

**Integrated Safeguards and Security  
Management  
Project Plan  
National Nuclear Security Administration  
U.S. Department of Energy  
Albuquerque Operations Office  
Office of Safeguards and Security**

## Acronyms

**AEC** U.S. Atomic Energy Commission  
**AL** U.S. Department of Energy Albuquerque Operations Office  
**DOE** U.S. Department of Energy  
**ISM** Integrated Safety Management  
**ISSM** Integrated Safeguards and Security Management  
**NNSA** National Nuclear Security Administration  
**S&S** Safeguards and Security

## 1.0 INTRODUCTION

Since 1956 the Albuquerque Operations Office (AL) has played a prominent role in the research, design, manufacture and transportation of nuclear weapons. The classified nature of this work has demanded the implementation of formal security procedures and requirements. Historically, security work has been implemented using a “top-down” approach with security requirements led and directed by the AL Safeguards and Security (S&S) divisions. Recent incidents at National Nuclear Security Administration (NNSA) facilities have caused NNSA and the U.S. Department of Energy (DOE) to review how security is being implemented at their facilities. It has been discovered that this top-down approach to security did not ensure that employees at all levels – both contractor and Federal – understood and took ownership of their individual responsibility for integrating security into their work practices. NNSA therefore challenged its Federal managers to agree to a set of principles and a methodology to promote individual ownership and improvement of security performance at all DOE/NNSA facilities and thereby increase the level of protection provided. This resulted in the development of an Integrated Safeguards and Security Management (ISSM) system for DOE. ISSM is not a standard but a set of principles and a formal methodology that is the basis of integrated management of security in all work practices at all levels by all AL employees. In developing ISSM, DOE drew heavily upon a similar program, the Integrated Safety Management (ISM) system. However, ISSM is not creating a new “program” but rather weaving together existing programs into a “system” that has at its foundation personal responsibility, and including security in all work practices.

With the issuance of DOE Policy, 470.1, *Integrated Safeguards and Security Management*, DOE established a formal framework for the implementation of ISSM at all of its facilities. When fully implemented ISSM will help each employee, and thereby AL as an organization, improve its security performance. This framework, when fully employed, will enable each employee to realize improved security performance and continuous improvement.

The overarching goal of ISSM is relatively simple: effective understanding and implementation of safeguards and security requirements by all AL employees to enable this organization to strive for the goal of 100 percent compliance, 100 percent of the time.

## 2.0 PURPOSE

The purpose of this plan is to define and establish the processes that will be used to develop and implement an effective, compliant, and integrated ISSM system for AL facilities, programs, and projects. Through the execution of this program plan, an ISSM system will be developed and implemented to:

- Communicate AL’s long-term goals, objectives, and philosophies for informing and involving the AL staff in the implementation of ISSM;
- Define how ISSM will be implemented at AL; and

- Provide an over-arching framework to support the accomplishment of AL's ISSM goals and objectives.

### **3.0 ISSM Guiding Principles**

The guiding principles<sup>1</sup> presented below are the fundamental policies that will guide AL actions, from development of safeguards and security directives to performance of work.

Individual Responsibility and Participation. Each individual is directly responsible for following security requirements, and contributing to secure missions and workplaces.

Line Management Responsibility for Safeguards and Security. Line management is directly responsible for the protection of the DOE assets. Appropriate risk analysis is performed prior to work being authorized. Residual risk must be accepted by line management and controls must be in place and verified prior to authorization of operations.

Clear Roles and Responsibilities. Clear and unambiguous lines of authority and responsibility for ensuring safeguards and security must be established and maintained at all organizational levels within the Department and its contractors.

Competence Commensurate with Responsibilities. Individuals must possess the experience, knowledge, skills, and abilities that are necessary to fulfill their security responsibilities.

Balanced Priorities. Resources must be effectively allocated to address safeguards and security, programmatic, and operational considerations, realizing that achieving programmatic goals is a significant component of achieving safeguards and security. Protecting the DOE assets must be a priority whenever activities are planned and performed.

Identification of Safeguards and Security Standards and Requirements. Before work is performed, the associated risk must be evaluated and an agreed-upon set of safeguards and security standards and requirements shall be established which that, if properly implemented, will provide appropriate assurance that DOE assets the worker, the public, and the environment are protected from adverse consequences.

Tailoring of Protection Strategies to Work Being Performed. Administrative and engineering controls to prevent and mitigate risk must be tailored to the work being performed.

