W5516
Task #14

LANL Safeguards & Security Assurance Program

FSS
Planning and Assessment Office

April 3, 1995

Revision 6

Los Alamos National Laboratory

S&S Program Manager

DOE/LAAO SNSD

LANL Audits & Assessments

DISCLAIMER

Contents

Introduction

The Safeguards and Security (S&S) Assurance Program provides a continuous quality improvement approach to ensure effective, compliant S&S program implementation throughout the Los Alamos National Laboratory (LANL). The program integrates all oversight activities both internal and external through sharing, teaming, and communication. Any issues identified through the various internal and external assessments are documented, tracked and closed using the Safeguards and Security Issue Management Program. Our commitment is to eliminate duplication of effort, provide consistent guidance to our customers, lessen resource impact, and to continuously improve our program implementation by sharing information and reaching agreement between all oversight organizations.

The LANL Safeguards & Security Assurance Program (S&SAP) is established to ensure the adequacy and effectiveness of the LANL S&S Program. The Laboratory utilizes an integrated S&S systems approach to protect US Department of Energy (DOE) interests from theft or diversion of special nuclear material (SNM), sabotage, espionage, loss or theft of classified/controlled matter or government property, and other hostile acts that may cause unacceptable impacts on national security, health and safety of employees and the public, and the environment. The S&SAP is designed to assist line managers with internal S&S processes (assessments, follow up and feedback) so they can effectively conduct their programmatic work activities while maintaining their organizational safeguards & security requirements.

The S&SAP provides:

- a means for LANL managers to continuously assess their organizations' S&S programs to ensure compliance and develop corrective actions when required;

- a proactive teaming environment for the continuous maintenance of the LANL S&S Program to be shared by affected stakeholders, who have the same purpose and objectives, i.e., DOE Los Alamos Area Office (LAAO), DOE Albuquerque Operations Office (AL), DOE Headquarters Office of Security Evaluation (OSE), University of California (UC), LANL Audits and Assessments (AA-2) and the Facility Safeguards and Security Planning and Assessment Office (S&S PAO);

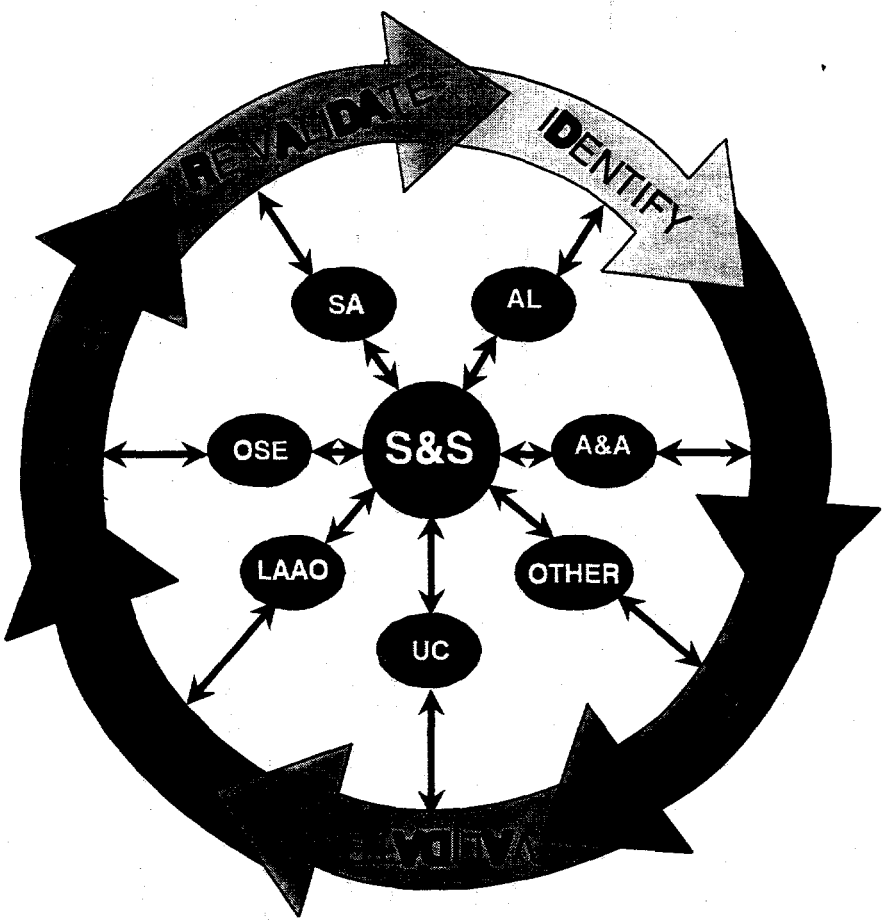
- a mechanism for discovering deficiencies, determining root causes, conducting risk assessments, analyzing cost vs. risk, developing and implementing corrective actions with the appropriate compensatory measures, documenting the self-assessment process, tracking corrective actions until closure, and conducting trend analysis.

This document explains the basis, scope, and conduct of the S&S process to include: self-assessments, issue management, risk assessment, and root cause analysis. It also provides a discussion of S&S topical areas, roles and responsibilities, process flow charts, minimum requirements, methodology, terms, and forms.

Figure 1 below depicts the interactive relationship of issues and oversight organizations which is pictorial representation of the S&SAP plan. The outside circle represents a continuous review process of identifying, correcting, verifying, validating, trending, re-verifying, and re-validating of issues.

Figure 1

SAFEGUARDS & SECURITY ASSURANCE PROGRAM



LAAO	DOE Los Alamos Area Office
OSE	DOE Headquarters Office of Security Evaulation
SA	Self-Assessment
AL	DOE Albuquerque Operations Office
A&A	Audits and Assessments
UC	University of California
Other	Other internal/external evaulation agencies/organizations

Safeguards and Security Program Basis

Purpose

The Laboratory-wide S&S Program ensures that safeguards and security operations and activities are conducted in an effective and efficient manner consistent with DOE and regulatory requirements, sound business practices, and programmatic requirements.

Graded Approach

Program strategies are based on a graded approach utilizing the results of table top analysis, vulnerability and risk assessments, and cost benefit analysis. The basis for this graded approach is found in the DOE threat policy and guidance and the Laboratory threat statement found in the approved Site Safeguards and Security Plan (SSSP). In addition, customer requirements and programmatic needs are also important considerations when S&S decisions are made.

DOE Contract W-7405-ENG-36

A Laboratory-wide Safeguards and Security Self-Assessment Program is mandated by the terms of the Department of Energy/University of California contract, according to the terms of which UC manages and operates Los Alamos National Laboratory for DOE. The Modification to Contract No. W-7405-ENG-36, states that "the University will conduct an ongoing self-assessment process including self-assessments performed at the Laboratory, as the principal means by which to evaluate compliance with the performance measures . . . against which the University's overall performance of obligations under the contract will be determined.

