

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

<b>DOE Directive</b>	<b>Requirement Citation</b>
<p><b>DOE M 470.4-1 Chg 1</b>  (Manual, 03-07-06)  <b>Safeguards and Security Program Planning and Management</b></p>	<p><b>CONTRACTOR REQUIREMENTS DOCUMENT</b></p> <p><b>ATTACHMENT 2</b></p> <p><b>PART 1 – PLANNING AND EVALUATION</b></p> <p><b>SECTION A – SAFEGUARDS AND SECURITY PROGRAM PLANNING</b></p> <p><b>2. REQUIREMENTS</b></p> <p>c. <b><u>S&amp;S Program Operations:</u></b> Actions must be taken to ensure an acceptable S&amp;S program</p> <hr/> <p>2. c. (1) <u>Site-specific Characterization.</u> Protection programs must be tailored to address specific site characteristics and requirements, current technology, ongoing programs, and operational needs to achieve acceptable protection levels that reduce risks in a cost- effective manner.</p> <hr/> <p>2. c. (2) <u>Threat/Policy Guidance.</u> DOE O 470.3, Design Basis Threat (DBT) Policy must be used with local threat guidance during the conduct of vulnerability assessments (VAs) for protection and control program planning.</p> <hr/> <p>2. c. (3) (a) <u>Targeted Protection Strategies</u> (Strategies for the physical protection of SNM and vital equipment must incorporate the applicable requirements established in DOE M 470.4-2, Physical Protection.</p> <hr/> <p>2. c. (3) (f) Strategies for the protection of government property not covered above must reflect a graded approach.</p> <hr/> <p><b>3. PLANNING</b></p> <p>a. S&amp;S plans must be developed for facilities with any of the following S&amp;S interests:</p> <ul style="list-style-type: none"> <li>(2) Category IV SNM;</li> <li>(5) intra/intersite transportation of SNM</li> <li>(7) facilities engaged in the protection of Government property</li> </ul>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

