

Cyber Security Walk-Through Procedure

This procedure provides a description of the Cyber Security Walk-Through program of the Ames Laboratory, as required by the Ames Laboratory Cyber Security Program Plan.

Comments and questions regarding this procedure should be directed to the contact person listed below:

Name: William Sears
Cyber Security Manager
Address: 334 TASF
Phone: 294-3590

Sign-off Record:

Reviewed by: _____ **Date:** _____
William Sears, Cyber Security Manager

Approved by: _____ **Date:** _____
Dianne DenAdel, Manager, Information Systems

Approved by: _____ **Date:** _____
Tom E. Wessels, Manager, Environment, Safety, Health, and Assurance

Approved by: _____ **Date:** _____
Mark Murphy, Chief Operations Officer

Approved by: _____ **Date:** _____
Dr. Bruce Harmon, Deputy Director

Note: Original Sign-off Record with signatures is on file with ESH&A

1.0 Revision/Review Log

This document will be reviewed once every two (2) years as a minimum.

<u>Revision Number</u>	<u>Effective Date</u>	<u>Contact Person</u>	<u>Pages Affected</u>	<u>Description of Revision</u>
0	11/1/2007	C. Strasburg	All	Initial Issue
1	4/16/2007	C. Strasburg	7	See Revision Description Document
2	2/25/2010	B. Sears	1,2,3	See Revision Description Document

2.0 Purpose and Scope

The Laboratory's policy for Cyber Security Walk-Throughs is documented in Section CM-6 of the Ames Laboratory Low Security Controls Baseline. The Walk-Through program is an integral part of the Ames Laboratory Integrated Safeguards and Security Management (ISSM) System (Plan 10200.029) and the Ames Laboratory Oversight and Assurance Program (Plan 10200.034). A Walk-Through is a planned tour of a Department/Program or area on a routine, scheduled basis, with a specific focus applicable to that Department/Program. The Laboratory's Cyber Security Walk-Through program is designed to provide a mechanism for personal observation and evaluation of the Laboratory's cyber security implementation by management and specialists. It is a look at specific attributes of cyber security against requirements promulgated by the Laboratory, DOE, and other governmental organizations. The Walk-Through process is not intended to produce administrative burden or place unrealistic expectations on managers. However, deficiencies noted will be recorded, analyzed, tracked, and resolved.

3.0 Prerequisite Actions and Requirements

The members of the Walk-Through team have adequate technical understanding of the special requirements and policies they will be assessing against. Also, the Walk-Through team will have an understanding of this Cyber Security Walk-Through procedure and receive orientation to effectively conduct their assigned Walk-Through functions.

4.0 Performance

4.1 Prior Notification

The Cyber Security Manager shall schedule the Cyber Security Walk-Throughs. The Program Director/Department Manager and the Assistant Computer Protection Manager shall be notified in writing two weeks prior to the performance of the Walk-Through. Notification shall include a general definition of the scope of the Walk-Through and a brief description of the Walk-Through process.

4.2 Walk-Through Team Members and Specialties

The Cyber Security Walk-Through Team will involve one cyber security representative to answer questions and discuss cyber security policies and procedures, and another representative to perform system checks and work with the Assistant Computer Program Manager (ACPM) for that program on implementation.

4.3 Walk-Through Process

The Walk-Through process will be conducted according to the following guidelines.

4.3.1 Pre Walk-Through Process

- A meeting is conducted with department managers, program directors, and ACPMs. Participants are briefed by the Walk-Through Team of what will be evaluated and any potential emphasis that may be assessed according to new regulations (DOE, NIST, OMB, etc.).
- A pre-Walk-Through checklist (Form 48400.030, “Pre-Walk-Through Meeting”) details the topics covered and is submitted following this activity.
- A system inventory based on network registration data is provided to the ACPM to ensure that central inventory data is up to date. After corrections are made, machines are selected for review using the following criteria in order of preference:
 1. Systems with recent compliance problems, or for which central monitoring has detected problems with the configuration.
 2. Systems which have been recently registered on the network.
 3. A random selection of remaining systems to ensure that a sufficient number are reviewed.

4.3.2 Walk-Through Process

- When recording notes, observers will tell representatives what they have observed and are writing for report purposes.
- If observers do not understand the computer system’s condition or function, they should ask a supervisor or employee for a briefing of the present security controls.
- Observers should move steadily through the program or department area. If conditions warrant, they will announce that they need to return for a more in-depth appraisal of the computer systems.
- Of the scheduled time, observers will allow about seventy percent for looking at the selected systems, about twenty five percent for wandering around and asking general questions about computer security implementation, and about five percent for a post observation Walk-Through conference.
- Observers will record conditions as concerns or noteworthy practices during the Walk-Through.

4.3.3 Post Walk-Through Process

- Concerns and noteworthy practices will be submitted to the Cyber Security Manager for the final report, tracking, and screening for event reporting.

Ames Laboratory	Procedure	48400.010
Office Information Systems	Revision	2
Title Cyber Security Walk-Through Procedure	Effective Date	02-25-10
Page 4 of 7	Review Date	02-25-12

4.4 Post Walk-Through Conference

The conditions noted during the Walk-Through will be reviewed with the Program Director/Department Manager, Assistant Computer Protection Manager, and other interested members of the Program/Department at the end of the Walk-Through or at a mutually agreed upon time. This conference will provide an opportunity to discuss appropriate corrective actions.

