitate overlapping fields of fire with adjacent elements?
  o Are protective force fixed posts equipped with a duress alarm capability?
    ▪ If equipped with duress capabilities, the duress system must be tested weekly.
    A review of duress alarm check documentation will be conducted.
  o Do hardened fighting positions at facilities possessing Category I and II SNM provide UL Standard 752 protection (i.e., high power rifle)?
    ▪ Are protected routes or methods of approach to hardened fighting positions available to protective force personnel?
• Does the protective force SRT at Category I/II sites have sufficient appropriate mechanical and/or explosive breaching resources to support recapture/recovery operations?
- Are the explosives used for breaching stored in accordance with the ES&H requirements?
- Is breaching equipment deployed in a manner that facilitates timely response?
- The absence of specialized functional capabilities, such as mechanical or explosive breaching, or precision rifleman/forward observer teams (PRFOT) must be justified. The site/facility must demonstrate alternative methods that can be utilized to meet these functional capabilities, and/or demonstrate that the absence of these capabilities does not affect the ability of the SRT to successfully execute recapture/recovery.

* Has the site established appropriate inventory and accountability protocols for keys assigned to the protective force?
* Are protective forces training facilities sufficient to conduct realistic training and qualification programs safely?

5.4 Duties

- Do protective force personnel possess the general skills and knowledge needed to perform routine duties, including:
  - Observation, assessment, and reporting
  - Weapons employment and maintenance
  - Individual tactics and self-defense
  - Vehicle operation
  - Communications
  - Portal control
  - Alarm station operations
- Are protective force personnel able to effectively and efficiently operate all equipment assigned to them for the performance of their duties?
- Do protective force personnel possess knowledge of relevant laws, policies, and orders?
- Can protective force personnel effectively execute a security emergency plan and respond in a tactically effective manner to satisfactorily address a major adversary threat?
- Have comprehensive protocols been developed that support the safe conduct of realistic performance testing and are those protocols implemented effectively?
- Does the performance test program effectively integrate all forms of testing (no-notice alarm response and assessment exercises, individual and team LSPT, and major ESS enhanced force-on-force exercises)?
- Are test results shared among performance test operations and training personnel for incorporation into the identification of performance enhancement needs?
- Are major performance tests (e.g., force-on-force) being conducted in the numbers and frequencies prescribed by current DOE policy?
- Do the major tests incorporate/reflect testing against current DBT parameters and are scenarios tested restricted to worst case pathways as established by vulnerability assessment modeling or does the testing have the flexibility to accommodate other adversarial initiatives that might better stress the system?
- Is the protective force evaluated during force-on-force exercises in individual and team tactical skills, application of force, weapon skills, the ability to communicate, and the ability to conduct operations in a chemical environment?
• Are response plans (including those for fresh pursuit, recapture, and recovery) fully tested during force-on-force exercises?

6.0 MATERIAL CONTROL AND ACCOUNTABILITY

6.1 Scope
The inspection of site MC&A program will include sub-topical areas of Program Administration, Materials Accountability and Materials Control. Performance testing will be conducted in the areas of measurements, tamper-indicating devices, inventory and accounting. Additionally, front and back checks of items that are in accountability will be performed. Review of the site-specific procedures and interviews of personnel responsible for the sub-topical areas will be accomplished. A tabletop exercise will be used to evaluate MC&A response to site developed scenarios. Also included in this inspection will be a review of the progress made in the correction of MC&A issues identified during the previous Independent Oversight inspections, site assistance validations, and surveys.

6.2 MC&A Program Administration

The administration sub-topic addresses the MC&A organization and its established MC&A program. The administrative element defines and documents the roles and responsibilities for all individuals having MC&A responsibilities. This element also institutionalizes the MC&A program by developing and approving written procedures, allocates sufficient resources to manage and operate the MC&A program, and monitors the performance of MC&A activities.

Lines of Inquiry for MC&A Program Administration
• Does the MC&A plan have the proper approval and is the plan comprehensive and current?
• Are procedures consistent and responsibilities clearly defined for all MC&A functions?
• Has the training program received the approval from the training approval program?
• Does the training program address all personnel performing MC&A functions?
• Have the Material Balance Areas (MBAs) been categorized and roll-up evaluated?
• Do the Vulnerability Assessments demonstrate MC&A analyses?
• Is the performance-testing program active and effective?
• Is occurrence investigation and reporting defined and incorporated into the overall facility program?
• Is the internal review and assessment program defined, comprehensive, and on schedule?
• Is possession of DOE-owned material by NRC licensees verified and documented?

