

Integrated Safeguards And Security Management System Communications Plan

April 16, 2001

BACKGROUND

The Laboratory is launching its Integrated Safeguards and Security Management (ISSM) program during 2001, with a goal of having it fully implemented by December 31, 2002. This communications plan supports this effort and has the following five broad stages:

- Stage I: Directives Evaluation (underway; to be completed mid-July. Involves subject-matter-experts and selected employees).
- Stage II: Introduction of ISSM to all employees (timing to be determined).
- Stage III: Gathering feedback and reporting progress to target groups (April-July).
- Stage IV: Introducing ISSM implementation action plan; startup of comprehensive security awareness program (Sept.-Dec.).
- Stage V: Supporting ISSM implementation; ongoing awareness program and other security system improvements (during 2002).

This plan describes the communications designed to support the development and implementation of an ISSM program at the Laboratory. Though specifics are presented and proposed sequences of events are included, this plan should be considered a living document. As such, it will be reviewed periodically and altered as needed to meet current situations.

The plan is designed to be flexible for two reasons. First, to accommodate needed changes to the Laboratory's site-specific program, resulting from the five stages described above. Second, to accommodate the elements included in the DOE's six-month communications schedule. Any posters, videos, fact sheets, or other media developed will be blended into the LLNL program as they become available.

A variety of techniques will be used in implementing the communication program. These are described in detail in Appendix A.

INTENT

As emphasized by General John Gordon, "The success of our national security mission depends on a commitment to excellence in all work we perform..."

while protecting our vital assets. He has stated that this must be done in a laboratory environment that furthers the co-existence of science and security. To this end, the LLNL ISSM communications program is intended to accomplish the following:

- Make sure each employee understands our security program.
- Make sure each employee knows what needs to be protected and why.
- Make sure employees know they need to ask security questions, obtain answers, and propose changes that will improve security.
- Foster in employees an understanding of the need for continuous improvement and feedback in regards to security.
- Help employees understand the need for them to take ownership of security.

STRATEGIES

The following strategies will guide the introduction and implementation of the communication program:

- A low-key but Lab-wide kickoff event will signal the beginning of the ISSM effort, and will be followed immediately with a steady flow of well-timed activities.
- Some employees from all levels will be asked to participate in a feedback program that examines various aspects of the Laboratory's security program. At a minimum, feedback mechanisms would include focus groups, use of directorate Security Points of Contact, and a response system similar to Dialogue that allows receipt of classified or UCNI comments.
- Management will stress the need to establish and maintain two-way communications with employees about ISSM. It is intended for the subject of ISSM to be included regularly in meetings, as appropriate; managers and supervisors are to encourage employees to provide feedback through mechanisms provided; managers and supervisors are to encourage discussion and ask for feedback from their people and pass what they learn back up the chain.
- Communications will be targeted to various employee segments based on what they need to know in regard to ISSM; everyone will not be expected to know everything.
- Employees will be given an explanation of what is new and different about ISSM and why it is better than what we did before. Part of this effort will be the dissemination of the principles and functions of ISSM as outlined by General Gordon.
- Comparisons to ISM will be made and differences will be described clearly.

THE FIVE STAGES

Stage I: Directives Evaluation

In January, General Gordon initiated a three-phase review aimed at ensuring that security requirements changed during the past year are cost-effective for the long-term (Ref. No. 1). He also instituted a six-month hiatus from implementation of new security requirements so as to facilitate the review. According to his directive, each site would develop its own action plan, based on these dates:

- Phase 1, complete by March 6: Review list of security policy requirements documents (attached to letter from John C. Todd, Feb. 21, 2001), "Review of Security Directives, Policy Memoranda, and Other Guidance Issued Since Spring 1999."
- Phase 2, complete by May 1, 2001: Identify details of how implementations can be accomplished on a more cost-effective basis; prepare other options.
- Phase 3, complete by July 13, 2001: Review groups established by DNS for study of concerns raised in Phase 2.

LLNL is now working on Phase 2. This will involve subject matter experts and the input from various LLNL directorates to assist in the evaluations. One or more focus groups will be conducted as part of the process. Communications about this effort will be included in all updates described in future stages of this plan.

Stage II: Introduction of ISSM to all employees

Communications during the introductory period will be aimed at establishing ISSM goals and concepts in the minds of employees. An important aspect of the communications is to help employees understand that ISSM is under development and that the developmental effort requires their participation. They will be asked to participate via an extensive feedback program that will provide all employees opportunities to give opinions, suggestions, and criticisms about ISSM.