Lab-wide communication

The S&S Program combines the efforts of all Laboratory employees supported by line management. The program is coordinated and communicated across the Laboratory by the *Director's Policy* letter, the Laboratory Leadership Council guidance and direction, *Safeguards and Security Manual,* the *Organizational Safeguards and Security Plans* (OSSPs), the *Property Protection Program*, the *Personnel Security Assurance Program*, *Security Assistance Program*, Performance-Based Security Training, and the *Security Education and Awareness Program.* Communication is enhanced in the Laboratory using various employee

awareness methods, such as the *Security Bulletin*, on-line system updates, and the Laboratory's *Newsbulletin*.

Facility Management Program

The Safeguards & Security Program is an integral part of the Laboratory's facility management program. This program provides for facility-wide communication and coordination between all support activities and a team approach to addressing complex issues that are specific to a facility. Solutions are shared and implemented where appropriate throughout the Laboratory. This program ensures that managers will be involved in addressing security-related concerns in their facilities.

Management Program

The Laboratory provides a Safeguards and Security Program Office to ensure the S&S Operations are providing an effective and efficient quality service to support the Laboratory's programs.

Scope of S&S

The scope of S&SAP includes all of the S&S Program topical areas listed below:

Program Planning and Management
- Planning Process
- Budget Process
- Organization and Management
- Site Safeguards and Security Plan (SSSP)
- Peer Review and Self-Assessment
- Reporting and Notification
- Resolution of Findings

Protection Program Operations
- Physical Security Systems
- Property Protection
- Protective Force
- System Performance Tests

Material Control and Accountability
- Program Management
- Material Accounting
- Material Control
- Administrative Controls
- System Performance Tests

Information Security
- Management Program
- Control of Secret and Confidential Documents
- Classification Guidance and Derivative Classifiers
- Control of Top Secret Documents
- Classified Material Control
- Security Infractions/Violations
- Technical Surveillance Countermeasures
- System Performance Tests

Computer Security
- Computer Security Management and Planning
- Protection of Information Assets
- Physical Protection of Computing Resource Assets

Safeguards and Security Assurance Program Concepts

Assurance Program

The S&S AP is designed to provide a continuous process for assessing the S&S Program at the Laboratory. This process identifies, corrects, verifies, validates, trends, re-verifies, and re-validates S&S issues for the purpose of ensuring that the Laboratory has an effective S&S program that meets or **exceeds** the expectations of the DOE and the UC. All internal and external auditing and assessing organizations/agencies share in this process. The trending process identifies problem areas so that resources can be redirected and focused in those areas. The program:

- involves managers at all levels in regularly reviewing organizational elements, operational activities, and facilities under their cognizance to ensure compliance with all S&S requirements and the utilization of best management practices;
- enhances the timely identification and correction of existing weaknesses to improve overall organization effectiveness;
- is cost effective by targeting problem programs and organizations who need assistance resulting in a reduction of the required resources;
- uses a conduct of operations methodology that reduces the recurrence of past S&S deficiencies.

Formality of Operations

The assurance program is based upon formal procedures within and between all programs, line organizations, and oversight organizations which ensure formality of operations.

Peer Review

A peer review of this plan will be performed on an annual basis to ensure it meets with Laboratory, DOE, and UC expectations. The Peer Review Panel will consist of representatives from DOE, other DOE Laboratories, UC and internal customers.

S&S PAO Support

The S&S PAO provides a formal process for accomplishing the in-house self-assessments and issue management. Issues identified through the self-assessment process are documented with corrective action plans and milestones.

Integration and Teaming

The S&SAP integrates all internal and external assessments and audits by teaming with the DOE/LAAO, the AA-2, the various Facilities Security and Safeguards Division (FSS) topical areas, and the Laboratory's line organizations. Teaming provides the opportunity to combine all local oversight activity which eliminates duplication of effort, shares resources, provides the opportunity to resolve policy and order interpretation conflicts, and eliminates repetitive assessment visits to line organizations.

Coordination

All audits/assessments are coordinated through AA-2. AA-2 notifies Laboratory line organizations of scheduled audits and assessments in accordance with Laboratory Director's Policy (DP) 111. DOE and FSS are responsible for providing AA-2 with all audit/assessment schedules in a timely manner in accordance with DP 111. In addition, AA-2 participates in the coordination of all PAO self assessments.

Self Assessment

The S&S Assessment program is a three tiered approach to ensure an effective Safeguards and Security program implementation:

Tier I

FSS developed an *Organizational Safeguards and Security Plan (OSSP)* for all Laboratory organizations. The OSSP is a template which is tailored to each organization and supplements the Site Safeguards and Security Plan (SSSP). The plan identifies the security interests, protection measures, personnel assignments, position descriptions, and training requirements. Additionally, the OSSP provides the organization specific guidance and compliance check sheets to conduct annual self-assessments in each topical area. If the organization finds areas where they are not compliant, a corrective action plan is developed and submitted to S&S PAO for tracking in the Issue Management Program. These line organization

assessments are coordinated by the Organizational Safeguards and Security Officers (OSSO).

Tier II

Each FSS/S&S Group is responsible for scheduling, conducting, and reporting security assistance visits (SAVs) throughout the year. SAVs are designed to assist the line-organizations in implementing and maintaining compliant and effective security programs. During the SAVs, the compliance check sheets are reviewed and validated. Non compliance to DOE order requirements are formally reported to the organization and S&S PAO.

Tier III

Tier III consists of formal assessments which are scheduled and conducted by a team of subject matter experts from FSS, DOE/LAAO, and AA-2.

The goal of this three tier approach is to reduce the tier III activity to validation of tier I and II which will substantially reduce compliance oversight costs at the Laboratory while still ensuring compliant and effective programs. (See Self Assessment Process Section for details.)

Scheduling

S&S PAO is responsible for developing and distributing the annual S&S self-assessment schedule to be conducted from October 1 through August 1 each fiscal year, preparing a final report to be forwarded to AA-2 for compilation and submission to UC.

OSSPs

Each Laboratory organization (subcontractors excluded) is required to develop and update annually an OSSP that contains the methods and tools for managing S&S within their organizations. This plan also provides the schedule for periodic self-assessments to ensure compliance with applicable DOE safeguards and security orders.

Review Methods

Assessment methods include, but are not limited to, observation, interview, document review, and performance tests. Assessments will be based on DOE Orders, standards and criteria, inspector's guides, results of past internal and external audits, surveys, and inspections.

Documentation

Documentation to support the self assessment process is very important. Therefore, the OSSOs will submit the results of their organizational Tier I self assessment to S&S PAO for review and required follow-up activities. The S&S topical area team leaders will also provide to S&S

PAO the following documentation for assistance visits and self assessments that occur during the fiscal year: list of all scheduled visits conducted to include the organization and personnel visited, security specialists involved, assistance provided, issues/concerns/findings identified, corrective action plans, and a summary status report. If check lists were used to complete the task, they should also be included as part of the documentation provided to S&S PAO.

Issue Resolution

The results of self-assessments, management reviews, internal and external audits, surveys, and inspections are expressed as issues.

Such issues and the corresponding corrective actions are prepared, tracked, and reported in accordance with the S&SAP process (See Appendix A).