<b>DOE Directive</b>	<b>Requirement Citation</b>
<b>DOE M 470.4-1 Chg 1</b> (Manual, 03-07-06) <b>Safeguards and Security Program Planning and Management</b>	3. c. Site Security Plan (SSP). At locations where an SSSP is not required because of limited scope of interests, an SSP must be developed by the contractor to describe the protection program.
	<p><b>SECTION A</b>  <b>APPENDIX 1 – SAFEGUARDS &amp; SECURITY MANAGEMENT PLAN</b></p> <p>The Safeguards and Security (S&amp;S) Management Plan provides a description of the contractor’s implementation of S&amp;S policy and provides detailed information on the assignments of roles, responsibilities, and authorities as well as the development of budgets an allocation of resources (<b>as stated in the LBNL Site Security Plan</b>).</p>
	<p><b>SECTION B – SECURITY CONDITIONS</b></p> <p>1. OBJECTIVE. To ensure that the Department uniformly meets the requirements of the Homeland Security Advisory System outlined in HSPD-3.</p> <p>3. e. A record of specific actions taken for each measure must be maintained.</p>
	<p><b>SECTION F – PERFORMANCE ASSURANCE PROGRAM</b></p> <p>1. OBJECTIVE: To demonstrate the effectiveness of the protection provided Departmental safeguards and security (S&amp;S) interests by systematically evaluating all protection program essential elements.</p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<p><b>DOE M 470.4-1 Chg 1</b>  (Manual, 03-07-06)  <b>Safeguards and Security Program Planning and Management</b></p>	<p><b>SECTION G – SURVEY, REVIEW, AND SELF-ASSESSMENT PROGRAMS</b></p> <p><b>2. REQUIREMENTS</b></p> <p>a. <u>Types and Frequencies of Surveys and Assessments.</u></p> <p>(1) <u>Initial surveys.</u> Initial surveys must be conducted at facilities where there will be a facility clearance established for a facility with an importance rating of: A,B, C, or PP.</p> <hr/> <p>2. a. (2) <u>Periodic Surveys.</u> Periodic surveys are conducted for all facilities and must cover all applicable topics to ensure survey program objective are met.</p> <p>(a) Facilities with importance ratings of A, B, or C must be surveyed once every 12 months (with the exception of Category IV SNM only facilities – (see [c] below).</p> <p>(b) Facilities with an importance rating of PP must be surveyed once every 24 months.</p> <p>(c) For facilities with Category IV SNM and nuclear material, including source material, the nuclear material control and accountability (NMC&amp;A) topical area must be surveyed at least every 24 months.</p> <hr/> <p>2. a. (4) <u>Termination Surveys.</u> Termination surveys must be conducted to verify the termination of Departmental activities and appropriate disposition of S&amp;S interests. Examples of survey activities include: the appropriate disposition, destruction, or return of classified information or matter, SNM, hazardous material, property, security badge retrieval, debriefings, and verification of the termination or transfer of Department of Energy (DOE) access authorizations.</p> <p>(a) Onsite termination surveys must be conducted at facilities possessing Top Secret matter, sensitive compartmented information (SCI/special access program (SAP) information or matter, or SNM</p> <p>(b) Onsite or correspondence termination surveys must be accomplished for all other possessing facilities.</p> <hr/> <p>2. a. (6) <u>Self-Assessments.</u> Contractors must conduct self-assessments between periodic surveys conducted by the cognizant security authority and include all applicable facility S&amp;S program elements,</p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<b>DOE M 470.4-1 Chg 1</b> (Manual, 03-07-06) <b>Safeguards and Security Program Planning and Management</b>	<p>2. a. (7). <u>Reviews or Inspections by Other DOE Elements or OGAs</u>. Reviews/inspections conducted by other DOE elements (including site quality assurance programs) or OGAs may be used to meet survey requirements. When using reviews/inspections conducted by other organizations to meet the requirements of the survey, these guidelines must be followed.</p> <p>(a) The review/inspection must have been conducted within the survey period.            (b) Applicable portions of the review/inspection must be attached to the survey report.            (c) Portions of topical and subtopical areas not covered by the review/inspection must be surveyed.            (d) If ratings were not assigned during the review/inspection, the surveying office must analyze the impact of any deficiencies and assign ratings.</p>
	<p>2. a. (8) <u>Extension of Frequency</u>. The results of previous surveys may affect the frequency of future surveys. Contractors may require that the interval between periodic surveys be increased up to 24 months by the DOE cognizant security authority. Documentation of the justification for increases in the interval of periodic surveys must be maintained by the DOE cognizant security authority.</p>
	<p>2. a. (8) (a) The following conditions must be met for extensions:</p> <ol style="list-style-type: none"> <li>1 the facility was rated satisfactory during the most recent survey activity</li> <li>2 the facility has not unmitigated deficiencies that impact the security posture of the facility, and all applicable topical area ratings are satisfactory from the previous survey; and</li> <li>3 all applicable topical area ratings from the most recent self- assessment are satisfactory, and the DOE cognizant security authority concurs with the ratings.</li> </ol>
	<p>2. a. (8) (c) All modifications to survey frequency requirements must be documented in the Safeguards and Security Information Management System (SSIMS).</p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<p><b>DOE M 470.4-1 Chg 1</b>  (Manual, 03-07-06)  <b>Safeguards and Security Program Planning and Management</b></p>	<p>2. b. <u>Scope and Methodologies</u>. Surveys and self-assessments must provide an integrated evaluation of all topical and subtopical areas to determine the overall status of the S&amp;S program and ensure the objectives of this section are met (see paragraph 1 above). The integrated evaluation is a comprehensive synergistic approach using multiple S&amp;S program elements that ensures total system effectiveness and, if properly implemented, will meet the objectives identified in paragraph 1 above. The scope of these activities and the methods used must include those listed below.</p> <p>(1) <u>Compliance</u>. Compliance reflects the status of the S&amp;S program as measured against implementation of applicable Federal statutes, regulations, policies approved site safeguards and security plans (SSSPs)/site security plans (SSPs), and other approved security plans.</p>
	<p>2. b. (2) <u>Performance</u>. Performance indicates the degree to which the elements of the S&amp;S program meet protection objectives based on the operations testing of program elements.</p> <p>(3) <u>Comprehensiveness</u>. Comprehensiveness identifies the breadth of protection afforded all activities and interests within a facility. This is accomplished by an evaluation of the adequacy and effectiveness of programs and a thorough examination of the implementation of policies, practices, and procedures to ensure compliance and performance. All applicable topical areas identified on DOE Form (F) 470.8, “Survey/Inspection Report” Form, must be evaluated.</p> <p>(4) <u>Other</u>. The scope of special and termination surveys is determined by the DOE cognizant security authority in coordination with the surveying office. Determinations of survey scope are predicated on the nature or status of operations at the facility, activity, or element being surveyed. These surveys may not cover all topical areas identified on DOE F 470.8.</p>
	<p>3. <u>CONDUCT</u>. Local survey and self-assessment procedures implementing this section must be developed, documented, and approved by the cognizant security authority. Procedures must ensure completion of the objectives contained in paragraph 1 above and must include the requirements listed below.</p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<p><b>DOE M 470.4-1 Chg 1</b>  (Manual, 03-07-06)  <b>Safeguards and Security Program Planning and Management</b></p>	<p>3. a. <u>Team Composition</u>. Contractor line management must determine that contractor survey and self-assessment team members possess qualifications, experience, and training sufficient to review and inspect the topical/subtopical areas of the survey/self-assessment. The National Training Center (NTC) provides training courses for survey/self-assessment team leaders and team members.</p>
	<p>3. b. <u>Planning, Scheduling, and Integration</u>. Surveys and self-assessments must be planned, scheduled, and conducted in an integrated manner to achieve the objectives identified in paragraph 1 above. If topical and subtopical area evaluations are performed separately, the surveying office must document and integrate the results of each into a single (periodic) survey report that includes a composite facility rating. The frequency between topical and subtopical areas cannot exceed the frequency for the single (periodic) survey.</p>
	<p>3. c. <u>Validation</u>. Results must be validated by methods including, but not limited to, document review, performance testing, and interview analyses and observations.</p>
	<p>3. d. <u>Exit Briefing</u>. An exit briefing must be conducted with the surveyed or assessed organization to include the minimum facts:</p> <ul style="list-style-type: none"> <li>(1) program strengths and weaknesses, including all findings;</li> <li>(2) corrective action reporting requirements for all open findings, regardless of source; and</li> <li>(3) topical and composite ratings. For less than satisfactory ratings, the communication of the composite rating initiates the actions required in paragraph 8 of this section.</li> </ul>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<p><b>DOE M 470.4-1 Chg 1</b>  (Manual, 03-07-06)  <b>Safeguards and Security Program Planning and Management</b></p>	<p>4. <u>FINDINGS.</u>  a. <u>Identification and Documentation.</u> Findings are any validated program deficiency (failure to meet a performance or compliance requirement) regardless of source. Findings may be reflected in documents resulting from internal and external reviews, audits, appraisals, and other sources [e.g., Office of Independent Assessment and Performance Assurance (OA), the General Accountability Office (GAO), Office of the Inspector General (IG), previous surveys, self-assessments, etc.].</p> <p>All open findings must be reviewed during the survey or self-assessment to validate the status of corrective action and to evaluate the impact on the existing S&amp;S program.</p> <p>Findings identified during the current survey or self-assessment must be reported immediately to the Departmental element and contractor line management if a vulnerability to national security, classified information or matter, nuclear materials, or Department property results, or may result, in a programmatic impact to the Department. Findings identified during a survey or self-assessment, even if closed during the survey or self-assessment activity must be documented in the associated report.</p> <hr/> <p>4. b. <u>Tracking.</u> Findings and deficiencies, regardless of source, and corrective action plans (milestones and estimated completion dates) must be entered into SSIMS in accordance with SSIMS guidelines and tracked until closed. Quarterly status reports must be entered into SSIMS by January 15, April 15, July 15, and October 15 of each year. Self-assessment deficiencies are not required to be entered into SSIMS; however, a local mechanism system must be used to track these deficiencies and corrective action until closed.</p> <hr/> <p>4. c. <u>Trending.</u> Trending evaluations must be considered in the resolution of findings in the subtopical area of program management to determine if systemic and systematic causal factors exist within the S&amp;S program. Results of this evaluation that indicate negative trends must be analyzed to ensure corrective action plans, address root causes, and the need to ensure continuous improvement of the S&amp;S program.</p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<p><b>DOE M 470.4-1 Chg 1</b>  (Manual, 03-07-06)  <b>Safeguards and Security Program Planning and Management</b></p>	<p>5. RATINGS.</p> <p>a. <u>Types</u>. Ratings must be based on the effectiveness and adequacy of the program at a facility and reflect a balance of performance and compliance results as well as the impact of the deficiency(ies) (e.g., findings, IG recommendations, etc.) and mitigating factors. The ratings listed below must be used for all surveys (except termination), reviews, and self-assessments. Does not apply (DNA) and Not Rated (NR) may also be used in applicable situations.</p> <p>(1) <u>Types of Ratings</u>.</p> <p>(a) <u>Satisfactory</u>. The element being evaluated meets protection objectives or provides reasonable assurance that protection objectives are being met.</p> <p>(b) <u>Marginal</u>. The element being evaluated partially meets protection objectives or provides questionable assurance that protection objectives are being met.</p> <p>(c) <u>Unsatisfactory</u>. The element being evaluated does not meet protection objectives or does not provide adequate assurance that protection objectives are being met</p> <p>.</p> <p>(d) <u>Inspection Ratings</u>. "Effective Performance," "Needs Improvement," and "Significant Weaknesses" are indicators of a management system performance level as outlined in DOE 0 470.2B, Independent Oversight and Assurance Program.</p>
	<p>5. a. (2) <u>Rating Determinations</u>.</p> <p>(a) <u>Existing Conditions</u>. Ratings must be based on existing conditions at the end of the survey and not future or planned corrective actions or conditions.</p> <p>(b) <u>Impact</u>. Ratings must be based on the impact of all open deficiencies, regardless of source.</p> <p>(c) <u>Marginal or Unsatisfactory Ratings</u>. Less than satisfactory ratings in any topical area must be based on validated weaknesses in the S&amp;S system or deficiencies in performance.</p> <p>(d) <u>Topical Area Ratings</u>. A topical area rating must not be marginal for consecutive survey periods and must be assigned an unsatisfactory rating unless one of the following conditions applies.</p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<b>DOE M 470.4-1 Chg 1</b> (Manual, 03-07-06) <b>Safeguards and Security Program Planning and Management</b>	5. a. (2) (d) 1 The current survey of the topical area results in a satisfactory rating. 2 The previous survey that resulted in a marginal rating identified different deficiencies and reasons for the rating. 3 The deficiencies and reasons that were the basis for the previous marginal rating were related to the completion of a line item construction project (LICP) or upgrade program. In that case, acceptable interim measures must have been implemented, physically validated pending completion of the project, and documented in the survey report.
	5. a. (2) (e) <u>Subtopical Ratings</u> . The decision whether or not to use all subtopical ratings must be documented in local procedures. <sup>21</sup> Regardless of the rating method used, the report must include the evaluation of all required subtopical areas which must be used as part of the appropriate topical area rating justification and rationale.
	5. a. (2) (f) <u>Justification and Rationale</u> . All ratings must be supported and documented to include the rating justification and rationale.
	6. <u>REPORT CONTENT</u> . a. <u>Initial/Periodic Survey Reports and Self-Assessment Reports</u> . Reports (to include self-assessment reports) must contain the following items. (1) A completed DOE F 470.8 or equivalent for self-assessments.
	6. a. (2) An executive summary containing: (a) the scope, methodology, period of coverage, duration, date of the exit briefing to management; (b) a brief overview of the facility, function, scope of operations, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security and overall scores assigned to the most recent contract appraisal); (d) the overall composite facility rating with supporting rationale; (e) a reference to a list of findings identified during the survey or self-assessment.