Employee communications will also stress that, in developing ISSM, the Laboratory will be looking to enhance security mechanisms already in place by doing the following: streamlining them where possible; making modifications to improve effectiveness; improving the ability of all aspects of security to be systematically integrated into management and work practices at all levels.

Finally, the introductory period will also prepare employees for a process that will take almost two years.

Some of the key elements of the introductory period include the following:

- Communications to all employees that explain the extent of the feedback program they will participate in, and its objectives. This will include a

description of the purpose of Stage I, though only a part of the employee population will be involved.

- Special communications to targeted groups explaining what aspects of safeguards and security that affect their work will be singled out for review and discussion.
- A pacing of activities so as to provide a buildup of information and continuity for all stages of the plan.
- Use of the payroll organizations to not only deliver ISSM messages, but to help people understand them.
- The development of tailored ISSM tools to assist the cascading of information through the management chain to employees.

The introductory program outlined here would take about four weeks. It may include several of the following: follow-up memos to ADs, presentations to department heads / division leaders, information to all employees including General Gordon's letters (Refs. 2 & 3) and comments from Director Tarter, meetings with employees led by payroll organizations, *Newsline* stories and a Director's Office Column. A poster campaign supporting the feedback effort may be introduced, along with a souvenir (mug, T-shirt, or similar item) for people who participate in any of the feedback mechanisms. Each activity would be timed so there is a buildup of information throughout the introductory period.

The first step in the program was to provide the associate directors with an overview of ISSM. This was done at a management offsite in February 2001. The sequence of events for Stage II follows:

Week One: Presentation by AD for Safety and Security to directorate Security Contacts. The Contacts will be given direction on how to bring the information back to their organizations to begin a process of rolling it out to all levels of management and supervision, and to employees. Contacts will be provided with viewgraphs to be used in their presentations, plus handouts.

Week Two: Contacts begin presentations within their directorates. They will provide an overview of ISSM, describe the two-year timetable and purpose of the feedback program to be conducted over next several months, discuss the communication plan including Stage I to show the scope of the overall project, give instruction on how to communicate this information to employees, discuss the similarities and differences between ISSM and ISM, provide a vision of where the Laboratory expects to be by end of 2002, give a preview of General Gordon memo for employees, and introduce ISSM components package.

Week Two: Start organizing up to three pilot focus groups to assess LLNL security programs. (Refers to Month One of Stage III, below.)

Week Three: *Newsline* Director's Office Column by a senior manager, e.g., Director Tarter, Deputy Director for Operations or Associate Director for Safety & Security. This column will cover the essence of directorate presentations, alert employees to General Gordon's memo, discuss feedback/employee involvement

as key component of building program, explain that details will come from payroll organizations, and introduce security contacts.

Week Three: General Gordon comments presented to all employees. Message would include introduction to General Gordon's memo and supportive comments from Director Tarter. All information will be included in a booklet for all employees.

NOTE ABOUT EXTERNAL MEDIA: At this time, we should be prepared for possible media inquiries — "Why are we starting work on an extensive security program at this time?"

Weeks Three and Four: Organizations discuss ISSM with employees. Booklet reprinting General Gordon's memo and presenting principles and functions is given to all employees.

Week Four: Poster 1—Overview of feedback program.

Week Four: *Newsline* reprints General Gordon's memo; updates employees on current activities.

Throughout introductory period: Two important ISSM communications tools will be under development:

1. A website that will serve as a source of information on all aspects of the current LLNL Security Program, including: cyber security, classified document protection, classification, badging, physical security, OPSEC, SAFE (Security Awareness for Employees), and FAQs (frequently asked questions). There will be a link from this site to an ISSM page that will include information about ISSM components, the communication plan, NNSA implementation, and other ISSM activities.
2. A Virtual Help Desk that will use voice and e-mail mechanisms to receive and answer employees' questions regarding security and that employ a searchable database to assure consistent answers.

Stage III: Gathering Feedback

Three types of feedback will be sought: 1) that needed to evaluate DOE policies; 2) ideas for alternative ways of working under DOE directives; 3) how LLNL's own security programs can be improved. Feedback for the latter issue will come from the general Laboratory population. Feedback for the first two will come from SMEs and focus groups from selected programs, and is to be gathered as part of Stage I.

Feedback regarding LLNL programs will be gathered both from focus groups and the Lab-wide employee survey being conducted by the Director's Office. This survey is expected to be done during Summer 2001 and will include security questions. In addition, a separate ISSM survey of a sampling of employees is being considered. Its purpose would be to provide quantitative data to enrich anecdotal data provided by the focus groups.