## **4.0 ROLES AND RESPONSIBILITIES**

### **4.1 Albuquerque Operations Office – ISSM Coordination Team.**

- Promote teamwork among DOE/NNSA personnel at sites, project offices, and program offices to achieve ISSM system goals and objectives;
- Coordinate ISSM activities for AL divisions and program offices to ensure ISSM is consistently implemented throughout the AL Operations Office;
- Serve as a resource and information clearinghouse by sharing the benefits, experience, and innovative programs among interested and affected parties;

---

<sup>1</sup> U.S. Department of Energy Policy 470.1, Integrated Safeguards and Security Management (ISSM) Policy, dated May 8, 2001.

- Work with DOE-Headquarters Program Offices to avoid imposition of unreasonable demands;
- Develop and implement communication vehicles that encourage feedback including the sharing of lessons learned with all AL employees, supervisors, and managers;
- Provide security assistance, including on-the-job training, desk-top procedures, and contributing to the DOE/NNSA ISSM website, and providing a link on the AL Intranet by which AL employees can provide feedback;
- Assist AL organizations in performing self-assessments; and
- Continually evaluate the effectiveness of the AL ISSM system and promote continuous improvement.

#### **4.2 AL Employees**

- Integrate security, using the ISSM five-step process, into their day-to-day work processes, and help colleagues do the same, by identifying the work processes and determining if security is a factor in the process. If it is, then they discuss how to make sure security is being effectively addressed;
- Promote security awareness, including actively sharing lessons learned with their colleagues;
- Provide input and feedback on the AL ISSM system at its inception and throughout its life-cycle;
- Seek help from AL security professionals as required to integrate security into their day-to-day work processes; and
- Participate in self-assessments and other measurement methodologies, including the development of effective corrective actions.

#### **4.3 AL Managers and Supervisors**

- Demonstrate their commitment to ISSM by communicating and using the ISSM guiding principles and five-step process in all work and work assigned to subordinates;
- Ensure that security and ISSM principles, values, and processes are fully understood and practiced within their programs and projects;
- Promote security awareness;
- Solicit assistance from AL security professionals as required to implement applicable security requirements into work practices;
- Actively support security self-assessments and other measurement measures to improve security at AL and within the AL community; and
- Provide the necessary human, information, systems, and financial resources required for viable security procedures and programs.

#### **4.4 AL Mission Council**

- Serves as the management body to provide periodic reviews of the AL ISSM system;
- Reviews the quarterly ISSM status reports and an annual report and provides feedback;
- Reviews and approves all ISSM goals, objectives and targets;
- Provides leadership and guidance to AL to ensure that the ISSM system promotes the integration of security into all AL work activities;
- Ensures that roles and responsibilities are clear for the implementation of ISSM at AL; and
- Provides the necessary human, information, systems, and financial resources required for viable security procedures and programs.

#### **5.0 SCOPE**

ISSM will be the single security management system that establishes the framework for integrating security into work practices for all people performing work at AL, no matter who employs them. ISSM requires that all work and all workers meet defined security requirements. Once ISSM is fully implemented at AL, every worker will be aware of the security requirements and vulnerabilities associated with their work and workplace, and have confidence in their mitigation. This includes being able to respond positively and confidently to the following questions:

- Are your work and workplace secure?
- How do you know?
- Do you know the security requirements governing your work/workplace and how they are being met?
- Do you know the security vulnerabilities in your work/workplace as they apply to your specific work and whether controls are sufficient to mitigate them?

At AL, ISSM will be implemented in four separate phases which are presented below. This approach will provide for a measured, systematic implementation of ISSM in support of AL's vital national security mission. AL employee ownership, participation, awareness, and feedback are essential elements to each phase.

#### **5.1 Phase I –Where are We Now? (Months One - Three)**

Phase I will focus on the AL-wide rollout, development, and initial implementation of ISSM. Emphasis will be placed on management commitment and employee participation in order to achieve ownership of this system by all employees. Although similar to ISM, ISSM is different and it is important that each employee at AL understand these differences. ISSM will be “formally” launched at AL by:

- Sending a letter from the AL Manager forwarding the brief overview pamphlet electronically to all AL employees.
- Appointment of a “Technical Champion.” Line ownership of ISSM will be key to the success of this system. Therefore, having the AL Manager formally appointing a “Technical Champion” for ISSM will be an important step in the acceptance of this system by AL employees and ensuring that ISSM is applied to all work;