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<b>DOE M 470.4-1 Chg 1</b> (Manual, 03-07-06) <b>Safeguards and Security Program Planning and Management</b>	6. a. (3) An introduction containing: <ul style="list-style-type: none"> <li>(a) the scope, methodology, period of coverage, duration, date of the exit briefing to management; and</li> <li>(b) a description of the facility, its function and scope of operations, security interests, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security and overall scores assigned to the most recent contract appraisal).</li> </ul>
	6. a. (4) Narrative for all rated topical and subtopical areas that includes: <ul style="list-style-type: none"> <li>(a) a description of the site's implementation of the program element;</li> <li>(b) the scope of the evaluation;</li> <li>(c) a description of activities conducted;</li> <li>(d) the evaluation results and associated issues (including other Department elements or OGA review or inspection results related to this topic/subtopic that were included);</li> <li>(e) the identification of all findings, including new and previously identified open findings, regardless of source (e.g., OA, IG, GAO), and their current corrective action status; and</li> <li>(f) an analysis that provides a justification and rationale of the factors responsible for the rating.</li> </ul>
	6. a. (5) Attachments, including: <ul style="list-style-type: none"> <li>(a) a copy of the current DOE F 470.2, "Facility Data and Approval Record" (FDAR);</li> <li>(c) a listing of all new findings resulting from the survey/selfassessment;</li> <li>(d) a listing of all previous findings that are open to include the current status of corrective action;</li> <li>(e) a listing of team members, including names, employer, and their assigned area(s) of evaluation; and</li> <li>(f) a listing of all source documentation used to support the survey/self-assessment conduct and results (e.g., GAO, IG, OA, and similar assessment documents).</li> </ul>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<p><b>DOE M 470.4-1 Chg 1</b>  (Manual, 03-07-06)  <b>Safeguards and Security Program Planning and Management</b></p>	<p>6. b. <u>Special Survey Reports</u>. Special survey reports must follow the format and content for initial and periodic survey/self-assessment reports except that an executive summary is not required. Attachments must be included as appropriate to the scope of the special survey.</p>
	<p>6. d. <u>Termination Survey Reports</u>. Termination survey reports must include:</p> <ul style="list-style-type: none"> <li>(1) verification of non-possession of classified information or matter, SNM, hazardous material presenting a potential sabotage threat, or Government property;</li> <li>(2) verification that all DOE access authorizations have been terminated or transferred and that termination statements have been completed and security badges have been accounted for;</li> <li>(3) validation that all findings have been closed in SSIMS;</li> <li>(4) verification of termination of all S&amp;S activities;</li> <li>(5) a copy of the terminating DOE F 470.2, FDAR; and</li> <li>(6) a completed certificate of non-possession.</li> </ul>
	<p>6. e. <u>Memorandum Report Content</u>. Memorandum reports for DOE programmatic entities and OGAs are generated when it is inappropriate to transmit a copy of the survey report due to need-to-know issues. Reports must contain:</p> <ul style="list-style-type: none"> <li>(1) a notification of inclusion of their activity in the survey;</li> <li>(2) the date of the survey;</li> <li>(3) ratings and rationale for the ratings associated with the activity; and</li> <li>(4) all findings applicable to that activity.</li> </ul>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
 As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<p><b>DOE M 470.4-1 Chg 1</b>            (Manual, 03-07-06)  <b>Safeguards and Security Program Planning and Management</b></p>	<p>9. <u>NOTIFICATION AND ACTION FOR LESS THAN SATISFACTORY SELFASSESSMENT COMPOSITE RATINGS</u>. Actions required in response to less than satisfactory self-assessment composite ratings are listed below:</p> <p>a. <u>Marginal Ratings</u>. Within 15 working days of the determination of a marginal composite rating, notification must be made to line management that includes:</p> <p>(1) a statement identifying the vulnerability and rationale for the rating;</p> <p>(2) a description of the corrective action/compensatory measures taken to date; and</p> <p>(3) a statement acknowledging physical validation of the adequacy of items listed in paragraph 9a(2) above.</p>
	<p>10. <u>CORRECTIVE ACTIONS</u>. Corrective action plans must be developed for all open survey and self-assessment findings. Corrective action plans for survey and self-assessments must be submitted and reported within 30 working days after the date of the exit briefing. If a finding is corrected during the survey, it must be identified in the survey report with a description of the closure/validation performed by the survey/self-assessment team. Quarterly reports of the status of corrective actions for each finding must be provided to the DOE cognizant security authority. All survey and self-assessment corrective actions must:</p>
	<p>10. a. be based on documented root cause analyses, risk assessments, and cost-benefit analyses to ensure the survey/self-assessment program objectives are met (see paragraph 1 above) and</p> <p>b. be reported, entered, tracked, and updated until completed, validated, and closed in SSIMS, where applicable (see paragraph 4b above).</p>
	<p>11. <u>UPGRADE OF COMPOSITE RATINGS</u>. When line management determines that the composite rating should be upgraded, the survey/self-assessment team must physically verify the completion and adequacy of corrective actions and make notification of the rating upgrade in accordance with approved local procedures.</p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<b>DOE M 470.4-1 Chg 1</b> (Manual, 03-07-06) <b>Safeguards and Security Program Planning and Management</b>	12. <u>RECORDS RETENTION</u> . Documentation associated with the conduct of survey and self-assessment conduct must be retained in accordance with approved procedures and appropriate records inventory disposition schedules.
	13. <u>CONTINUOUS IMPROVEMENT PROCESS</u> . The cognizant security authority must conduct an annual evaluation of their survey or self-assessment processes. This evaluation must ensure any identified process improvements (i.e., lessons learned) are incorporated in the S&S survey/self-assessment process.
	<p><b>SECTION I – FACILITY CLEARANCES AND REGISTRATION OF SAGEGUARDS AND SECURITY ACTIVITIES</b></p> <p><b>CHAPTER I – FACILITY CLEARANCE (FCL) PROGRAM</b></p> <p>1. <u>GENERAL</u>. The FCL program regulates Departmental approval of a facility’s eligibility to access, receive, generate, reproduce, store, transmit, or destroy classified information or matter, special nuclear material (SNM), other hazardous material presenting a potential radiological, chemical, or biological sabotage threat, and/or Department of Energy (DOE) property worth more than \$5 million, exclusive of facilities and land values (hereinafter referred to as security activities).</p>
	<p><b>CHAPTER II – IMPORTANCE RATINGS</b></p> <p>1. <u>FACILITY IMPORTANCE RATINGS</u>. Importance ratings are used to identify the protection importance of facilities. Each facility’s assigned importance rating must be recorded on DOE F 470.2 FDAR.</p> <p>c. “C” Importance Ratings. Ratings assigned to those facilities that meet any of the following criteria: (1) government property of a significant value greater than \$5 million, exclusive of facilities and land values.</p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<p><b>DOE M 470.4-1 Chg 1</b>  (Manual, 03-07-06)  <b>Safeguards and Security Program Planning and Management</b></p>	<p><b>CHAPTER III – ORGANIZATIONAL STRUCTURES AND FCLs</b></p> <p>1. FCL FOR SINGLE LEGAL ENTITIES  a. Single FCL Registration. Only one FCL registration is required if the company and its classified security activities meet the following criteria.  (1) A centrally directed security program is maintained that covers all security activities.</p> <p>(2) The distance between the security activities is such that the contractor is able to maintain daily supervision of its operations, including day-to-day observations of the security program.</p>
	<p><b>CHAPTER VI – FACILITY CLEARANCE</b></p> <p>1. <u>REQUIREMENTS</u>. As part of the DOE FCL Program, facilities are evaluated against a set of requirements to determine their ability to meet Departmental protection standards. Approval of a FCL by DOE is based on a favorable evaluation of all of the following requirements:</p>
	<p>1. a. <u>DOE F 470.2 FDAR</u>. Completion and registration in SSIMS of DOE F 470.2 FDAR.</p>
	<p>1. c <u>Security Plan</u>. Approval of a security plan by the DOE cognizant security authority that describes the controls necessary within the facility to appropriately protect the security activities being performed.</p>
	<p>1. d. <u>Survey</u>. For facilities with importance ratings of A, B, C, or PP, a comprehensive initial survey must be conducted in accordance with Section G of this CRD. The survey must result in a composite facility rating of “satisfactory”.</p>
	<p>1. e. <u>Facility Security Officer (FSO)</u>. The FSO must be an employee of the company. The FSO must be appointed in writing. The FSO and others performing security duties must complete security training in accordance with Section J of this CRD.</p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<b>DOE M 470.4-1 Chg 1</b> (Manual, 03-07-06) <b>Safeguards and Security Program Planning and Management</b>	1. g. <u>Nuclear Materials Management and Safeguards System (NMMSS)</u> . A reporting identification symbol (RIS) code for NMMSS must be established for facilities authorized to possess SNM and a nuclear materials representative must be appointed with the contractor requirements in DOE M 470.4-6, Nuclear Material Control and Accountability.
	<p align="center"><b>SECTION J – SAFEGUARDS AND SECURITY TRAINING PROGRAM</b></p> 1. <u>OBJECTIVE</u> . To establish programs that ensure personnel are trained to a level of proficiency and competence that ensures they are qualified to perform assigned S&S tasks and/or responsibilities ( <b>as stated in LBNLs Site Security Plan</b> ).
	<p align="center"><b>SECTION K – SAFEGUARDS AND SECURITY AWARENESS PROGRAMS</b></p> 1. <u>OBJECTIVE</u> . To inform individuals of their S&S responsibilities and to promote continuing awareness of good security practices.
	<p align="center"><b>SECTION M – DEVIATIONS</b></p> 1. <u>OBJECTIVE</u> . To establish procedures, coordination, and approval levels that must apply to all deviations from Department of Energy (DOE) safeguards and security (S&S) program directive requirements.
	2. <u>REQUIREMENTS</u> . There are 3 categories of deviations: variations; waivers; and exceptions. Deviations from S&S program directive requirements require approval before implementation. Table M-1, Deviation Approval Process, depicts the approval level required for the various types of deviations. <p>a. <u>Deviations</u>. Deviations from S&amp;S program directive requirements require approval before implementation. Table M-1, Deviation Approval Process, depicts the approval level required for the various types of deviations. Coordination, approval, and duration limits are as follows.</p>
2. a. (1) <u>Variances</u> . Variances are approved conditions that technically vary from an Office of Security directive requirement but afford equivalent levels of protection without compensatory measures. <p align="center">(a) Approval Process for Variances.</p>	