Overall, up to 20 focus groups will be planned involving 8 to 12 people each (see Appendix B). This includes up to three pilot groups used to test and fine-tune the approach. Groups may include one group of middle managers and two groups of supervisors. Remaining groups will be drawn from the directorates. Though all directorates will be represented, groups will be weighted towards those with the more complex security issues. Also, employees who are not part of a focus group will be encouraged to contact focus group participants or department contacts with their ideas and suggestions.

An important aspect of Stage III is keeping employees apprised of the progress of the feedback process, and how issues raised are being dealt with. This will help cement ISSM as a concept with employees. Monthly e-mails from the AD for Safety & Security to other ADs (started during the first week of Stage I) would bring this information to all organizations. *Newsline* (and *NewsOnLine*) would be the other mechanism for this reporting, covering what groups will be meeting, who is assessing the data, how we are doing in meeting the schedule and other points about the process. Reporting on the results of the security portion of the Lab-wide survey would be part of Stage III. Stage III would take about five months. A sequence of events follows:

Month One

- Conduct pilot focus groups.
- Assess pilot focus group data; fine-tune process.
- Conduct 5 to 7 focus groups using refined process.
- Start program of including *Newsline* articles every two weeks updating employees on ISSM status. Progress of Lab-wide survey will be part of this reporting.
- Poster 2—Encourages people to participate in focus groups, if asked.
- Also during this month: introduce security program website; introduce Virtual Help Desk. Extensive promotion will accompany introduction of both tools, including use of *Newsline*, posters, electronic posters accessed via *NewsOnLine*, direct mail.

Month two

- E-mail from AD for Safety & Security to other ADs updating status of ISSM. (*NOTE: Continue with at least one per month from now on.*)
- Conduct additional focus groups to complete set.
- Poster 3—Continued support for focus groups.

Month three

- Evaluate focus group and other data from employees. This information must be available for inclusion in gap analysis development. Gap analysis is to be completed by August 23.

Months four and five

- Using data gathered, develop comprehensive security awareness program.
- Plan for supporting ISSM Action Plan, due to DOE September 28, 2001.

- Poster 4—Focus groups are over but feedback opportunities exist through security contacts, payroll organizations, Virtual Help Desk.

Stage IV: Communicating ISSM action plan

This stage will be conducted during the final quarter of 2001, following submittal to DOE by September 28 of an action plan based on the gap analysis. The plan is to specify actions necessary to demonstrate that adequate progress will be made towards the December 31, 2002 implementation of ISSM.

Communications regarding the action plan will explain ISSM as it has evolved based on employee feedback, its rationale, what is expected of employees, what is expected of groups/divisions/departments/directorates, and how full implementation will be reached.

An awareness program will be conducted concurrently with communications regarding the action plan. The awareness program will use a multimedia approach to engage employees and educate and inform them about all aspects of security.

On-going communications through the payroll organizations, using guidance and materials developed from a central point, will be supported at the institutional level. The following techniques will be used: Web-based information, *Newsline*, a Security Lessons Learned program, videos, publications, speakers, flyers, and other communications as required.

Activities regarding both the action plan and the awareness program will be scheduled for maximum effectiveness, to minimize conflicts with other programs, to capitalize on the increased awareness resulting from feedback activities, and to maintain a steady—but not frantic—communications flow.

Stage V: Communications to support full implementation

During 2002: A plan will be developed to extend throughout the year. The following guidance will be used in planning a program that will not only be informative and effective, but that can be sustained for the long-term.

- Have top management support *and participation*.
- Develop plan so no activity stands alone. For example, when focus groups are held, follow-up with reports back to the groups, include *Newsline* coverage, look for actions to bring to closure, report on them.
- Tailor messages to specific audiences (supervisors, crafts, people who work on classified computers vs. those who do not) and target areas of the Laboratory with programs that address local situations; avoid “one size fits all” concept.