Trend Analyses

A trend analyses is conducted by the Issue Management Coordinator (IMC) on a frequent basis to identify problem areas. The results of these trend analyses are provided to the S&S Program Manager, Self Assessment Project Leader , S&S topical area Group Leaders (GLs) and Office Leaders (OLs), and OSSOs. The S&S topical area GL is responsible for identifying and implementing corrective actions for these trends.

Roles and Responsibilities

Laboratory Director

The Laboratory Director has overall responsibility and authority for the safeguards and security programs at the Laboratory. Through the Laboratory Leadership Council, the FSS Division Director, and the Safeguards and Security Program Manager, the Director exercises management prerogatives and actions that will ensure that S&S activities comply with the provisions of the UC performance objectives, applicable DOE orders, and management directives.

DOE/LAAO - SNSD

The LAAO Safeguards and Security Department personnel team with FSS/S&S personnel to conduct self-assessments, issue tracking, and issue closure activities. LAAO - Safeguards and Security Division (SNSD) approves all issue action plans and validates or verifies the closure of all issues (See Appendix A flow chart).

LANL Audits and Assessments

LANL Audits and Assessments Office coordinates assessment schedules and teams with S&S personnel to conduct self-assessments/audits during the same time frame to reduce the overall impact on the organizations being evaluated. They also coordinate all external audits with the auditing organization/agency and the Laboratory.

FSS Division Director and S&S Program Manager

The FSS Division Director and the Safeguards and Security Program Manager have overall responsibility for the management of the S&S program at the Laboratory. The FSS S&S Program Manager is responsible for the oversight and coordination of all S&S program activities as they relate to compliance with the terms of the DOE/UC contract.

The S&S Program Manager is responsible for ensuring that self-assessments are conducted and corrective action plans are executed for identified deficiencies that meet the requirements contained in DOE Orders and the DOE/UC contract.

The S&S Program Manager

- Ensures full implementation and execution of this plan.

- Establishes issue corrective action priorities for external findings.
- Reviews, approves, and recommends the closure of all issues before the closure packages are forwarded to DOE/LAAO as appropriate for verification/validation and closure.
- Notifies DOE of completed issues.

FSS/S&S GLs/OLs

FSS/S&S Group Leaders (GLs) and Office Leaders (OLs) are responsible for the implementation and oversight of the safeguards and security topical area programs. They formally schedule, document and follow-up on organization assistance visits and self assessments and provide copies of this documentation to S&S PAO. They review, approve and monitor the issue action plans resulting from weakness in their topical areas, and ensure that S&S issues are resolved to meet DOE and Laboratory requirements. They also establish issue corrective action priorities for systemic topical self assessment issues after coordination with S&S PAO and the affected organizations. If issues are found to be systemic, they coordinate Lab-wide corrective action with all organizations that may be affected.

S&S PAO

The S&S Planning and Assessment Office (S&S PAO) manages the Safeguards and Security Assurance Program. The S&S PAO serves as the central focal point for issue related activities and self-assessments, and coordinates with all affected organizations.

S&S PAO ensures that information is shared between organizations and that the annual submission of the consolidated S&S self-assessment report is sent to the appropriate laboratory official(s).

PAO Project Leader

S&S PAO self assessment project leader selects a team leader, provides support and coordination, reviews documentation and in general assures the effectiveness of the assessments. The Team Leader reports directly to the Project Leader who reports to the S&S Deputy Program Manager.

The IMC

Issue Management Coordinator

- Functions as the S&S point of contact between the S&S Program Manager and DOE/LAAO or DOE/AL as appropriate within the scope of this plan.

- Administers the S&S Issues Management Process (IMP) to include screening and entering the issues and assignments and identifying duplicate issues and/or existing plans.

- Reviews OSSO/GL/OL Issue Action Plans (IAPs) addressing issues for completeness and applicability to the root cause and risk analysis and tracks the information in the IMP.

- Liaisons with the OSSOs/GLs/OLs or their designated representatives for recurring issues, commitments, status updates, and completions.

- Provides periodic reports to the S&S Program Manager, OSSOs, and GLs/OLs on the status of the issue resolutions.

- Reviews closure packages submitted by OSSOs/GLs/OLs for completeness before forwarding closure packages to the S&S Program Manager and DOE/LAAO.

- Maintains historical records of issues.

- Monitors the status of the requests-for-approval submitted to DOE, including comments received, approvals granted, and issues resolved. This includes, but is not limited to, Compliance Schedule Approval (CSA) (deviations) related documentation.

- Reviews and coordinates all deviation documentation before it is passed to the S&S Program Manager and DOE/LAAO.

Line Management

The Line Manager

- Responsible for the S&S Program within his/her organization.
- Appoints responsible person to resolve internal and external S&S issues.
- Recommends issue priority.
- Coordinates with other groups/offices to complete assigned tasks.
- Ensures timely completion of assigned commitments.

Facility Manager

The Facility Managers

- Responsible for all safeguards and security activities within their facilities.
- Manage all facility S&S Protection Program Operations
- Coordinate all other S&S topical area programs with the S&S Facility Team Leader and the OSSO(s).

Organizational Safeguards and Security Officer

The OSSOs are responsible for the coordination of S&S activities within their organizations.

- Ensures S&S requirements are properly implemented through out their organization.
- Oversees the self-assessment program in their organization.
- Prepares Issue Action Plans (IAPs) within their organization.
- Submits IAPs addressing internal and external generated issues to the IMC for entry into the IMP.
- Prepares and submits the closure package to the IMC.

Self-Assessment Process

Each Laboratory organization develops a formal OSSP which contains the methods and tools for conducting periodic self-assessments to ensure compliance with applicable DOE safeguards and security orders.

FSS provides a formal structure for consistent guidance through security manuals, performance-based training, performance testing in applicable areas, and security assistance visits. This structure shall be customer focused to provide continuous quality improvement in safeguards and security throughout the Laboratory.

The S&S PAO provides a formal self-assessment program plan to include annual assessment schedules. This planning document is reviewed annually and updated as required. Additionally, weaknesses identified through the self-assessment process are written as issues with corrective actions and milestones. Both root cause analysis (priority 1 & 2 issues) and risk/cost/benefit analysis are conducted and are considered critical to the success of the self-assessment process.

Review Methods

Assessment methods will include, but are not limited to, observation, interview, document review, and performance tests. In each case, the scope of the assessment and the method or review is clearly indicated in a written plan.

Written Plans

Each Laboratory organization's OSSP includes self-assessment provisions consistent with the self-assessment criteria described herein. Each OSSP includes a description of how assessments are documented and reported.

Formal Plan

A formal plan including an assessment schedule for the Laboratory's annual safeguards and security self-assessment will be developed no later than September 1 each year. The assessment begins with FSS programs and is based on DOE orders, standards and criteria, and on past surveys and inspections.

Audit and Review Schedules

The self-assessment plan of each division and organizational unit includes a schedule of planned self-assessments. The self-assessment reviews focus on applicable topical areas within the organization and are

based on performance measures as provided in the DOE/UC contract.