4.5 Walk-Through Report

4.5.1 The written Walk-Through report shall be prepared within two weeks and sent to:

- Deputy Director
- Chief Operations Officer
- Program Director
- ESHA Manager
- Information Systems Manager
- Assistant Computer Protection Managers
- Group Administrators

4.5.2 The report shall include:

- Identification of the individual(s) who conducted the Walk-Through
- A listing of areas and systems reviewed
- A record of the cyber security conditions observed including Findings, Noteworthy Practices and Strengths
- Planned corrective actions

4.5.3 Concerns are categorized by the following for Laboratory wide trend analysis.

1. Adherence to baseline system configurations
2. Effectiveness of user account management procedures
3. Effectiveness of system inventory practices

5.0 Post Performance Activity

5.1 Closeout of Walk-Through Observations

There are three broad observation categories used during the Walk-Through process: Noteworthy Practices, Strengths, and Findings.

Noteworthy Practice

A positive observation, based on objective assessment data, of a particular practice, procedure, process, or system considered so unique or innovative enough that the entire Laboratory might find it beneficial. Mere compliance with mandatory requirements is not considered to be a noteworthy practice. Examples include: implementing an encrypted backup system with off-site media rotation, automated detection, notification, and disabling of idle user accounts, or directly providing cyber security alerts or training to users in the program.

Strength

A mature process or activity that has consistently demonstrated the ability to meet expectations, or a process or activity that efficiently and effectively facilitates and integrates processes, activities, and resources. Examples include: removing all local user accounts from systems, all users operating without administrative privileges, or maintaining a fully up-to-date system inventory.

Finding

A finding is a determination of deficiency pertaining to implementation of a requirement based on a recognized inadequacy or weakness. Findings are categorized as levels 1, 2, or 3. This categorization is necessary to identify the degree of management formality and rigor required for the correction, tracking to closure, and trending of findings.

- **Level 1 Finding:**

Determinations of deficiency of major significance that warrant a high level of attention on the part of line management. Typically these reflect a gap in addressing requirements or a systemic problem at implementing requirements. If left uncorrected, this level of finding could negatively impact the SC mission. Examples include: inadequate network access controls, wide-spread lack of security policy settings, or systemic failure to apply patches in a timely fashion.

- **Level 2 Finding:**

Determinations of deficiency that represent a non-conformance and/or deviation with implementation of a requirement. Multiple determinations of deficiency at this level, when of a similar nature, may be rolled-up together into one or more Level 1 Findings. Level 2 findings can be further qualified by noting the significance of the issue.

High significance issues: Conditions that are an immediate threat to the security of Ames Laboratory's computing environment, could cause severe or permanent data loss, or have potential for significant programmatic impact, such as: user accounts with a blank password, lack of an antivirus program, or systems missing updates.

Moderate significance issues: Conditions that could cause minor or temporary loss in data confidentiality, integrity, or availability, or have potential for minor programmatic impact, such as: users running with unnecessary administrative privileges, failure to meet all baseline security recommendations, using local accounts as opposed to domain accounts.

- **Level 3 Finding:**

Determinations of deficiency where it is recognized that improvements can be gained in process, performance, or efficiency already established for meeting a requirement. This level of finding should also include minor deviations observed during oversight activities that can be promptly corrected and verified as completed. Examples include: unused accounts which have not been disabled on a system, lack of a structured system inventory maintenance plan, or screensaver duration set too long.

Documentation of findings should include the statement of the specific requirement (e.g. Laboratory

policy, control source, etc.), the description of the programmatic breakdown (if applicable), and objective evidence demonstrating the deficiency.

It is the responsibility of the Program/Department to perform the actions necessary to closeout the concerns identified during the Walk-Through according to the requirements for the Finding level assigned to the observation. This includes requesting assistance or desktop support from Information Systems to perform maintenance/service. The following is the time schedule for closing out the QA discrepancies:

- Level 1 Findings – A corrective action plan will be developed and a Plan of Action and Milestones entry will be submitted to track corrective action progress. The plan will be developed and submitted within 30 days of report date. The plan will be completed within 1 year of the report date. Verification is performed by the Chief Operations Officer (COO).
- Level 2 High Significance Findings – Close out by the end of the first full workday after the concerns are identified, or develop a corrective action plan for closeout which must be approved by the CPPM or the COO. Verification is performed by the CPPM.
- Level 2 Moderate Significance Findings – Close out within 60 days of report date or develop corrective action plan for close out which must be approved by the CPPM or COO. Verification is performed by the CPPM.
- Level 3 Findings – Close out as soon as possible, as resources are available. Verification is performed by the area ACPM.

5.2 Lessons Learned

Lessons Learned Reports will be prepared for feedback and continuous improvement as a result of observations identified during the Walk-Through process.

5.3 Annual Trend Analysis of Cyber Security Concerns

Statistics are generated annually by Cyber Security staff based on the Walk-Through observations and quarterly cyber status reports. This information will be communicated to the Executive Council through an annual report.

5.4 Disposition of Records

Walk-Through records will be maintained by the Information Systems office.

Appendix A Tentative Program Review Schedule

January	Condensed Matter Physics (CMP)
February	Materials and Engineering Physics (MEP)
March	Applied Math and Computational Sciences (SCL)
April	Center for Sustainable Environmental Technologies (CSET)
May	Chemical and Biological Sciences
June	Administrative Services
July	
August	
September	No Walk-Through – Year End
October	Environmental and Protection Sciences (EPSCI/MFRC)
November	Information Systems and ESH&A
December	Materials Chemistry (MatChem)