6.3 Materials Accountability

The material accountability sub-topic addresses the various methods used for establishing databases, maintaining appropriate records, and accounting for nuclear materials at the facility. In addition, physical inventory frequencies and their conduct, measurement systems and measurement control, and documentation of nuclear material transfers are addressed.
Lines of Inquiry for Materials Accountability

- Is Local Area Network Material Accountability Software employed with the accounting database?
- Have attractiveness levels been determined for MBAs?
- Is shipment/receipt data accurate and entered in a timely manner into the accounting system?
- Are limits of error for shipments calculated?
- Are shipper/receiver agreements appropriate?
- Does the facility meet the Nuclear Materials Management and Safeguards System error rate goals?
- Is the inventory reconciliation fully documented and supported?
- Are accounting adjustments properly reviewed?
- Are Tamper Indicating Devices (TIDs) recorded in the accounting database?
- Are material transfer checks timely and measurements appropriately completed?
- Are results from the measurement systems entered into the accounting system accurately and in a timely manner?
- Are adequate security procedures established for personnel performing accounting functions?

6.3.1 Measurements and Measurement Control

The objectives of measurement and measurement control programs are to establish values for nuclear materials and assure the quality of the data.

Lines of Inquiry for Measurements and Measurement Control

- Do the calibration standards have traceability?
- Are measurement uncertainties defined?
- Are the qualifications and re-qualifications for measurement personnel identified?
- Does the sampling process for measurements yield representative samples?
- Are control limits established based on proper statistical assumptions and effectively implemented to ensure system control?
- Are materials not amenable to measurement clearly and accurately defined?

6.3.2 Nuclear Material Inventory Program

The purpose of the physical inventory is to determine the quantity of nuclear materials on hand at the time of the inventory, to compare the nuclear materials on hand to the book inventory. Also, differences between the physical inventory and book inventory should be investigated and resolved.

Lines of Inquiry for Nuclear Material Inventory

- Are the MBA boundaries clearly and properly defined?
- Are physical inventories taken at appropriate frequencies, in a systematic manner, and promptly reconciled?
- Are hold-up locations identified and properly recorded for inventory purposes?
- Are statistical sampling plans properly selected and appropriately implemented?
- Is the propagation of variance calculation done correctly?
• Is the inventory difference evaluation program thorough and complete?
• Have valid Inventory Verification/Confirmation Measurement and Measurement Control programs been established?

Lines of Inquiry for Nuclear Material Transfers
• Is controlled documentation maintained for internal and external transfers?
• Have appropriate Reporting Identification Symbols been established for the facility?
• Are internal transfers monitored on a graded safeguards basis?

6.4 Access, Containment, and Surveillance

The purpose of the access, containment, and surveillance program is to ensure that nuclear material is not removed from an authorized location without approval or timely detection. The program is intended to provide graded protection for all nuclear material consistent with the graded safeguards concept.

Lines of Inquiry for Access, Containment, and Surveillance
• Are access controls appropriate for the material category?
• Are transfer procedures complete and appropriately implemented?
• Is the two-person rule used effectively?
• Are the appropriate material surveillance programs in place for Cat I and II material?
• Are material access areas and protected areas appropriately established?
• Are TIDs properly controlled and maintained?
• Are portal monitor tests effective and timely?
• Is waste monitoring appropriate and comprehensive?
• Are the Daily Administrative Checks comprehensive and complete?

7.0 CLASSIFICATION AND INFORMATION CONTROL

7.1 Scope

The inspection of Classification and Information Control will include the following sub-topical areas: Program Administration; Authorities; Guidance; Training; Document Reviews; and Program Evaluation. A review of site specific procedures and interviews of personnel responsible for the sub-topical areas will be accomplished. A random sample of classified, UCNI, Official Use Only (OUO) and unclassified documents will be reviewed.