Report Tracking

Each organization keeps the FSS/PAO Office informed of the results of its reviews so that the database can be maintained.

Report Standards

A formal self-assessment requires a written plan defining scope and methodology and a informal written report describing the results of each assessment. These reports are collated into a formal Laboratory report at the completion of the annual PAO self assessment process.

Informal self-assessments or management reviews are limited in scope to the protocol covering the subject and scope of the management review in the OSSP. An internal self-assessment or management review is normally conducted by a single individual or manager. It requires a written report. The results of the review may be recorded using a safeguards and security issue data entry form or a similar format in lieu of a formal report. These forms are included in the OSSP which because of its limited scope, may be shortened accordingly. However, a management review may also include an in-depth report if desired. The OSSP also provides a format for reporting informal self-assessments.

Supporting Documentation

Records of self-assessments shall document the following: subject of the audit; compliance criteria (DOE order standards and criteria or best business practices); names of the reviewers; dates of audits and interviews; the activities of those conducting the audit; the individuals interviewed; all self-assessment issues, both positive and negative; all significant observations or quality problems; and results of root cause analysis, if applicable. The corrective actions, if any, may be listed in the report or documented in a follow-up corrective action and close-out report. A recommended course of action will be outlined in the report.

The following records will be maintained in self-assessment report files:

Start and completion dates of all audits and reviews,

Copies of all audit and review reports completed for previously conducted audits and reviews,

Listings of self-assessment issues and deficiencies,

Root Cause identification (if required),

Actions to correct self-assessment issues and deficiencies and/or to establish best business practices, and

Lessons learned.

Self-Assessment Issue Resolution Requirements

The results of self-assessments and management reviews are expressed as self-assessment issues, even if they are in the categories of findings, deficiencies, or observations.

Issues and corrective actions for self-assessments are prepared, tracked, and reported at regular review meetings and processed according to the Self-Assessment IMP.

Self-Assessment Plan Criteria

Determine the type of assessment to be used: team approach, management review, or self-assessments.

Determine assessment methods: observation, interviews document reviews, or performance tests.

Develop a data call list to be published with the assessments scheduled.

Select/appoint self-assessment team members.

Conduct FSS self-assessment in all topical areas using DOE safeguards and security orders and standards and criteria with emphasis on formality of operations, consistency of approach, cohesiveness of organization, and program planning and management to achieve goals and objectives for customer service and continuous quality improvement.

Review and analyze OSSPs to assist in selecting organizations for assessment.

Use the FSS self-assessment as the basis for selecting the criteria for Laboratory-wide self-assessments.

Develop an assessment schedule that provides the Laboratory and DOE confidence that the programs have

been sufficiently reviewed to ensure Laboratory-wide compliance.

Schedule Structure

There are 29 Laboratory organizations. The organizations to be assessed are selected based on the amount of classified, SNM or unclassified sensitive work being done in the organization. Each year's self-assessment schedule will cover at a minimum 85% (UC Performance Metrics) of all Laboratory organizations. Organizations responsible for SNM will be assessed every year. All other Laboratory organizations will be assessed at a minimum every two years. Assessments will be conducted every fiscal year between October 1 and August 1. A schedule of specific dates will be published annually. A final report to the UC will be prepared and published by August 31 each year.

Selection Criteria for Self-Assessment Participants

Participants in the self-assessment process for safeguards and security are knowledgeable in the topical areas they are assessing. They have attended training in their topical area and have a familiarity with the standards and criteria used to implement the applicable DOE orders. Training records are available to the team leader for the selection process. Additionally, participants are recommended by the cognizant group leader.

Contractor support is used for participation in the self-assessment process as appropriate. Contractors have job experience in the topical areas they are assessing and/or have demonstrated experience in inspections or surveys for the topical areas they are assessing.

The assigned team leader has demonstrated knowledge, skills, and abilities in at least one topical area. Additionally, the team leader has experience in formal self-assessment programs.

Risk Assessment and Priority Assignment

The initial step in the self-assessment issue resolution process is to conduct a risk assessment and assign a priority to each identified issue. Each self-assessment issue will be assigned one of four priority levels in Appendix B.

The Issue Management Process

Issue Identification

S&S compliance/noncompliance with DOE requirements will be identified by external reviews, occurrence reports, internal reviews and self assessments.

The Issue Management Coordinator (IMC) reviews all S&S-related external issues for duplicates, current IAPs that may resolve newly identified issues, or a determination that some issue resolutions are not required by DOE Orders, Laboratory policy, or other requirements.

- If the issue is not a duplicate or cannot be addressed by an existing plan, it is assigned to the appropriate GL/OL responsible for the new IAP.

- For duplicate issues, it is sufficient to cross-reference the existing issue. Similarly, if an existing IAP addresses the new issue, it is sufficient to record the new issue on the plan. **It is not necessary to generate duplicate documentation.**

- If an issue is determined not to be a required action (i.e., lacks associated requirements), it may be challenged by submitting an Issue Closure Certificate (Appendix D). The challenge is to include, as a minimum, the issue number, narrative summary, and cited source. Close coordination with DOE counterparts and discussion of the issues is desirable before the challenge is formalized. The basis and reasoning for the challenge (i.e., conflicting requirements, existing compensatory measures, deviations, etc.) are addressed in the "Summary of Corrective Actions" section of the closure certificate.

- All generated issues are entered into the system and tracked to closure by the IMC.

Evaluation

Root Cause Analysis

For externally generated issues, the responsible topical area GL/OL does a root-cause analysis and determines (1) the fundamental and contributing basis of the condition,

(2) corrective actions to prevent a recurrence, (3) whether the issue is related to a previous problem, and/or (4) if one solution can resolve several issues. Care should be taken to minimize the use of generic root causes such as "training." Be specific. If training is determined to be the root cause, the analysis should continue to decide the specific training aspect that is deficient.

For internally (self assessments) generated issues, the responsible topical area GL/OL teams with line management to assign a root cause for the issues, using a graded approach (see Appendix B for details.)

Graded Approach

It enables a prompt and effective response to the issue in a context of limited resources.

Risk Assessment

When the specific cause has been identified and defined, a risk assessment is done. A priority is assigned for each identified issue. (See Appendix B for priorities.) Using a graded approach, the GL/OL will assess the impact and whether compensatory measures are required. Based on this assessment, the GL/OL will make a prioritization corrective action recommendation to the S&S Program Manager for his approval.

Cost Benefit Analysis

If compensatory measures currently exist, the GL/OL completes a cost-benefit analysis to decide if the risk justifies the cost of new measures. When the resource requirements for alternative actions are known, they are combined with expected net benefits to establish priorities.

Prioritization and the ACA

If compensatory measures do not exist, the issue is prioritized based on the risk assessment. The group leader will determine an alternative course of action (ACA). The ACA includes the level of effort and resources required to resolve the issue. Because issues are noncompliances that must be responded to, the ACA cannot include the option

of doing nothing. If appropriate, a vulnerability analysis is done to determine the most appropriate ACA.