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<b>DOE M 470.4-1 Chg 1</b> (Manual, 03-07-06) <b>Safeguards and Security Program Planning and Management</b>	<p><u>2</u> <u>Variations Related to Other S&amp;S Program Contractor Requirements.</u></p> <p><u>a</u> The cognizant security authority for the contractor must submit the request for a variance through the contractor line management to the DOE cognizant security authority for approval.</p> <p><u>b</u> The contractor line management must not implement the variance without DOE approval.</p>
	<p>2. a. (1) (b) <u>Duration of Variations.</u> There is no restriction on the length of time for which a variance can be approved.</p>
	<p>2. a. (2) <u>Waivers.</u> Waivers are approved nonstandard conditions that deviate from a contract requirement that if uncompensated would create a potential or real S&amp;S vulnerability. Waivers, therefore, require implementation of compensatory measures (e.g., additional resources to implement enhanced protection measures) for the duration of the waiver.</p>
	<p>2. a. (2) (a) <u>Approval Process for Waivers.</u></p> <p><u>2</u> <u>Waivers Related to Other S&amp;S Program Contractor Requirements.</u></p> <p><u>b</u> The contractor line management must not implement the waiver without DOE approval.</p>
	<p>2. a. (2) (b) <u>Duration of Waivers.</u> Waivers must not be approved for periods exceeding 2 years.</p>
	<p>2. a. (3) <u>Exceptions.</u> Exceptions are approved deviations from a contract requirement that can create S&amp;S vulnerability. Exceptions must be approved only when correction of the condition is not feasible and compensatory measures are inadequate to preclude the acceptance of risk.</p>
	<p>(a) Approval Process for Exceptions.</p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<p><b>DOE M 470.4-1 Chg 1</b>  (Manual, 03-07-06)  <b>Safeguards and Security Program Planning and Management</b></p>	<p>2. a. (3) (a) <u>3</u> <u>Exceptions Related to All Other S&amp;S Program Directive Requirements.</u></p> <p><u>a</u> The cognizant security authority for the contractor must submit the request for an exception through the contractor line management to the DOE cognizant security authority for approval.</p> <p><u>b</u> The contractor line management must not implement the exception without DOE approval.</p> <p>i. comments provided by HQ elements are formally reconciled before exception implementation;</p> <p>ii. adequate compensatory measures are in place before exception implementation; and</p> <p>iii. documented performance testing/VAs, if appropriate, are accomplished prior to exception implementation.</p> <p><u>c</u> Exceptions to national policy requirements, such as the NISP or the Personnel Security Program, must have the concurrence of the Director, Office of Security.</p> <hr/> <p>2. a. (3) (a) <u>3</u> (b) <u>Compensatory Measures.</u> Compensatory measures implemented as the basis for an exception request must be subject to formal VAs. Compensatory measure implementation must be tested and validated.</p> <p>(c) <u>Duration of Exceptions.</u> Exceptions must not be approved for periods exceeding 3 years (36 months).</p> <p>(d) <u>Annual Validation.</u> The need for an exception must be validated annually (at least every 12 months) and documentation submitted through the DOE cognizant security authority to the Office of Security and cognizant Departmental element.</p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<b>DOE M 470.4-1 Chg 1</b> (Manual, 03-07-06) <b>Safeguards and Security Program Planning and Management</b>	2. b. <u>Documentation.</u>  (1) <u>Deviation Request Format.</u> Specific information requirements for deviations are provided in Appendix 8, Format for Deviation Requests.  (2) <u>Assessments and Performance Testing.</u> The results of VAs and tests must be documented in the deviation request and in the site safeguards and security plan (SSSP)/site security plan (SSP), as appropriate.  (3) <u>Security Plans.</u> Approved deviations must be documented in the SSSP/SSP and site procedures as appropriate. A deviation request approved out of cycle with the S&S plan formulation and approval process must be documented as an attachment to the applicable plan until the next annual update.
	2. c. <u>Extensions.</u> Any extension to the approved period of time for deviations requires reapplication of the deviation process.
	<p align="center"><b>SECTION M – DEVIATIONS</b>  <b>APPENDIX 8 – FORMAT FOR DEVIATION REQUESTS</b></p>
	<p align="center"><b>SECTION N – INCIDENTS OF SECURITY CONCERN</b></p> 1. <u>OBJECTIVES.</u> To set forth requirements for the DOE Incidents of Security Concern Program, including timely identification and notification of, response to, inquiry into, reporting of, and closure actions for incidents of security concern.  2. <u>REQUIREMENTS.</u> d. Locally developed procedures must be established, documented, approved by the Departmental element, and disseminated to ensure the identification, reporting, root cause analysis, and resolution of incidents of security concern.