7.2 Program Administration

Classification, UCNI, and OUO programs are administered and overseen by a Classification Officer (CO) to ensure classified, UCNI, and OUO information is identified and protected. Most programs are administered by a local CO who is primarily responsible for the programs. If a CO has not been designated for a particular site, the site may have an agreement with another CO to act in that capacity for the local programs.
Lines of Inquiry for Classification and Information Control Program Administration

Resources

- Have adequate resources been provided to fulfill the classification and unclassified controlled information program requirements contained in DOE directives?
- Does the CO receive assistance from another CO (e.g., for training or guidance distribution)?
- If so, is there a written agreement that describes specifically what support is provided?
- Is the CO responsible for implementation of the OUO directives in the field element?
- Does the CO or staff have any duties not related to classification, UCNI, or OUO? If so, what are they?
- What percentage of time is spent by the CO [and each staff member] on work related to classification, UCNI, and OUO?
- Are there adequate resources to ensure the timely completion of all work related to classification, UCNI, and OUO?
- Is there any work related to classification, UCNI, or OUO that has been delayed or left undone due to pressure of other work or lack of available resources?
- If so, describe the work that cannot be completed, and explain the reason the work could not be completed (e.g., insufficient resources, other priorities, etc.).
- Has the CO requested additional resources?

Program Administrator

- Is there a CO located within the field element?
- If not, where is the CO located?
- Is there an agreement for support between the field element and the organization where the CO is located?
- If the CO is not located within the field element, has the field element appointed a Classification Coordinator?
- Has the Classification Coordinator attended the required briefing?
- Does the CO have a scientific or technical degree related to the field in which he/she is working?
- If so, specify the degree(s).
- If not, provide a description of the relevant work experience.
- Is the CO an original classifier (OC) (Federal COs only), derivative classifier (DC), and derivative declassifier (DD)?
- Has the CO completed the required training?

Performance Evaluation

- Are OCs, the CO, and the Classification Coordinator (if appropriate) evaluated on management of classified information?
- How many DCs’ and DDs’ duties significantly involve the creation of classified information?
• How do you determine which DCs and DDs must be rated on management of classified information.
• Explain how the evaluation is conducted (e.g., annual personnel performance rating system, personnel evaluations based upon the Integrated Safeguards and Security Management system, or an organization’s internal self-assessment system.)

Locally Issued Procedures

• Are the locally issued CIC procedures consistent with DOE directives?

Deviations

• Have any deviations from DOE classification, UCNI, or OUO directive requirements been approved by the Office of Classification, and do they continue to be necessary?

7.3 Authorities

DOE classification and UCNI programs are implemented by certified officials. Classification and UCNI officials must be trained and tested prior to receiving authority. Authorities are granted for specific subject areas, for a specific position and for a specific period of time. This sub-topical area evaluates whether or not each official has current authority in the subject areas they work and if there are sufficient DOE classification and UCNI officials to support site operations.

Lines of Inquiry for Authorities

Authority Distribution

• Are the type and scope of authority and numbers of officials sufficient for the classification and information control programs to fulfill DOE directive requirements?

Authority Descriptions

• Does each authority description meet DOE requirements?

Certification

• Has each appointed Derivative Classifier (DC) and Derivative Declassifier (DD) successfully completed required training and an examination prior to being granted such authority; successfully completed an examination for recertification; and, been recertified during the required time frame?
• Has each UCNI Reviewing Official (RO) completed training prior to being granted authority?
7.4 Guidance

Appropriate guidance is critical for classification and UCNI determinations. Locally issued guidance must be reviewed at least every five years for consistency with DOE directive requirements and guidance and each official must have access to appropriate guidance. Additionally, Contract Security Classification Specification (CSCS) forms are reviewed to determine if DOE contract guidance is appropriate and guidance for Work for Others (WFO) does not contradict DOE guidance.

Lines of Inquiry for Guidance
- Does each DC, DD, and UCNI RO have access to appropriate guidance that is current?
- Is locally issued guidance approved by the appropriate authority?
- Does locally issued guidance meet DOE directive requirements and not contradict DOE-approved guidance?
- Is locally issued guidance reviewed at least once every five years to ensure consistency with DOE directive requirements, and is the review documented?
- Has DOE Form 470.1, Contract Security Classification Specification, been completed for contracts that require access to classified information; all information required by DOE directive requirements been identified; and an authorized person certified that the information is correct?
- Has classification guidance that does not contradict DOE guidance been provided by the funding organization for all classified non-DOE and non-NNSA funded work (i.e., WFO)?

7.5 Training

Training is critical to ensure each person with a clearance and each official understands the classification and UCNI programs and their responsibilities within the programs. Training must be consistent with DOE directive requirements, including content, who receives it, and how often it is required. To evaluate the training component, submitted training material is reviewed, training may be observed, and trainers and DCs who attended training are interviewed.