- Holding focus group discussions with selected AL employees who are representative of the entire AL workforce to identify issues and specific actions that should be taken to improve security at AL. Key issues that will be discussed include:
  - ✓ Do you know the security requirements that apply to your job?
  - ✓ What role should management play in implementing ISSM?
  - ✓ Have you been adequately trained to carry out your security responsibilities?
  - ✓ What, if anything is preventing you from fulfilling your security responsibilities?
  - ✓ How can we effectively inform and involve all AL employees in the implementation of ISSM?
  - ✓ How should we measure our success in implementing ISSM?
- Conducting interviews with key management representatives to gain their input on what needs to be improved and how to better involve AL employees in the implementation of ISSM; and
- Sending knowledge tests to selected AL employees to gather data on where security performance and awareness needs to be improved. Results will be anonymous and the short test will be structured around what the “average” AL employee needs to know in order to carry out their security responsibilities.

Employees selected or identified for these discussions also will be contacted throughout the year to obtain one-on-one feedback on ISSM implementation.

## **5.2 Phase II – Where Are We Going? (Month Three)**

The results of the focus group discussions, management interviews, knowledge tests, and AL Intranet feedback will be used to establish the ISSM system objectives and targets for the first year of implementation.

## **5.3 Phase III - ISSM Implementation (Months Three – Twelve)**

The implementation methodologies identified for increasing security awareness will keep employees and management informed and involved in the development and implementation of ISSM at AL. Attached to this Program Plan is a proposed calendar listing of events that will take place during the first six-months of implementation. This listing contains both communication methodologies and activities that are proposed at this time. After the conduct of the management interviews and employee focus group discussions, additional activities will be added to cover the second six-months of implementation and the listed events may be altered and timing changed in order to implement the actions and concerns voiced by AL employees.

Implementation activities are expected to change each year in order to address the ever-evolving goals, targets and objectives. Upon completion, this listing of activities and the ISSM goals, targets, and objectives will be sent to AL Mission Council for review, approval and acceptance as the overall direction for the AL ISSM system.

## **5.3 Phase IV – Management Review**

Management reviews are key to ensuring the overall “health” and continual integration of security into all aspects of the AL mission. They also are required in order to ensure that the AL ISSM system continues to meet AL’s organizational needs over time. As this system is implemented, it may become apparent that certain activities that were put into action during the first year of implementation, are no longer need to meet AL’s overall ISSM goals. Management reviews therefore, will also offer a great opportunity for AL to keep its ISSM system efficient and cost-effective.

The AL Mission Council will serve as the management body to provide periodic reviews of the AL ISSM system. The ISSM Coordinator will send quarterly status reports and an annual report to the Mission Council in order to keep them informed on the implementation of the AL ISSM system. Changes to the ISSM system or issues that AL Management wants to be addressed will be noted and tracked. Additionally, any decisions regarding the AL ISSM system made by the Mission Council will be noted in the AL ISSM system documentation. The frequency of reporting may change subsequent to the management interviews that will be performed during Phase I or after the first year of implementation.

Questions that may be discussed during AL ISSM system Management Reviews may include:

- Are we achieving our objectives and targets? If not, why not and should the objectives be modified?
- Are roles and responsibilities clear and do they make sense?
- Are the right resources being applied?
- Is there adequate monitoring of this system?
- Are employee concerns being identified and addressed?
- Is the AL community truly integrating security into all aspects of its work?
- Is the AL ISSM system assisting AL in integrating security into all aspects of the AL mission?

## **6.0 PARTNERING FOR SUCCESS**

ISSM success is dependent on teamwork among all employees, managers, and security professionals at AL. Teamwork is dependent on effective communications and clear understanding of what is expected. Employees must be empowered to improve security, and provide input on requirements. This is done most effectively at a local level and relies heavily on trust and a belief that suggestions for improvement will be heard. Therefore, it is imperative to implement formal and informal communication methodologies. Proposed communication and implementation methodologies and activities are delineated below.

### **6.1 Fact Sheets**

Fact sheets are a brief summary of administrative and/or technical information that are used to inform the public about a variety of topics that may include (1) proposed DOE actions, projects, or programs; (2) the status and findings of ISSM data gathering activities; (3) release of new security requirements. They present technical and/or procedural information in a format that uses clean and understandable language. They can vary in length and complexity from simple two-page documents to ten-page documents complete with graphic illustrations and glossaries.

Fact sheets are an excellent way in which to facilitate employee understanding by summarizing information contained in complex security orders and manuals in a manner that will promote employee understanding and compliance. Formatting techniques and graphics will be used to make fact sheets more interesting and easy to read. Fact sheets can be produced relatively inexpensively and are easy to distribute. Fact sheets can also be tailored to meet specific information needs identified through feedback.