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

<b>DOE Directive</b>	<b>Requirement Citation</b>
<p><b>DOE M 470.4-1 Chg 1</b>  (Manual, 03-07-06)  <b>Safeguards and Security Program Planning and Management</b></p>	<p><b>CHAPTER I – IDENTIFICATION AND REPORTING REQUIREMENTS</b></p> <p>1. <u>GENERAL.</u></p> <ul style="list-style-type: none"> <li>a. A system for controls and procedures must be developed, approved, implemented, enforced, and maintained.</li> <li>b. Inquiries are used to determine the root causes of and individuals responsible for incidents of security concern.</li> <li>c. All discussions and documents associated with an incident of security concern must be classified or controlled according to current classification or control guidance and follow procedures contained in contractor requirements.</li> </ul> <hr/> <p>3. <u>REPORTING REQUIREMENT.</u></p> <ul style="list-style-type: none"> <li>a. 24-hour Determination/Categorization period</li> <li>b. Initial Incident Reporting</li> <li>c. Reporting Incidents Receiving Media Attention</li> <li>d. Reporting Incidents Associated with Non-U.S. Citizens</li> <li>j. Separate but Related Reporting <ul style="list-style-type: none"> <li>(1) Occurrence Reporting Processing System.</li> <li>(2) DOE O 151.1B</li> <li>(4) Special Reporting Situations.</li> </ul> </li> </ul>
<p><b>DOE M 470.4-2 Chg 1</b>  (Manual, 03-07-06)  <b>Physical Protection</b></p>	<p><b>CONTRACTOR REQUIREMENTS DOCUMENT</b></p> <p>All requirements contained in DOE M 470.4-2, Physical Protection, apply to contractors who are responsible for operating and/or administering the DOE, including NNSA, Physical Protection Program for protecting S&amp;S interests.</p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<p><b>DOE M 470.4-2 Chg 1</b>  (Manual, 03-07-06)  <b>Physical Protection</b></p>	<p><b>SECTION A – PHYSICAL PROTECTION</b>  <b>CHAPTER I. PROTECTION PLANNING</b></p> <p>1. <u>PLANNING</u>. The implementation of graded physical protection programs required by this manual must be documented. Site physical protection programs must be systematically planned, executed, evaluated, and documented as described by a SSSP or SSP.</p>
	<p>2. <u>PROTECTION STRATEGIES</u>. Protection strategies, as described in DOE M 470.4-1, Safeguards and Security Program Planning and Management, must be selected, developed, and implemented to protect S&amp;S interests.</p>
	<p>3. <u>GRADED PROTECTION</u>. Protection must be applied in a graded manner that is commensurate with S&amp;S interests.</p>
	<p><b>CHAPTER II. PROTECTION OF NUCLEAR WEAPONS, COMPONENTS, SPECIAL NUCLEAR MATERIAL, AND CLASSIFIED INFORMATION AND MATTER</b></p> <p>1. <u>GENERAL REQUIREMENTS</u>. This chapter defines requirements for protecting nuclear weapons and Category I through IV quantities of SNM.</p> <p>a. A facility must not possess, receive, process, transport, or store nuclear weapons or SNM until that facility has been cleared commensurate with DOE M 470.4-1, Safeguards and Security Program Planning and Management.</p>
	<p>1. c. Physical protection for each category of SNM must consider the following factors: quantities, chemical forms, and isotopic composition purities; ease of separation, accessibility, concealment, portability; radioactivity; and self-protecting features.</p>
	<p>1. f. Specific physical protection measures and protective force response capabilities must be described in a SSSP or SSP.</p>
	<p>1. g. The protection afforded SNM must be graded, according to the nuclear material safeguards category and attractiveness level, and reflect the specific nature of the nuclear material or SNM at each site.</p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