- Create umbrella communication program aimed at all employees that supports targeted programs. The overall program should form a backdrop for security awareness and focus on broad, key messages.
- Do not just talk to people and send messages down through the management chain; encourage upward and two-way communication.
- Pace broad and local programs so messages have time to register but also so they are reinforced through repetition, continuity, consistency.
- Use many avenues to engage employees: management visibility; communication through first-line supervision; meetings; home mailings; communication trees; print and electronic media; employee involvement through feedback programs, and problem-solving groups.
- Stress the point that this is a management/supervisor program to raise employee awareness and to help implement ISSM, and not a communication effort to be carried out by communicators. In other words, a *Newsline* article does not replace a supervisor working with his or her people on ISSM issues.
- Stress the point that ISSM is not something we, as Laboratory employees, attend to when we have time; it is part of the way we do our jobs.
- Develop clear statements of what the Laboratory wants to accomplish and repeat them often.
- Seek closure on all issues.
- Keep track of the program's effectiveness—are messages getting through, are they understood? Use feedback from employees, interviews with supervisors, spot telephone polls.
- Provide managers/supervisors with tools and guidance to do the job being asked of them.
- Encourage a cascading approach of information dissemination—senior manager to manager, manager to supervisor, and supervisor to employee. But realize that the cascade approach is too slow for time-oriented news or information.
- When dealing with external media, make sure that—whenever possible—employees are notified first of information that will go public.
- Change pace or tone of programs from time-to-time.
- Have a good rationale for why the Laboratory and DOE are implementing ISSM and help employees understand the reasons.

- Use every opportunity to answer this question for employees: What's in it for me?
- Involve employees in developing approaches and testing them.
- Promote successes; help everyone learn from the failures.
- Once program is started don't neglect it.

MEASUREMENT

Formal and informal measurement techniques will be used to test the effectiveness of various aspects of the communication plan. These techniques include the following:

- Focus groups may be held at different times to see if messages are reaching employees, if they are clear, and if new approaches would be effective.
- Surveys may also be employed to determine employees' level of understanding of communications.
- Feedback will be gathered through Security Points of Contact.
- Additional feedback will be gained through observations of supervisors, with the information being passed up the management chains.
- Data will be gathered through the Virtual Help Desk and "frequently asked questions," and will be analyzed to determine problem areas where additional communication, or clearer communication, is needed.

REFERENCES

1. Memo dated January 19, 2001, from John A. Gordon: "Effort to Consolidate Recent Security Requirements in a Cost-Effective Manner."
2. Letter dated March 26, 2001 from John A. Gordon to Distribution: "Implementation of 'Integrated Safeguards and Security Management' for the National Nuclear Security Administration (NNSA)."
3. Letter dated March 26, 2001, from John A. Gordon to all NNSA Federal and Contractor Employees: "Implementation of 'Integrated Safeguards and Security Management' in the National Nuclear Security Administration."

APPENDIX A

Techniques Used for ISSM Communications

The ISSM Communications Plan employs a multi-media approach using existing Laboratory tools and new ones under development (indicated by *). These are described below:

Newsline: This weekly publication is distributed to all employees and will regularly carry security messages through feature articles, news stories, the Directors Office Column, and display advertisements.

NewsOnLine: This electronic newsletter goes to all employees with e-mail access. Issued weekly, or more frequently if needed. Is best used to remind employees of impending activities, to get news out in a timely manner, to underscore messages.

***Virtual Help Desk:** Easily accessible method of answering employees' security questions; will use searchable database to assure consistent answers. Database will also provide information on types of questions most frequently asked; this information may point to problem areas.

Security Refresher Briefing: All employees are required to review Laboratory security requirements annually and pass a quiz. This is a computer-based program.

Security Bulletins: Published as needed to alert employees to security issues.

Director's Video Talks: All employees see these talks, which are usually done twice a year. Security messages to support ISSM development and implementation will be included.

***Safeguards & Security Website:** Source of information on all aspects of current program, including cyber security, classified document protection, classification, badging, physical security, OPSEC. An important feature of this website is a section on "Frequently Asked Questions."

***ISSM Website:** Includes information about ISSM components, communications, implementation, and other activities.

***Foreign Travel Checklist:** This website helps Laboratory travelers plan for safe and secure trips. Links provide information on export controls, counter intelligence warnings, and related subjects.

SAFE Program: The "Security Awareness for Employees" (SAFE) program concentrates on counter-intelligence efforts. In addition to having a comprehensive website, the program employs posters, speakers, focus groups,

briefings, and other awareness/feedback mechanisms to deliver counter-intelligence messages to employees.

Export Controls Website: Provides guidance on the export controls that govern the transfer of commodities, technologies, and software to non-U.S. entities.

Posters: Used regularly to deliver security messages. Will be used as part of ISSM to encourage employees' participation in feedback programs.

***Souvenirs:** Usable items help remind employees of security measures. Such items were used in promoting ISM, and proved popular (flashlights, visors, pins—all with logos).

Directorate Security Contacts: Representatives from all directorates help to ensure consistent security messages are being delivered, serve as feedback conduits from employees to management, and help in planning ISSM implementation.

Focus groups: This technique is used regularly at the Laboratory to test the effectiveness of communications, gain employees' attitudes towards new programs, review directives, and for other issues where thoughtful feedback is required. Will be used as part of ISSM as needed.