Lines of Inquiry for Training
- Were training materials consistent with DOE directive requirements when last presented?
- Has each person authorized access to classified information received annual classification refresher training?
- Has each person authorized access to classified information who is working in a classified subject area received subject-matter-related classification awareness briefings.

7.6 Document Reviews

Reviews are conducted to determine if documents have been correctly classified (level and category), declassified or determined to contain unclassified controlled information. The review also determines if the documents are marked in accordance with DOE Manual 475.1-1A, Identifying Classified Information.
Lines of Inquiry for Document Reviews

- Are documents and materials correctly classified or controlled based on appropriate guidance by an appropriate authority and according to DOE directive requirements?
- Has all required information for documents that have been declassified and determined to be publicly releasable been submitted to the Office of Scientific and Technical Information for inclusion on OpenNet?
- Has the CO notified the appropriate authority of any declassification review that exceeds 25,000 pages, and followed a properly prepared large-scale review plan?

7.7 Program Evaluation

It is critical for all programs to periodically evaluate their own effectiveness. Without sufficient feedback, programs may be unaware that the processes and procedures developed are not effective. Programs that have subordinate organizations must conduct oversight reviews of such organizations and ensure they perform a self-assessment. All self-assessments and oversight reviews must meet DOE directive requirements and perform a valid evaluation of program performance.

Lines of Inquiry for Program Evaluation

- Has a written self-assessment been conducted in accordance with DOE directive requirements?
- Has an oversight review of each subordinate organization been conducted in accordance with DOE directive requirements?
- Have appropriate corrective actions been taken within the specified timeframe to address findings that are still valid from previous oversight reviews?
- Has an annual review of a sample of classified and unclassified documents generated in classified subject areas been conducted and documented?

8.0 CLASSIFIED AND UNCLASSIFIED CYBER SECURITY

8.1 Scope THIS SECTION NEEDS INPUT FROM HS-62*****

The Cyber Security inspection process will evaluate the effectiveness of DOE, NNSA, and contractor line management in protecting the integrity of classified and unclassified information systems consistent with Federal, DOE, and NNSA policies and requirements. The inspection will include evaluations of aspects of site and Integrated Safeguards and Security Management and Federal Information Security Management Act (FISMA) processes relating to cyber security.

8.1.1 Cyber Security Program Management and Implementation

The inspection evaluates those elements that are considered essential for an effective cyber security program consistent with applicable Federal, DOE, and NNSA directives and guidance. Inspection activities will include a review of documentation to ensure adequate program planning and compliance with Federal, DOE, and NNSA directives and guidance. Interviews with line managers and information management specialists will be performed to ascertain knowledge of policies and requirements and to determine if essential elements for an effective cyber security program are in
place. Performance testing will be utilized to measure the effectiveness of site cyber security programs.

8.1.2 Performance Testing

Independent Oversight typically conducts both internal and external penetration testing of unclassified computer networks. External testing assesses the site's effectiveness in addressing threats from the Internet, (e.g., hackers, foreign intelligence agencies, economic competitors). Internal penetration testing addresses threats from authorized users (e.g., disgruntled employees, visiting researchers, and foreign nationals) seeking access to information or computer services for which they are not authorized. Internal testing assesses the site's ability to keep authorized users (both classified and unclassified) from migrating beyond predetermined "need-to-know" boundaries or to disrupt or inappropriately modify information.

Penetration testing is conducted in four phases - information gathering, scanning, penetration, and reporting. During penetration testing, various tools and techniques are applied to identify vulnerabilities associated with the site's computer systems, and attempt penetrations of networked computers to assess the significance of these vulnerabilities. Testing includes employing techniques, such as footprinting, scanning, enumeration (making active connections to systems and directed queries), gaining access to systems, and escalating privileges.

A Technical Assessment Protocol document will be developed to establish an agreed upon framework for the conduct of performance testing between the designated approval authority, within NNSA and Independent Oversight. Independent Oversight will work with the designated approval authority to provide for certification and accreditation of techniques and tools to be utilized during testing as needed.

8.2 Program Management

Performance Objective: DOE Program and Site Office managers are actively engaged in the protection of classified and unclassified information through effective cyber security management processes.