<b>DOE Directive</b>	<b>Requirement Citation</b>
<b>DOE M 470.4-2 Chg 1</b> (Manual, 03-07-06) <b>Physical Protection</b>	6. <u>STORAGE CONTROLS</u> . Each facility must have controls for nuclear weapons and SNM consistent with the graded safeguards approach required by paragraphs 7 through 10 below.
	10 <u>CATEGORY IV QUANTITIES OF SPECIAL NUCLEAR MATERIAL</u> .
	10.a. <u>In Use or Processing</u> . The SNM must be used or processed within at least a property protection area and in accordance with local security procedures approved by DOE line management.
	10.b. <u>Storage</u> . The SNM must be stored in a locked are within at least a PPA, and procedures must be documented in an approved SSP or SSSP.
	10.c.(2) <u>Transportation</u> . Shipments of unclassified Category IV quantities of SNM may be made by truck, rail, air, or water craft in commercial for-hire or leased vehicles.
	<b>CHAPTER IV. SECURITY AREAS</b>
	1. <u>GENERAL REQUIREMENTS</u> . Security areas include Property Protection Areas (PPA), Limited Areas (LAs), Exclusion Areas (EAs), Protected Areas (PAs), Vital Areas, Material Access Areas (MAAs), and specially designated areas. [e.g., Sensitive Compartmented Information Facilities (SCIFs) and Special Access Program Facilities (SAPFs)]
	1.a. <u>Prohibited Articles</u> . The articles listed below are not permitted in any security area without authorization, unless identified in approved local procedures. (1) explosives (2) dangerous weapons (3) instruments or material likely to produce substantial injury (4) controlled substances (5) an other item prohibited by law
	3. <u>PROPERTY PROTECTION AREAS (PPAs)</u> . PPAs are established to protect Government-owned property against damage, destruction, or theft.

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<b>DOE M 470.4-2 Chg 1</b> (Manual, 03-07-06) <b>Physical Protection</b>	3. a. <u>General Requirements</u> . Protection may include: physical barriers, access control systems, protective personnel or persons assigned administrative or other authorized security duties, Intrusion Detection Systems (IDS), and locks and keys. The designation of and description of PPA protective measures must be approved by DOE line management (e.g. SSP or SSSP). The requirements for PPAs must be configured to protect Government-owned property and equipment against damage, destruction, or theft and must provide a means to control public access.
	3. b. <u>Access Control</u> . Access controls may be implemented to protect employees, property, and facilities.
	3. c. <u>Signs Prohibiting Trespassing</u> . Signs prohibiting trespassing must be posted around the perimeter and at each entrance to the PPA.
	3. d. <u>Inspections</u> . Personnel, vehicles, hand-carried items, and packages entering or exiting the PPA are subject to inspection to deter and/or detect unauthorized introduction or prohibited articles and removal of Government assets.
	3. e. <u>Physical Barriers</u> . Physical barriers such as fences, walls, and doors may be used to identify the boundary of the area.
	<p><b>CHAPTER X. LOCKS AND KEYS</b></p> <p>1. <b>GENERAL REQUIREMENTS</b>. A lock and key program must be established to ensure control and protection of nuclear weapon components, special nuclear material (SNM), high-value government assets, and classified matter.</p> <p>2. a. <b>Locks</b>. Inventories must be conducted to ensure an accurate and up-to-date accountability of level I, II, and III security locks, key rings, key ways, and pinned cores.</p> <p>3. f. Panic hardware or emergency exit mechanisms used on emergency doors located in security areas must be operable only from inside the perimeter and must meet all applicable Life Safety Codes, as listed in Section B, DOE M 470.4-7, <i>Safeguards and Security Program References</i></p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<b>DOE M 470.4-2 Chg 1</b> (Manual, 03-07-06) <b>Physical Protection</b>	2. g. Locks and keys must be categorized according to the asset being protected and an inventory and accountability system must be implemented
	2. g. (1) Security keys include mechanical keys, key cards, and access codes. Security keys do not include administrative or privacy lock keys to factory installed file cabinet locks, desk locks, toolboxes, etc. Access codes must be protected from compromise.
	2. g. (2) Security key stock must be stored in a manner to prevent loss, theft of unauthorized use. Personnel responsible for the control and issuance of locking systems and/or security keys must maintain an access authorization (security clearance) commensurate with that required for access to the asset (s) to which the key(s) provides direct access.
	2. g. (2) (a) The organization responsible for the pinning and cutting of Level I, II , and III security locks and keys must report to the cognizant security authority.
	2. g. (2) (b) The pinning and cutting of Levels I, II, and III security locks and keys must be done within a Limited Area and have equivalent type protection measures.
	2.g.(3) Security keys and locks are divided into four levels, Levels I through IV.
	2. g. (5) Level III security lock and keys are typically on buildings, gates in fences, cargo containers, and storage areas for the protection of Government property.
	2. g. (5) (a). All Parts of broken Level III security keys must be recovered. If the functional part of the key (the blade) is lost or not retrievable, it must be reported to the cognizant security authority.
	2. g. (5) (b). Obsolete, damaged, or inoperative Level III keys must be destroyed and such destruction recorded. Keys must be destroyed in a manner authorized by the cognizant security authority.
	2. g. (5) (c). Fabrication, issuance, return, and destruction of Level III security keys must be documented.
	2. g. (5) (d). Site specific procedures must be developed for control and accountability of Level III security keys and be approved by the cognizant security authority.
	2. g.(6) Level IV locks and keys are typically used for offices where there is no open storage of classified matter and no classified matter in use. Desk, office and vehicle keys are considered administrative and have no control and accountability requirements,