IAP Development

When an ACA is selected, an Issue Action Plan (IAP) is developed using inputs from affected organizations to ensure that the analysis, actions, and compensatory measures are coordinated and represent the most effective solution. (See Appendix D)

IAPs are forwarded to the S&S Program Manager for review.

The following IAP development guidelines apply : (IAP forms the basis for deviation or Compliance Schedule Approval (CSA) requests). The IAP must be as complete and concise as possible.

- Include a summary of the technical bases for proposed actions or positions. Avoid stating a position without a supporting rationale. Include a description of planned activities whenever possible. This will help explain the proposed actions in the context of planned improvements.

- Include recommended corrective action priorities

- Describe the identified root cause(s) or descriptions of planned, ongoing evaluations.

- Include completion/acceptance criteria for each IAP and ensure it matches the stated actions.

- Estimate completion times and budget considerations for actions.

- Delineate deliverance's and responsible organizations associated with each task.

- State the proposed work schedule including realistic deliverables and milestones.

The IAP documents the resolution activities. At a minimum, each issue in the Issues Management System

has an IAP with cross-references showing the issues being resolved by a single plan. Changes in issue status should be reported to the IMC as they occur.

- Perform a cost-benefit analysis to aid in deciding if the risk justifies the cost of new measures. If the cost cannot be justified, a deviation request is prepared citing the analysis and supporting justification and is forwarded to the S&S Program Manager for review.

If the ACA is justified, but FSS resources are not sufficient to address the required actions, the S&S Program Manager will request funding as a part of the annual budget submission.

When funds are allocated, the original IAP is reviewed to find out whether, under the current conditions, the allocated resources are sufficient to do the tasks or whether the scope needs to be refined.

If funding is not allocated by the beginning of the next budget cycle, the GL/OL will prepare and forward a deviation request to the S&S Program Manager for review.

Resolution

The IMC reports all resolution-related activities to Group/Office personnel in FSS as well as entities not under the purview of the S&S Program Manager for their information and response.

FSS Group /Office personnel inform the GL/OL of the status of resolution activities.

The GL/OL provides biweekly progress reports to the IMC for tracking. In turn, the IMC will submit periodic summary reports to the S&S Program Manager and DOE/LAAO.

The IMC informs the GLs /OLs of upcoming milestones.

Verification

When an IAP has been completed, the GL/OL submits a closure package to the IMC documenting resolution. (See "Closure Package" in Appendix C and Appendix D.)

The IMC, with the GL/OL, reviews and verifies the package for completeness and compliance with DOE

requirements, including Standards and Criteria, other guidance, and applicable directives.

Depending on the closure package content, a field evaluation may or may not be required. If an evaluation is required, the IMC and the GL/OL will conduct a joint evaluation/verification.

- If the verification shows the issue has not been addressed, the package is returned to the GL/OL with comments.

- If the verification confirms the work satisfies the issue, the IMC signs and dates the Issue Closure Certificate and recommends S&S Program Manager approval. Once approved, the IMC forwards the closure package to DOE/LAAO or DOE/AL, as appropriate.

The Issues Completion Certificate and the closure package are quality assurance records. Copies of the certificate and the closure package are retained by the IMC and the GL/OL.

Closure

DOE/LAAO or DOE/AL validates the status of externally generated S&S issues and resolutions. The primary S&S contact for this is the IMC.

The IMC coordinates all completion developments with DOE/LAAO and in some cases DOE/AL.

Internally generated S&S issues will be validated by the S&S Program Manager.

Tracking

The S&S PAO maintains the Safeguard and Security Classified Issues Management System (CIMS). This database documents past and on-going S&S audits, reviews and inspections, and self-assessments. It identifies: organizational responsibilities, the results of the reviews and inspections, corrective action milestones, and a database administrator who can produce reports.

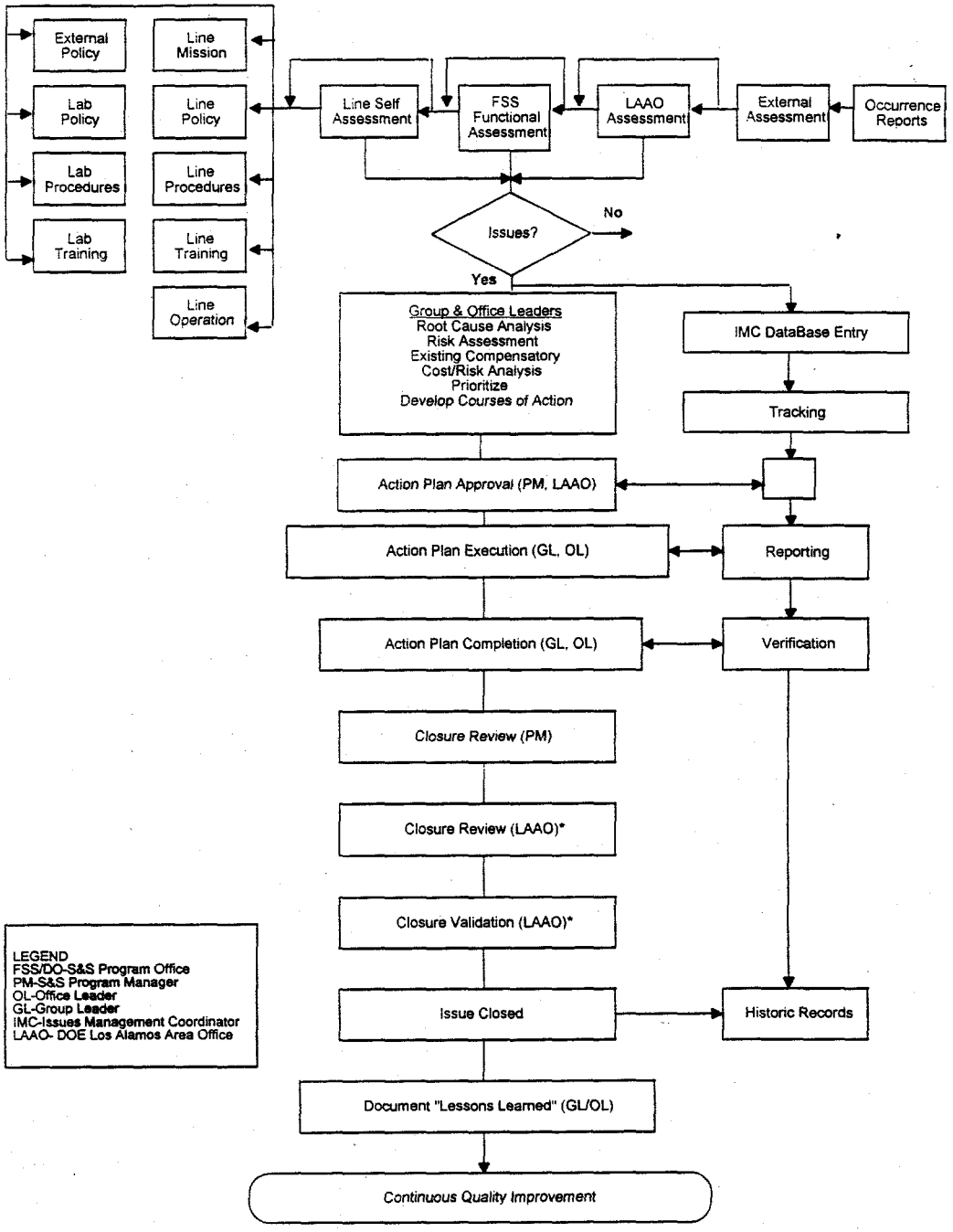
The purpose of this database is to provide a central repository for documentation and results of the various outside inspections and internal self-assessments. The database also provides a proactive program-wide tracking

mechanism to ensure that all findings and self-assessment issues are listed for resolution. The database will track the status and numbers of inspections, self-assessments, and issues throughout the S&S Program. Specialized reports are automated, trends identified and tracked, and other statistical and planning information documented and reported as appropriate.