## **6.2 Graphical Identity**

A graphical identity will be developed so that all ISSM materials will have the same look and feel. This will increase the ready identification of ISSM materials by AL employees.

## **6.3 E-Mail Lists**

The ISSM Implementation Team will use the AL e-mail system to communicate with AL employees, management and other AL Complex ISSM coordinators and teams. E-mail lists of individuals wanting to be kept informed and involved will be developed to facilitate quick communication.

## **6.4 Small Group Security Awareness Meetings**

Large security education meetings and seminars are not as effective as they could be. All too often, employees come to these meetings and are able to checkout because they do not identify with the topic and are not engaged in the meeting. To increase the effectiveness of AL security awareness, educational endeavors will be held in smaller venues such as team, branch, and division meetings. This will allow the security awareness materials to be tailored to meet the needs of each organization. Additionally, this format will encourage employees to ask questions and become more involved, thus increasing the level of understanding by all employees.

## **6.5 Management Interviews**

Management interviews are informal, face-to-face or telephone interviews held with AL managers to acquire information on citizen concerns and attitudes about the DOE, NNSA, and AL S&S program. Information obtained through these interviews will be used to assess the AL community's concerns and information needs and to prepare effective communication methodologies and respond to the concerns and issues identified in the interview process.

## **6.6 Desk-top Procedures**

To ensure that security is properly integrated into all AL work activities; certain operations and activities must be addressed through written procedures. DOE/NNSA has a myriad number of security requirements that are presented in a large number of DOE orders, policies, manuals, and guides. These documents are complex in nature and it is not reasonable or prudent to expect the "average" AL employee to read through them and be able to translate how they apply to their day-to-day work assignments. Therefore, the AL ISSM Team will work with the AL community to identify those situations or work practices that need to be controlled by documented procedures in order to ensure compliance with DOE requirements. Once the procedures are identified, a succinct version will be

developed and distributed to all AL employees as a desktop procedure. Additionally, these procedures will be posted on the AL Intranet.

## **6.7 DOE/NNSA ISSM Website**

Society today is in transition from relying on the mainstay of static analog media to learning to use one that is digitally- based, information rich, and much more adept at communicating complex ideas through imagery and interactive displays of information. To that end, many organizations are communicating messages clearly, simply, and quickly through internal websites.

Historic events, past communication practices and the events of the past year have all worked synergistically to shape current employees' opinions about security. Partnering is the key to the future success of integrating security into all work. Building understanding and consensus for security requirements among security stakeholders requires open communications that promote the dissemination of project information in a manner and form that enables each person to understand their responsibility in implementing ISSM throughout DOE/NNSA. A website will support effective information sharing and consensus building using a variety of standard website tools and techniques. A link to the NNSA/DOE ISSM website will be posted on the AL Intranet.

### **Overview of Proposed Features**

---

Presented below are features that are commonly use in websites and have been proposed for the DOE/NNSA website.

- **About ISSM** - History of ISSM, Charter - Why is it necessary? What are the main tenants? ISSM Policy
- **What's New** - This section updates visitors to the website on what portions of the site contains new information. Within each item there is a link to the new section.
- **ISSM News** - Newsletters, news articles, fact sheets, posters, flyers, quarterly reports, and annual reports
- **ISSM Tools** – Site Spotlight, Where to Start, Gap Analysis Methodologies, Measuring and Monitoring, Raising Awareness, and Project Plans
- **Frequently Asked Questions** - This feature is a listing of commonly asked questions and officially approved responses.
- **Ask the Security Wizard** - An e-mail form that allows people to submit questions directly to ISSM and/or S&S experts.
- **Feedback** - An e-mail form that allows people to tell the ISSM Implementation team how well they are communicating with the public.
- **Slide Show Presentations** - Any slide show that is presented on ISSM will be posted on the web – allowing all AL employees to gain information about what is happening without attending each slide show. Tools such as Microsoft PowerPoint as well as HTML editing programs will be used to convert or prepare any presentation to the web. This gives citizens who missed public meetings the opportunity to review what was presented by the project team.
- **Related Links** - Links to other websites of interest.

- **Future - Discussion Forums** - Online discussion forum application provides a way for employees to discuss issues that are of importance to them from the comfort and convenience of their own office. This feature allows individuals to swap information and continually draws them back to the site.
- **Future - Subscription Services** - The challenge in any web project is to keep visitors coming back. Content has to be fresh and visitors need to be informed of the latest updates. Through an automated subscription service, visitors can sign up to be notified via e-mail every time a page is updated or added to the site or about updates to only those sections to which they have subscriptions. At any time, users can easily cancel or modify their subscription choices or e-mail information.