Lines of Inquiry

- Line managers establish clear cyber security roles, responsibilities, authorities, delegations and interfaces between DOE Headquarters, field organizations, and the site including coordination of line management direction from multiple program offices.
- Expectations for cyber security performance for DOE, NNSA, contractor, and other organizations are established and communicating, through contracts and other mechanisms.
- DOE Headquarters and field office line management are involved in, cognizant of, and supportive of priorities associated with cyber security.
- Timely and sufficient guidance is provided on expectations for implementation of cyber security requirements, standards, and DOE and NNSA initiatives.
bullet Cyber security requirements are incorporated into binding agreements, such as a contract, to ensure timely implementation by contractors, subcontractors, and other organizations utilizing DOE and NNSA information technology resources.
bullet System security plans for classified and unclassified systems are reviewed and approved to ensure protection strategies are appropriate and effective.
bullet DOE and NNSA line management has an understanding of and accepts the residual risk for operating classified and unclassified information technology systems.
bullet Effective, performance-based processes for monitoring and assessing contractor cyber security performance are established consistent with DOE Order 226.1.
bullet DOE/NNSA line managers ensure that evaluations are conducted at required intervals and are effective in evaluating the structure and effectiveness of classified and unclassified cyber security programs.
bullet Contractors and personnel are held accountable for the effectiveness of cyber security performance.

Performance Objective: Line managers within operating organizations (Federal and contractor) take necessary actions to establish effective cyber security policies and programs.

Lines of Inquiry
bullet Senior site line managers demonstrate a commitment to cyber security and promote its understanding, acceptance, and timely implementation. Additionally, initiatives to improve classified and unclassified cyber security programs are championed, as appropriate.
bullet An appropriate set of policies and performance expectations are established and communicated consistent with applicable Federal, DOE, and NNSA directives and guidance.
bullet Challenging cyber security program goals are established and tracked to accomplishment through performance metrics. Organizations and individuals are held accountable for cyber security performance.
bullet Both horizontal and vertical integration of cyber security is performed throughout organizational functions at all organizational levels.
bullet Managers and supervisors at all levels accept, actively promote, and set an appropriate example for the integration of cyber security into site activities.
bullet Roles, responsibilities, and authorities for cyber security are clearly defined, documented and understood (including line managers, cyber security staff, computer operations staff, and computer users).
bullet Cyber security responsibilities and authorities flow down from senior management to each person utilizing or interfacing with classified and unclassified information systems.
bullet Functional relationships and responsibilities are clearly defined among all organizational entities that share information technology resources or are incorporated within the site’s trusted network structure.
bullet All DOE, NNSA and contractor personnel, including managers, supervisors, administrators, and users are held accountable for cyber security performance through a combination of performance expectations, incentives, and negative consequences for poor performance.
bullet Risk-based, decision-making processes are utilized to resolve disputes, establish priorities, and balance operational needs against cyber security requirements.
• Effective, consistent, and risk-based decision-making processes are established for appropriately funding cyber security, including providing resources for addressing identified issues, deficiencies, and commitments.
• System administrators, users, project managers, and stakeholders are involved in the prioritization and allocation of resources to maintain an appropriate balance between operational needs and cyber security requirements.
• Effective management systems are established that link cyber security issues, commitments, and deficiencies to business mechanisms associated with planning, prioritizing, and budgeting.
• Effective management processes are in place to ensure that the certification and accreditation of systems is in accordance with Federal, DOE, and NNSA directives and the FISMA requirements.

8.3 Program Implementation

8.3.1 Define the Scope of Work

Performance Objective: The architecture of information networks are sufficiently defined and understood so that risks to networks and information resources can be assessed. Processes are in place to define the scope of new work activities and projects so that changes in risk can be evaluated.

Lines of Inquiry
• The architecture of information systems is sufficiently defined to allow for an accurate analysis of cyber security risks. Site personnel understand network configurations, and risk assessments are based upon accurate parameters.
• Information systems performing critical and mission essential functions are identified so that risk can be properly assessed.
• The site ISSM/Departmental Cyber Security Management system provides for integration of cyber security into all applicable business processes. Cyber security needs are considered when defining new projects and/or work activities.
• Formal processes are established that incorporate cyber security considerations over the life cycle of projects to achieve Federal, DOE, and NNSA expectations for security.
• The site’s hierarchy of work planning processes provides increasingly detailed descriptions of the work at successively lower tiers such that broad mission objectives are translated into discrete tasks that address cyber security needs.
• The level of detail and formality in the work scope definition is commensurate with the importance of the work, its complexity, and potential threats to information technology systems.
• The definition of a scope of work is an integrated and collaborative activity that considers cyber security and involves all appropriate organizational units.
• Cyber security personnel, workers, program personnel, and stakeholders are actively involved in providing an appropriate balance between mission objectives and protection of DOE and NNSA information technology resources.