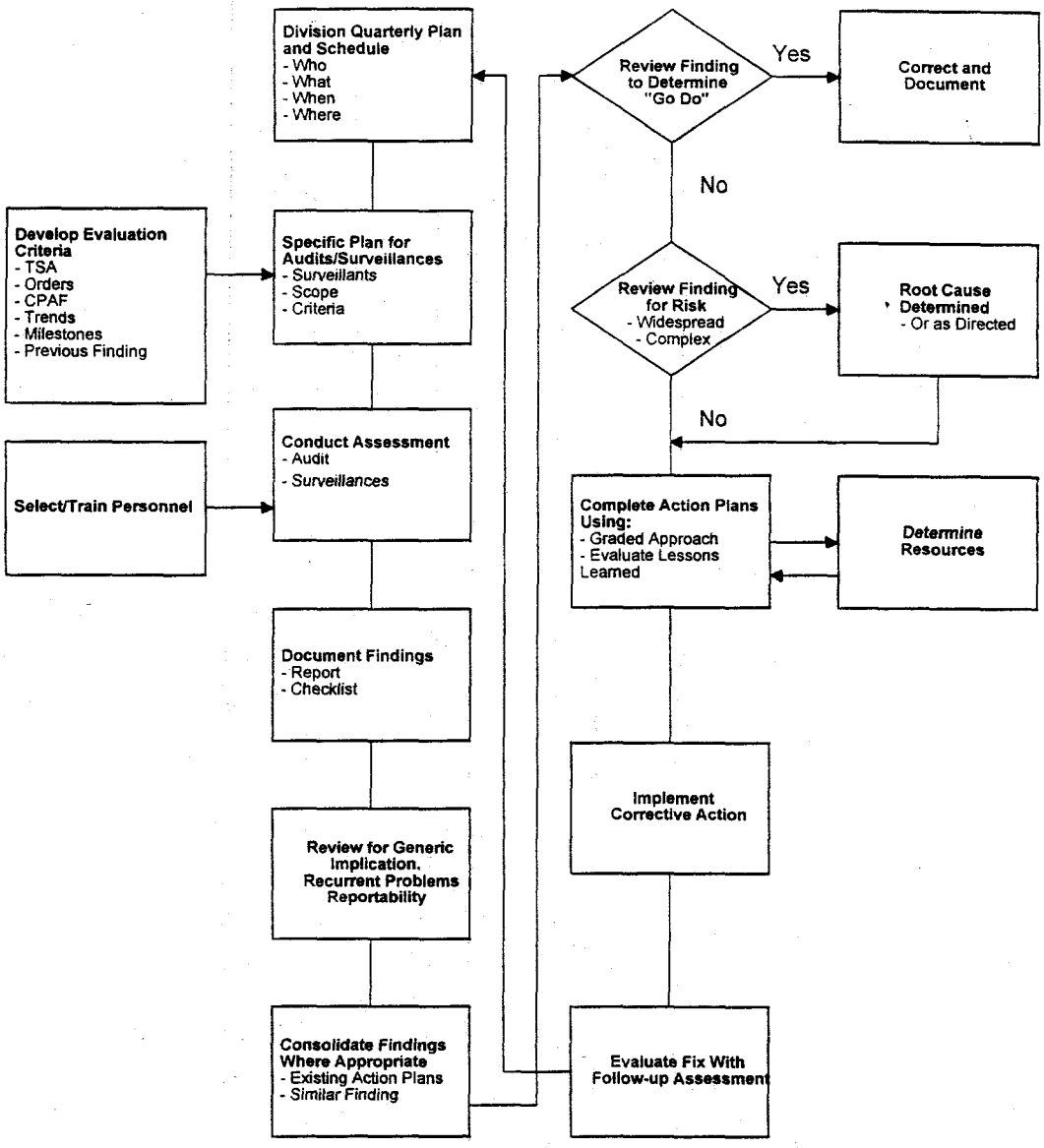
Issues are assessed bimonthly (or more frequently) with review meetings and are tracked until closure.

The tracking process emphasizes total quality management and incorporates analysis to determine associated risks, root cause, duplication and/or trends, cost benefit, and best management practices.