New employee orientation: This program ensures that people joining the Laboratory are given essential security information before they begin work.

Security training: An extensive array of courses, both classroom and computer-based, make sure employees have additional security training as their jobs demand throughout their Laboratory careers.

Local newsletters: Various departments throughout the Laboratory produce their own newsletters, either electronically or printed. These will be used to deliver tailored security messages to specific groups of employees.

***ISSM introduction:** The introduction is Stage II of the ISSM Communication Plan. This is an orchestrated program that will introduce the various components of ISSM to all employees. A cascading approach will ensure information moves through all levels of management to employees.

APPENDIX B

Planning for ISSM Focus Groups

Groups will be held during April and May. Up to three pilot groups will be conducted. Each group will last 90 minutes, starting and stopping promptly as a courtesy to participants.

Basic preparations

Facilitators: Due to the number of groups being planned, arrange for at least two or three. These people will run meetings and take flip chart notes.

Documenter: Will use laptop to record comments as accurately as possible.

Project lead: This person (or designee) will sit in on each group to monitor discussions and help answer questions, if needed. Will start off each meeting by introducing sponsor. Also can act as clock-watcher.

Sponsor: AD for Safety & Security. The AD or designee should be at each meeting to thank participants and set tone (see below).

Schedule/rooms: A schedule for all dates and times groups will be held needs to be established. Meeting rooms need to be reserved. Rooms should be reserved for 2.5 hours to allow time to set up and debrief after meeting.

Selection of participants: Participants will be randomly selected. Groups will include one group of middle managers and two groups of supervisors. Remaining groups will be drawn from the directorates. Though all directorates will be represented, groups will be weighted towards those with the more complex security issues.

Group size: Unless people are assigned to attend, we need to invite about twice as many as we hope will be there. We should try for 8 to 12 confirmations. A group can start with four people; it should be canceled if fewer show up.

Invitations: Letters need to be sent to participants asking for RSVP. Follow-up calls (or e-mails) need to be made to participants to remind them to attend.

Thank you's: An ISSM giveaway for each participant would help promote the program and also show appreciation for help. Also, a thank you note should be sent to each participant.

Groups pre-meeting: At least one meeting should be held with facilitators, documenters, project lead and sponsor to go over details, understand roles and logistics.

Schedule for each focus group

Part 1: Getting started—15 minutes

- Gather and settle, take coffee, etc.
- Project lead introduces sponsor.
- Sponsor speaks about 5 minutes; explains why group is important to him; what he expects to gain from them; what he plans to do with information; how it will be reported to participants.
- Project lead takes about 3 minutes to thank participants, explain that they represent thinking of fellow employees; introduces facilitator and documenter.
- Facilitator takes over; gives ground rules, reminds people that comments are captured, not names. Confidentiality is explained.

Parts 2 through X, depending on number of questions and types of questions (see below)—60 minutes

Final part—Communications—15 minutes

This is an exercise to get an idea of how people prefer to receive their communications regarding security. All possible media used or contemplated at the Laboratory would be listed. People would be asked to rate first, second, and third choices and comment at will. They will have from 15 to 20 choices.

Wrap-up

Possible Questions for ISSM Focus Groups

- Q.** Part of introduction—First round: Please give your name, department, and describe—in about one minute — the general mood about security within your workgroup. Include a one-word description—Enthusiastic, Indifferent, Resistant.
Second round: Comment the same way, but this time about your department.
- Q.** Regarding your personal attitude towards security at the Laboratory, would you comment on how good you believe it to be, and why. Use personal experiences and observations as a basis for comment.
Now, please comment on what areas of security should be improved, why you believe this, and what improvements you would suggest.
- Q.** General Gordon has said, “Each individual is directly responsible for following security requirements.” Do you feel responsible? Do you think you need more training or information to carry out this responsibility better? In what areas do you feel your training is insufficient?
- Q.** General Gordon has also said, “My goal is to have your personal commitment of protecting our nation’s vital assets.” What would it take for you to feel more personally committed to the protection of our assets?

Q. The security program is committed to improving employees' awareness of security concerns and how to address them. Communications will come in a variety of ways. Please rate the ways that are the most effective in reaching you (choose three in order of effectiveness):

- *Newsline; NewsOnLine*
- Video productions on Lab TV
- Video productions shown in Laboratory meetings
- Directorate-led training
- Booklets
- Posters
- Letters from Director
- Communications through first-line work supervisor
- Web pages
- Communications through directorates
- Noted speakers

NOTE: Additional questions about improvements to the Laboratory's security system are to be determined.