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

<b>DOE Directive</b>	<b>Requirement Citation</b>
<b>DOE M 470.4-2 Chg 1</b> (Manual, 03-07-06) <b>Physical Protection</b>	2. h. An inventory system must be implemented to ensure the accountability of Levels I, II, and III security locks, keys, key rings, key ways, and pinned cores. Each accountable key and key core must have a unique identifying number placed on it. Cores will only be prepinned for the number required to fulfill the identified need. An inventory of prepinned cores will not be maintained for convenience.
	2. h. (1) Fabrication, issuance, return, and destruction of Levels I, II, and III security keys must be documented. Grand master security keys must be kept to an operational minimum and under strict control. Duplicate and replacement keys must not have the same key number assigned as the key being replaced or duplicated. The inventory record must identify the specific duplicate and replacement keys. If replaced, the disposition of the key being replaced must be identified
	2. h. (2) Inventories must include locks, keys in possession of key holders, issuance stock, and keys assigned to key rings/key cabinets.
	2.h.(2) (b) document the location of the locks(s) and keys
	2. h. (4) An annual inventory must be conducted to account for all Levels II and III locks and keys. In a Level III lock or key is discovered missing or tampered with, the incident must be reported through the Reporting Incidents of Security Concern process. These types of events should be categorized as IMI-4 incidents as identified in DOE M 470.4-1, <i>Safeguards and Security Program Planning and Management</i> , unless the cognizant security authority elevates the IMI categorization level.
	2. h.(5) Level IV locks and keys have no inventory requirement
	2. h. (6) Sites should implement a training plan for key custodians and anyone having responsibility for a security key to ensure they understand their responsibilities for security key control and accountability.
	2 .h.(7) Sites must have documented plans for key turn-in when personnel or programs are terminating or moving from one program to another

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
 As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<p><b>DOE M 470.4-2 Chg 1</b>            (Manual, 03-07-06)  <b>Physical Protection</b></p>	<p><b>CHAPTER XIII. MAINTENANCE</b></p> <p>1. <u>GENERAL REQUIREMENTS</u>. Security-related subsystems and components must be maintained in operable condition. A regularly scheduled testing and maintenance program must be established.</p> <p>2. <u>CORRECTIVE MAINTENANCE</u>. Corrective maintenance must be performed on site-determined critical and non-critical physical protection system elements.</p> <p>d. <u>Other Corrective Maintenance</u>. Corrective maintenance procedures for protecting Category III and Category IV quantities of SNM, or Secret or Confidential matter must be approved by line management and prescribed in the site's operation procedures.</p>
	<p><b>CHAPTER XV. DOE BADGE PROGRAM</b></p> <p>1. <u>GENERAL REQUIREMENTS</u>. DOE security badges must be issued to and worn by all DOE and contractor personnel to gain access to DOE facilities with S&amp;S interests and security areas. The DOE security badge or the Office of Science (SC) badges are the only format to be used.</p>
	<p>1.a. <u>DOE Security Badge</u>.</p> <p>(2) The DOE security badge will be accepted at all Departmental facilities.</p>
	<p>1.a. (2) Individuals at SC facilities with an access authorization must be issued a DOE security badge to gain access to non-SC Departmental facilities.</p>
	<p>1.b. <u>Office of Science Badge</u>. DOE line management must approve locally developed procedures for the issuance, use, recovery, accountability, protection, and destruction of the SC badge that are documented in the security plan.</p>

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<b>DOE M 470.4-6 Chg 1</b> (Manual, 08-14-06) <b>Nuclear Material Control and Accountability</b>	<b>CONTRACTOR REQUIREMENTS DOCUMENT</b>  <b>NUCLEAR MATERIAL CONTROL AND ACCOUNTABILITY</b>  2. <u>OBJECTIVES.</u> a. To prescribe DOE requirements, including those for the NNSA, for nuclear material control and accountability (MC&A) for DOE-owned and DOE-leased facilities and DOE-owned nuclear materials at other facilities that are exempt from licensing by the Nuclear Regulatory Commission.
	<b>SECTION A – NUCLEAR MATERIAL CONTROL AND ACCOUTABILITY</b> <b>CHAPTER I – PROGRAM ADMINISTRATION</b> 1. <u>GENERAL.</u> DOE line management and site/facility operators must consider MC&A requirements, systems, technologies, and activities when planning, designing, constructing, and operating new or renovated DOE facilities. The site/facility operator must use techniques and equipment that maximize material loss detection sensitivity, increase the quality of accountability measurements, minimize material holdup, and reduce the magnitude of inventory differences and associated control limits consistent with the consequences of the loss of the material.
	1. a. An MC&A program must be established and maintained for all materials identified in Table 1-1, Nuclear Materials.
	1. b. SNM must not be received, processed, or stored at a facility until a facility approval has been granted.
	1. c. MC&A programs must be design to deter and detect theft and diversion of nuclear materials by both outside and inside adversaries.
	1. d. A performance testing program to verify MC&A procedures and practices and to demonstrate that material controls are effective must be established.
	1. f. This Manual requires that various documents, actions, and activities be approved by the DOE cognizant security authority.

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<b>DOE M 470.4-6 Chg 1</b> (Manual, 08-14-06) <b>Nuclear Material Control and Accountability</b>	1. g. The site/facility operator must designate a management official to be responsible for the MC&A program. This official must be organizationally independent from responsibility for nuclear material utilization programs, including nuclear material production, storage, processing, research, and disposition. This official must have responsibility for and the authority to ensure the safeguards of accountable nuclear material, along with operations personnel.
	1. h. A reporting identification symbol (RIS) must be established for all nuclear materials on inventory.
	1. i. A nuclear materials representative (NMR) must be designated for each site/facility with a RIS .
	1. j. Authorities and responsibilities for MC&A functions must be defined and documentation must be maintained.
	1. k. MC&A program implementation must facilitate, to the extent practical, the cost effective integration of the operational mission of the program while protecting the environment, health and safety of employees and the public.
	1. l. Personnel performing MC&A functions must be trained and qualified to perform their duties and responsibilities.
	1. m. An MC&A plan providing the safeguards authorization basis must be developed and maintained for each facility possessing nuclear materials.
	1. n. The MC&A plan must specify how nuclear material inventory holdings will be accounted for and controlled.
	1. o. Procedures must be established by the site/facility operator for emergency conditions and periods when MC&A systems are inoperative .
	1. u. Doe line management must assure that technical standards developed or adopted by voluntary consensus standards bodies, such as the American Technical Standards Institute and ASTM International, are considered in development of MC&A programs under their cognizance.

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<b>DOE M 470.4-6 Chg 1</b> (Manual, 08-14-06) <b>Nuclear Material Control and Accountability</b>	1. v. MC&A systems should be integrated with physical security systems to protect against radiological and/or toxicological sabotage involving nuclear materials.
	2. <u>GRADED SAFEGUARDS</u> . The site/facility operator must establish and follow a graded safeguards program for nuclear materials.
	3. <u>MC&amp;A REQUIREMENTS FOR SOURCE AND OTHER NUCLEAR MATERIALS</u> .
	3. a. Separated neptunium-237 and separated americium (Am-241 and Am-243) must be protected, controlled, and accounted for as if they were SNM.
	3. b. Tritium is a nuclear material of strategic importance; therefore, a graded safeguards programs for tritium must be implemented according to the following categorizations.
	3. c. Excluding tritium, separated neptunium-237, and separated americium (Am-241 and Am-243), source and other nuclear materials listed in table I-1, Nuclear Materials, are exempt from the requirements of this Manual except for the following.
	4. <u>LOSS DETECTION EVALUATION, PERFORMANCE TESTING, AND PERFORMANCE REQUIREMENTS</u>
	4. b. Performance testing. MC&A performance testing programs must be developed and documented to support and verify loss detection capability and system effectiveness. The scope and intent of performance testing must be based on the graded safeguards concept, i.e. the testing program demonstrates greater testing for higher category facilities than for lower category facilities.
	4. c. MC&A Performance Requirements. Specific performance requirements for selected MC&A system elements are established below in (1) – (7)
4. c(5) Accounting Record System. The accounting record system must accurately reflect item identity and location for at least 99 percent of items selected.	