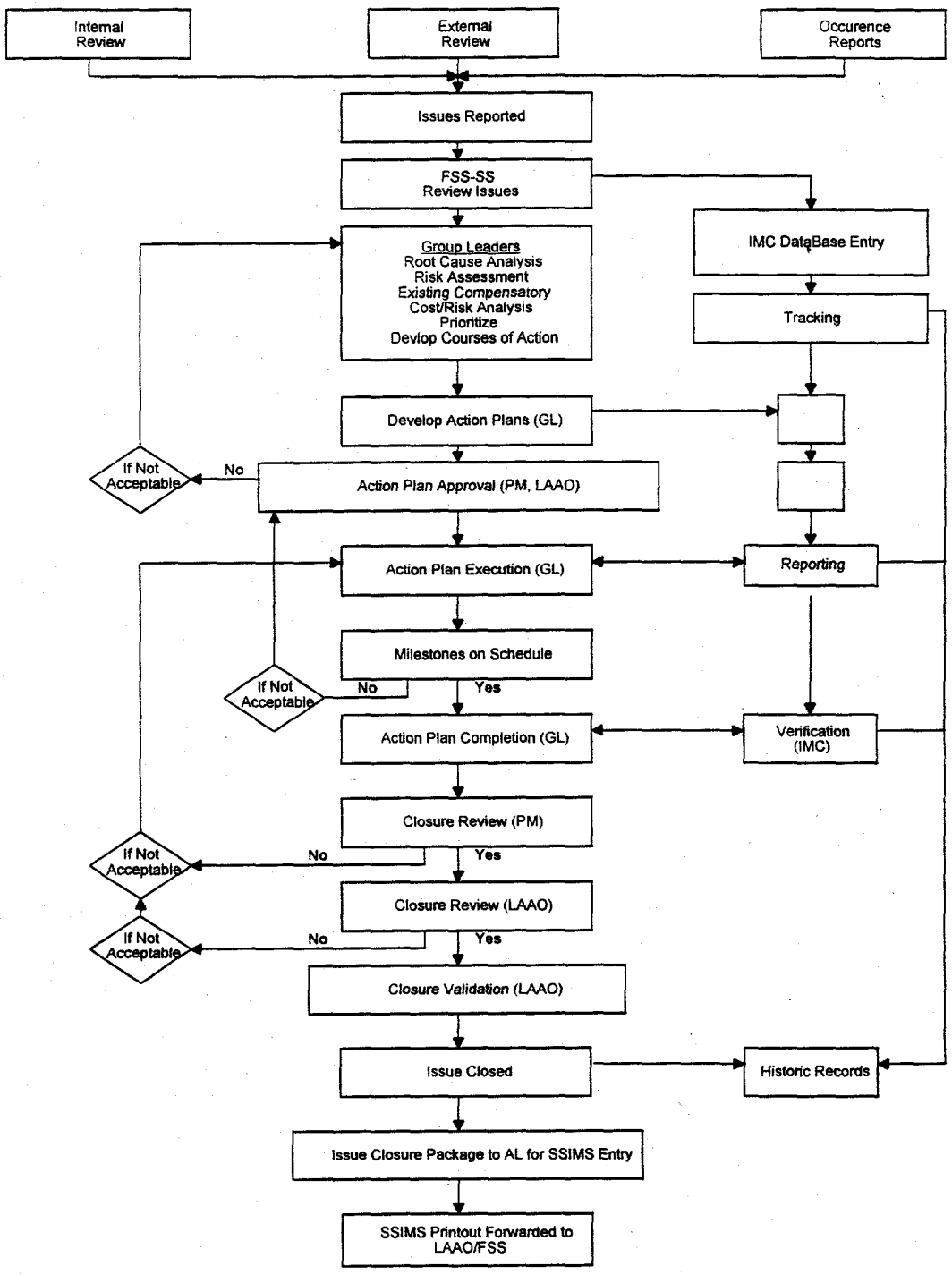
APPENDIX A
Self Assessment and Issue Management Flow Chart



Self Assessment Program Flow Chart



Issue Management Flow Chart



Appendix B
Risk Assessment and Priority Assignment

A root cause analysis is conducted for each issue and formally documented for all Priority 1 and 2 issues. Corrective action plans are developed for each issue. A cost/benefit analysis is conducted to ensure that the corrective action is appropriate considering the associated risk and priority of the issue.

Subject Matter Experts from S&S and organization representatives team to recommend priorities for self-assessment issues to GLs/OLs and make recommendations to the S&S Program Manager for all externally identified issues. This process focuses FSS/S&S on the higher-risk issues first and then on lesser risk issues. Each issue will be assigned one of four priority levels, specified as follows:

Priority 1 **Very High: For issues posing the greatest risk**

The requirement being evaluated does not meet the identified protection need or management requisite, is a vulnerability. If not corrected, it could lead to or cause a significant degradation in the S&S system or component part thereof. A vulnerability to the protection system has been identified, and immediate compensatory measures or system corrections are required.

Priority 2 **High/Moderate: For issues posing great risk**

The requirement being evaluated does not meet the identified protection need or management requisite and is out of compliance. This condition may be a vulnerability if associated with other known deficiencies. If not corrected, this condition could lead to or cause a significant degradation in the S&S system or a component part thereof, but singularly it does not. This issue will immediately be evaluated to determine whether compensatory measures or system corrections are required.

Priority 3 **Moderate/Low: For issues posing low risk**

The requirement being evaluated only partially meets the identified protection need or management requisite or only marginally meets the specified compliance requirement. There is not a significant degradation in the S&S system or a component part thereof. This issue

should be evaluated to determine whether compensatory measures or system corrections are required.

Low: For issues posing little or no risk **Priority 4**

The requirement being evaluated meets the identified protection need or management requisite or is not covered by specific requirements. Quality improvement is indicated as a matter of best business practice. There is no degradation in the S&S system or a component part thereof. This issue should be evaluated to determine whether compensatory measures or system correction is required.

Appendix C

Definitions

Alternative Means and Deviations. Alternate or equivalent means of providing adequate S&S may be proposed to DOE to meet a specific requirement of S&S Program Orders and associated Manuals. Deviations include (1) Variance, (2) Waiver, and (3) Exception. (See definitions below.)

Closed. A database status entry that an action plan has been completed and satisfies DOE requirements. Issues resulting from external surveys and inspections, such as those by DOE/HQ Security Evaluations (SE) and DOE Albuquerque Operations Office (DOE/AL), upon the recommendation of Laboratory S&S professionals must be reported to, and ultimately closed by, DOE. Internally generated issues (e.g., self-assessments and audits) are closed by the responsible S&S group office and verified by the S&S Program Office. (See Finding, Closure Package.)

Closure Package—Appendix D. Documentation forwarded to DOE Los Alamos Area Office (DOE/LAAO) or to DOE/AL for particular S&S disciplines by the S&S Program Office with the supporting rationales from the cognizant S&S group affirming that an external issue has been corrected and is ready for validation by DOE. (See Closed, Verification.) In a few cases, closure packages are sent directly to DOE/AL. At minimum, the package has adequate, organized documentation to present a complete narrative of the issue and its resolution. The following documentation is the minimum acceptable:

- A Certificate of Closure;
- Pertinent documentation (e.g., memos, new policies, audits, training, etc.);
- A completed Issue Action Plan (IAP).

Commitment. An action with a specific due date assigned to and acknowledged by an individual (Group Leader

(GL)/Office Leader (OL)). A commitment generally requires an IAP but can be a recurring action to satisfy Laboratory obligations. A commitment may include a request for information or action taken to satisfy a DOE Order (See Recurring Commitment).

Compensatory Measures. Actions deemed necessary to offset the risk(s) associated with a noncompliance condition until compliance (or a deviation) can be attained.

Compliance Schedule Approval (CSA). A request to DOE that identifies noncompliance to regulatory requirement(s) and seeks temporary relief from requirement(s) while compliance is being achieved. CSAs are required when compliance will take longer than 90 days to achieve from the date of initial submission to DOE.

Concern. An observation that has not been categorized as a finding, deficiency, or recommendation. (See Deficiency, Finding, Issue, Recommendation.)

Deficiency. An identified noncompliance with or deviation from an applicable requirement that is found in, but not limited to, Federal or State regulations or statutes; DOE Orders; contractor or DOE/AL operational procedures and administrative instructions; or any enforceable agreement, consensus, or industry standard. (See Issue.)

Exception. An approved deviation from a DOE Safeguards and Security Order requirement that creates a S&S vulnerability. Exceptions shall be granted only when correction of the nonstandard condition is adjudged to be not feasible and compensatory measures are inadequate to preclude the acceptance of risk. An exception must be approved by DOE/HQ. (See DOE Order 5630.11A.)

- Exceptions may be granted for a period of up to 3 years. All exceptions approved for an unspecified period of time shall be reviewed by the approving official and revalidated on an annual basis.