8.3.2 Analyze the Risk
Performance Objective: Systems and procedures are developed and effectively implemented to ensure that risks to DOE and NNSA information technology resources are identified, appropriately analyzed, mitigation strategies are developed, and management accepts residual risks.

**Lines of Inquiry**
- Threats, vulnerabilities, and risks associated with DOE and NNSA information technology systems are identified and continually assessed.
- Mechanisms/mitigation strategies are established to gather threat and vulnerability information to be considered during risk assessments.
- A disciplined, documented, methodical, and collaborative approach for ongoing cyber security risk assessments is established and consistently implemented.
- Knowledgeable information technology professionals, system administrators, and users are involved in the risk assessment process.
- Residual risks are identified and accepted by line management and DOE/NNSA management.

**8.3.3 Develop and Implement Security Measures**

Performance Objective: Management systems are established and effectively implemented to ensure development of controls to minimize risk to DOE and NNSA information technology systems. Residual risks are understood and accepted by DOE, NNSA and contractor line managers.

**Lines of Inquiry**
- Protection strategies are appropriately tailored to address risks associated with operating classified and unclassified DOE and NNSA information management systems.
- Effective risk mitigation strategies are established for DOE and NNSA information technology systems over their life cycle to reduce or mitigate threats.
- Protection strategies are considered in terms of near-term and long-term solutions and other factors (such as assigned mission, reliability, system performance, timeliness, life-cycle costs, and technical barriers). Management establishes a preferred hierarchy in the identification of security controls that promotes engineered/technical solutions ahead of administrative controls.
- Compensatory measures are identified to address unacceptable risks until time and resources are available to implement more optimal controls.
- Processes are established for managing cyber security requirements, including the translation of requirements and guidance into policies, programs, and procedures.
- Requirements are commensurate with the threat and risk to information technology systems (i.e., the cyber security requirements identification process is linked to the risk management process).
- Site policies, guidance, and procedures conform to Federal, DOE, and NNSA cyber security requirements and guidance.
- Cyber security requirements are appropriately incorporated into the site’s cyber security systems security plans for classified and unclassified systems.
- Where necessary, procedures are established that tailor site requirements to specific situations and provide sufficient detail to implement cyber security requirements at the working level.
• Line management formally accepts residual risk associated with the DOE and NNSA information technology resources prior to their operation. Additional cyber security controls are put in place if the level of residual risk is unacceptable to line management.
• Cyber security controls are appropriately documented in cyber security systems security plans for classified and unclassified systems in a manner that assures technical accuracy, usability, and quality. These plans are maintained current and accurate.
• The site has formal certification and accreditation processes in place to test, implement, manage, maintain, and revise cyber security controls as necessary to be effective.
• Significant changes in design, life cycle, operations, or conditions are analyzed for their impact on the protection of information technology resources, and ensuring that cyber security controls are modified as appropriate.
• The site’s network perimeter is clearly defined and line management establishes controls that provide adequate protection for information technology resources.
• Processes are established to control user access to classified and unclassified information stored electronically on information technology systems by establishing strong “need-to-know” controls. This includes establishing “need-to-know” boundaries within networks to protect sensitive information such as UCNI and personally identifiable information.
• Stringent controls over uploading and downloading files between classified and unclassified systems are established and verified.
• Appropriate controls are established for classified and unclassified laptop computers and portable electronic devices to mitigate the additional risk associated with the portability of these devices.
• Communication mechanisms are established to ensure that managers, system administrators, and users remain aware of cyber security policies, procedures, and guidance applicable to their responsibilities.
• Specifications are established for the necessary levels of education, experience, and training for technical cyber security personnel. Needs analysis and job/task analysis are used to support staffing level determinations and training requirements.
• Critical cyber security skills are identified that are needed to implement cyber security measures. Short-term and long-term strategies are established for recruiting and retaining competent personnel.
• Processes are in place so that all managers and users are adequately trained on cyber security risks, policies, and requirements prior to being given access to DOE and NNSA information technology resources. Annual training is provided to ensure that all managers, users, and technical personnel maintain this understanding.