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<b>DOE M 470.4-6 Chg 1</b> (Manual, 08-14-06) <b>Nuclear Material Control and Accountability</b>	4. c(7) Inventory Difference Control Limits. (b) For Category III and IV MBAs, limits-of-error of inventory differences must not exceed a specified percentage of the active inventory during the inventory period to a maximum of a specified quantity; the specified percentage and maximum quantity must be approved by the DOE cognizant security authority.
	5. <u>REPORTING INCIDENTS OF SECURITY CONCERN.</u>  a. The site/facility operator must identify MC&A loss detection elements for each MBA and must establish a graded program for monitoring these elements and associated data to determine the status of nuclear material inventories and to identify security incidents.
	6. <u>ASSESSMENT PROGRAMS.</u>  a. <u>General.</u> The site/facility operator must establish a program to periodically review and assess the integrity and quality of its MC&A program and practices. The frequency and content of these assessments must be on a graded basis approved by the DOE cognizant security authority.
	<b>CHAPTER II – MATERIALS ACCOUNTABILITY</b> 1. <u>GENERAL.</u> Nuclear material accountability programs must ensure accountable nuclear materials are accounted for and unauthorized acts detected. These requirements must be applied in a manner consistent with the graded safeguards concept. The Chapter is divided into five functional areas: accounting systems, physical inventories, measurement and measurement control, nuclear material transfers, and material control indicators.
	2. <u>ACCOUNTING SYSTEMS.</u> A system for tracking nuclear material inventories, documenting nuclear material transactions, issuing periodic reports, and assisting with the detection or unauthorized system access, data falsification, and material gains and losses must be established.
	3. <u>PHYSICAL INVENTORIES.</u> The site/facility operator must implement a physical inventory program for nuclear materials to demonstrate that materials are present in their stated quantities and to detect the unauthorized removal of nuclear materials.

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<b>DOE M 470.4-6 Chg 1</b> (Manual, 08-14-06) <b>Nuclear Material Control and Accountability</b>	3. a. Periodic Physical Inventories. (1) Conduct of Physical Inventories. Inventories must be based on measured values, including measurements or technically justifiable estimates of holdup. Table II-1. Minimum Sampling Parameters for Physical Inventories Category IV; Confidence level is 95 percent; Minimum Detectable Defect is 10 percent.
	3. a(2) Physical Inventory Frequencies. Physical inventories for Category IV SNM MBAs must be performed at a frequency specified by the DOE cognizant security authority, but at least every 2 years (every 24 months).
	4. <u>MEASUREMENT AND MEASUREMENT CONTROL</u> . Measurement and measurement control programs approved by the DOE cognizant security authority must be implemented at all facilities with nuclear materials. Measurement programs used to determine Category III and IV inventories of SNM must address topics in paragraphs 4.a through e., but the specific measurements and measurement control requirements will be determined by the DOE cognizant security authority.
	5. <u>NUCLEAR MATERIAL TRANSFERS</u> . The site/facility operator must develop and implement a program to control and account for both internal and external transfers of nuclear materials for each facility. This program must include documented procedures that specify requirements for authorization, documentation, tracking, verification, and response to abnormal situations that may occur during transfer of nuclear materials.
	6. <u>MATERIAL CONTROL INDICATORS</u> . The site/facility operator must develop and implement a program that is capable of detecting losses through evaluation and assessment of shipper/receiver differences, inventory differences, and other inventory adjustments.  a. <u>Shipper/Receiver Difference Assessments</u> . Written procedures must be developed for evaluating shipper/receiver differences and for investigating and reporting significant shipper/receiver differences.
	6. b. <u>Inventory Difference Evaluation</u> . (1) A program for evaluating all SNM inventory differences, including those involving missing items must be developed, documented and implemented for each facility. (2) For Category IV MBAs, control limits may be based on professional judgment with the approval of the DOE cognizant security authority.

**List of DOE Directives in the Lawrence Berkeley National Laboratory Contract  
As Implemented in a DOE Site Security Plan (SSP)**

DOE Directive	Requirement Citation
<p><b>DOE M 470.4-6 Chg 1</b>  (Manual, 08-14-06)  <b>Nuclear Material Control and Accountability</b></p>	<p><b>CHAPTER III – MATERIALS CONTROL</b></p> <p>1. <u>GENERAL</u>. This chapter describes the requirements for nuclear material control, consisting of four functional areas: access controls, material surveillance, material containment, and detection/assessment. The graded nuclear materials control program must be documented in the MC&amp;A plan.</p>
	<p>2. <u>ACCESS CONTROLS</u>. A graded approach must be established to control personnel access to: nuclear materials; nuclear materials accountability, inventory, and measurement data; data-generating equipment; and other items/equipment that misuse of which could compromise the safeguards system.</p>
	<p>3. <u>MATERIAL SURVEILLANCE</u>. A nuclear material surveillance program must: ensure that materials are in their authorized locations, be capable of detecting unauthorized activities or anomalous conditions, and be capable of reporting material status. The surveillance program must address both normal and emergency conditions and include periodic testing.</p> <p>(3) Category IV. The material surveillance program for Category IV quantities must be site-specific and approved by the DOE cognizant security authority.</p>
	<p>4. <u>MATERIAL CONTAINMENT</u>. A documented program must be in place to provide controls for nuclear materials operations relative to MAAs, PAs, MBAs, other authorized storage repositories, and processing areas.</p>
	<p>4. b. <u>Material Balance Area</u>. Controls must be established and implemented for each facility to ensure that nuclear materials are used, processed, or stored within an MBA and are controlled in accordance with the graded safeguards concept.</p>
	<p><b>SECTION B – BASIC REQUIREMENTS FOR NUCLEAR MATERIALS MANAGEMENT AND SAFEGUARDS SYSTEM REPORTING AND DATA SUBMISSION</b></p> <p>1. <u>DOCUMENTATION AND REPORTING</u>.</p> <p>a. All RIS-level nuclear materials transactions, material balances, and inventories must be documented in accordance with the instructions provided in Section B of this Manual and reported to the Nuclear Materials Management and Safeguards System (NMMSS), the national database for nuclear materials.</p>