- Requests for discontinuation of exceptions, including justification, shall be submitted for approval whenever a major change in site S&S configuration or mission

offers an opportunity for corrective action to terminate the nonstandard condition.

- Exceptions shall be documented in appropriate S&S planning documents.

Exception Request. A request to DOE that identifies noncompliance to specific DOE regulatory requirement(s) and seeks relief from said requirement(s).

Finding. A separate and distinct situation (issue) in a surveyed organization that is (1) not in compliance with directives or requirements, (2) a deficiency in the performance of a S&S system, or (3) a concern regarding the adequacy in the performance of a practice. Each "finding" shall reference a specific directive and be assigned a unique identification number to be used with a specific corrective action. (See Issue.)

External Finding. A noncompliance condition identified by an external (e.g., DOE/HQ-Security Evaluation, DOE/AL, etc.) review/survey or occurrence report. Externally generated findings (issues) must be addressed/resolved and can be categorized as closed only by DOE. (See Closed.)

Internal Finding. A Laboratory S&S self-assessment/inspection finding. In most cases, these findings (issues) do not require reporting to non-Laboratory entities and are closed by the S&S Program Manager. (See Closed.)

Graded Approach. The application of requirements such that the sequence of implementation, the depth of detail applied, and the magnitude of resources expended are commensurate with a facility's programmatic importance and potential impact on S&S, the environment, safety, and/or health.

Group Leader (GL)/Office Leader (OL). The individual accountable to the S&S Program Manager for management and staff oversight of a functional area. (See Responsible Manager.)

Issue. Generally, a deviation from an applicable requirement (i.e., Federal or State regulation or statute, DOE Order, or any legally enforceable agreement, consensus, or industry standard) applicable to facilities, personnel, management, etc. An issue may be a single deficiency or a group of deficiencies that represent a trend. However, an issue may be a project (e.g., an upgrade or enhancement) that is undertaken to prevent a non-compliance or deviation from an applicable requirement.

Issue Action Plan—Appendix D A formal document written by a responsible manager that describes the work required to complete a commitment. For the most part, Issue Action Plans (IAPs) describe the work to be done, the reason for performing the work, and associated tasks and schedules. Corrective action plans are a particular type of IAP used to correct survey or inspection findings.

Lead Manager. The person who has acknowledged responsibility for the development and completion of a task that is part of an IAP.

Noncompliance. An identified condition that does not completely conform to a recognized and documented requirement or a recurring commitment. (See Deficiency, Finding.)

Recommendation. A technical opinion from a reviewer that is not definitive, quantifiable, or tied to an applicable requirement.

Recurring Commitment. Commitments that require periodic response to the DOE and other regulatory agencies, i.e., reports, standard updates, and compliance documentation. (See Commitment.)

Responsible Manager (RM). The individual who has acknowledged the responsibility for the development of an Issue Action Plan and the successful resolution of an issue. This may be the S&S GL/OL, or someone designated by the GL/OL, or the S&S Program Manager. The GL/OL has the final responsibility to ensure that issues in his/her area are satisfactorily resolved.

Risk Assessment. The GL/OL must customize the methodology to represent his/her particular problem. This means defining evaluation criteria and scales appropriate to a particular prioritization activity and assessing trade-offs among them. The GL/OL must be able to defend these definitions as the best way to represent the problem's characteristics. When resource requirements for each alternative become known, they are combined with the expected net benefits to assist the S&S Program Manager in establishing priorities.

Root Cause. A root cause is the source of the problem; a issue is only a symptom. Identification of a root cause can be made by simple, informal analysis. All the root causes have been found if correcting them prevents recurrence of the problem.

Task. A singular step that contributes to the completion of an IAP. An IAP may require several tasks to be completed.

Validation. A documented review by DOE/LAAO or DOE/AL, or appropriate authority to ensure the technical adequacy of proposed/completed actions in resolving an issue and preventing a recurrence. If the issue is internally generated, the S&S Program Manager validates the proposed/completed corrective actions and resolution of issues.

Variance. A variance is an DOE/AL approved condition that technically varies from S&S Order requirements, but affords equivalent levels of protection without compensatory measures. A variance may be approved by the Head of a Field Element after coordination with the cognizant Secretarial Officer. (See DOE Order 5630.11A.)

- Variances may be approved for an indefinite period of time.
- Variances shall be documented in the appropriate S&S planning documents.
- Modifications to variances are approved by DOE/AL.

Verification. A documented physical review by the S&S Program Manager to ensure that the corrective actions

taken have resolved the issue and were performed according to the approved IAP.

Verification is a certification by the S&S Program Manager that a completed IAP satisfies the externally generated issue requirement. Verification is the last step before the issue is forwarded to DOE for validation and completion. If the issue is internally generated, the GL/OL will certify the verification to the S&S Program Manager. (See Closed, Validation.)

Waiver. A waiver is an approved nonstandard condition that deviates from DOE Order requirements which, if uncompensated, would create a potential or real vulnerability and, therefore, requires implementation of compensatory measures for the period of the waiver. (See DOE Order 5630.11A.)

- A waiver request shall be submitted to DOE/AL for approval.
- A waiver shall be for a period not to exceed 2 years. At the completion of the first year, a revalidation by HQ/DOE is required.
- Waivers shall be documented in appropriate S&S planning documents.

Appendix D

Forms

Los Alamos National Laboratory
Security & Nuclear Safeguards Survey/Evaluation
(Date of Survey)
Issue Action Plan

Issue No.: (DOE Finding Number)

Issue: (DOE Finding)

Reference: (DOE Reference (i.e. DOE 5637.1.III.4.h.(2)(f))

Root Cause: (A very concise, accurate statement.)

Functional Area: (The DOE functional area (i.e. COMPUTER SECURITY)

Lead Person: (The Group/Office Leader or designee)

Responsible Organization: (The responsible group/office)

Summary: (Several very concise statements describing where S&S program stands in mitigating the finding. Be sure to address the actions.)

Closed by: (The S&S Group/Office Leader) Closure Date: _____

Validation by: (DOE Representative) Validation Date: _____

MILESTONE(S)

Description	Target Date	Revised Date	Actual Date

One or more actions directed at mitigating the issue or deficiency. Actions 5 and 6 (below) are examples of what should be included in every action plan as the last two actions. Each entry should start with an action verb (i.e. develop, review, certify, etc.).

5. Verify closure documentation by S&S Program Manager. TBD

6. Validate closure by DOE. TBD

ISSUE CLOSURE CERTIFICATE

Issue Number:

Issue Statement:

Order/Requirement Statement:

Action Plan Reference (Attach for Verification): _____

Summary of Corrective Actions Taken (Attach Documentation - If Documentation is Not Attached, Provide Its Location and Point of Contact)

CERTIFICATION

1. Completion: _____
   Responsible Manager (Name)

2. S&S Program Manager Verification: Approved:_____ Rejected:_____
   Date:_____
   Comments:

   Verified by: _____
   Name

3. DOE Validation: Approved:_____ Rejected:_____ Date:_____
   Comments:

   Verified by: _____
   Name