8.3.4 Perform Work within Measures and Controls

Performance Objective: Line management ensures that authorized cyber security measures are in place and that work is performed consistent with security requirements.
Lines of Inquiry

- Personnel are qualified and knowledgeable of their responsibilities as they relate to cyber security controls and work performance.
- Cyber security staffing levels are adequate to maintain an effective program.
- Mechanisms are in place so that only qualified and competent personnel are assigned to technical work activities associated with securing and maintaining DOE and NNSA information technology resources.
- Personnel are qualified and trained to implement controls in accordance with established cyber security requirements, policies, and procedures.
- Responsibilities and authorities for verifying readiness to operate information technology resources are defined, including the appropriate level of review and approval for accrediting systems.
- The formality and rigor used to confirm readiness is based on the level of threat and risk.
- Agreeing upon controls and requirements are established for operating information technology resources prior to operations being initiated. DOE/NNSA has either directly authorized (where appropriate) or delegated approval authority, within clearly defined limits, to the contractor.
- Network and standalone system operations are conducted within established controls and follow requirements.
- Processes are in place for withdrawing accreditation/operations authorization for information technology systems deemed to be inadequately secured or protected.
- Site personnel adhere to cyber security controls and follow established procedures as a means to ensure adequate protection of DOE and NNSA classified and unclassified information technology resources.
- Managers, system administrators, and users appropriately implement the requirements for password protection and access controls in order to protect information technology resources from unauthorized use.
- DOE’s Banner and Warning Policy is appropriately implemented on all DOE and NNSA information technology resources.
- Processes are in place to evaluate “need-to-know” requirements for individual managers and users. Additionally, line management ensures effective implementation of “need-to-know” boundaries within networks to protect classified and unclassified information.
- Configuration management processes are established to control hardware and software modifications associated with site information technology systems to prevent existing controls from being undermined through the introduction of vulnerabilities.
- Ongoing monitoring and auditing of information technology systems is performed to ensure that configurations remain secure and unauthorized activities are prevented.
- Processes for reporting/responding to computer security incidents are established.
- Systems security plans for classified and unclassified systems are fully implemented and effective in protecting information technology resources.
- Computers are appropriately sanitized prior to their disposal or release.

8.3.5 Provide Feedback and Continuous Improvement
Performance Objective: Line management has established formalized mechanisms and processes for collecting both qualitative and quantitative information on cyber security performance. This information is effectively collected and used as the basis for informed management decisions to improve the security of information technologies through assessments, performance measures, and other feedback mechanisms.

**Lines of Inquiry**

- Processes are established consistent with DOE Order 226.1 for planning and conducting self-assessments, management assessments, and performance-based testing. Assessment activities are effective in identifying cyber security issues and weaknesses associated with current performance.
- Feedback from managers, systems administrators, and users is collected as a means of identifying potential improvements to cyber security. Managers, system administrators, and users participate in self-assessment activities.
- Results of assessments and other performance information are reported to senior management to enable informed determinations as to the effectiveness of ISSM/DCSM and cyber security performance.
- Mechanisms are established to identify applicable cyber security lessons learned from government and industry sources. Lessons learned are communicated to appropriate personnel through training, bulletins, and other avenues.
- Appropriate performance measures are used to monitor cyber security program effectiveness. Performance measures are linked to performance objectives and expectations established by line management.
- As part of its commitment to continuing cyber security program improvements, site personnel are cooperative with and responsive to evaluations conducted by DOE and external oversight organizations.
- Appropriate corrective actions are established in responses to identified deficiencies, adverse trends in performance measures, programmatic issues, recurring events, or other indicators by implementing meaningful corrective actions.
- Corrective actions include the assignment of responsibility for actions, identifying milestones, and committing resources.
- Processes are in place to ensure that corrective actions are incorporated into plans of actions and milestones to include site, Independent Oversight, and Inspector General identified issues and findings and that they are appropriately reported.
- Cyber security incidents and deficiencies (identified by any source) are analyzed to determine root causes, systemic issues, and measures actions to prevent recurrence.
- Cyber security issues and associated corrective actions are tracked to completion. Status information on corrective action completion is provided to site managers.
- Issues and corrective actions are appropriately prioritized on the basis of risk. Closure of deficiencies and corrective actions is based on objective, technically sound and verified evidence.