## **6.8 Checking and Corrective Actions**

Measuring and monitoring ISSM system effectiveness is integral to: (1) assessing the effectiveness of AL security performance; (2) analyzing the root cause of security problems; (3) identifying areas where corrective action is needed; and (4) improving overall system performance and increasing efficiency. In short, monitoring the performance of the security systems in place at AL will assist AL management and employees in managing our business better.

Measuring and monitoring system effectiveness can be a resource intensive effort. It is therefore important that existing reporting systems be used to maximum extent possible. These systems include the annual self-assessment (see below); reports of security incidents and infractions; and external audits. These measurement systems will be viewed from a “system” perspective and additional measurement and monitoring systems will be added only as required to assess ISSM system performance.

ISSM implementation will shift the way in which AL has traditionally performed its security business. Historically, all measurement of security system effectiveness was performed by external organizations that performed periodic independent audits which verified system conformance with DOE Orders. Under ISSM, emphasis will be placed on frequent, ongoing performance assessments that will be performed by the line organizations. Each branch, division, and assistant manager will be asked to identify any and all areas of noncompliance with DOE/NNSA Orders or other regulatory requirements. The AL ISSM Coordination Team will provide them with worksheets to assist them in this task. Individual group assessments will be consolidated into a master listing. This listing will be assessed to determine how many of these instances of noncompliance are stand-alone and how many indicate system-wide noncompliance. Accordingly, corrective action will be focused to address the specific needs of each organization as well AL as a whole.

DOE Order 470.1, *Safeguards and Security Program* requires each organization to perform an annual self-assessment to provide for internal monitoring of compliance and performance with DOE/NNSA/AL security requirements. Historically the AL Safeguards and Physical Security’s Internal Security Branch has performed these self-assessments. Under ISSM, each individual and division will take “ownership” for implementing applicable security procedures and practices. The AL Internal Security Branch will lead the AL self-assessment effort for the upcoming calendar year. However, each AL division with security interests shall perform an annual self-assessment as to how well they are

implementing DOE security requirements that apply to their work. As requested, the AL Safeguards and Physical Security Division's Internal Security Branch will assist the divisions in this endeavor and worksheets will be provided to assist the divisions and program offices in the assessment. AL-wide functions such as security awareness, physical security (e.g., visitor control, badge and pass, fencing, posting, lock and key, lighting, protective force operations) will continue to be assessed by AL Internal Security Branch. The results of these assessments will be rolled-up into a single report. This self-assessment report will be a key indicator of the success of ISSM. Therefore, the results of this effort will be reported to AL Mission Council as a part of the quarterly and annual ISSM status reports.

## **6.9 Knowledge Tests**

Periodically knowledge tests will be sent to selected employees who are representative of the AL community to gather data on how well security awareness campaigns are educating AL employees on their security responsibilities. The short tests will be structured around what an "average" AL employee needs to understand in order to integrate security into their day-to-day activities. Test results will be kept anonymous.





<b>What Will Be Done</b>	<b>Month One</b>	<b>Month Two</b>	<b>Month Three</b>	<b>Month Four</b>	<b>Month Five</b>	<b>Month Six</b>
<b>Data Gathering</b>	<ul style="list-style-type: none"> <li>✓ Focus Group Discussions</li> <li>✓ Management Interviews</li> <li>✓ AL Internet Website Suggestion Box</li> <li>✓ Suggestion Boxes at Guard Gates</li> </ul>	<ul style="list-style-type: none"> <li>✓ Focus Group Discussions</li> <li>✓ Management Interviews</li> <li>✓ Analyze results and adjust ISSM Program Plan</li> </ul>				
<b>Compliance Assessment</b>	<ul style="list-style-type: none"> <li>✓ Review of Survey Findings</li> <li>✓ Employee Knowledge Survey</li> </ul>	<ul style="list-style-type: none"> <li>✓ Analyze results and adjust ISSM Program Plan</li> </ul>		<ul style="list-style-type: none"> <li>✓ Development of Self Assessment Guide for AL Divisions</li> </ul>	<ul style="list-style-type: none"> <li>✓ Management Review and Approval of Self Assessment Guides</li> </ul>	<ul style="list-style-type: none"> <li>✓ Division Self Assessments</li> </ul>
<b>ISSM Goals, Objectives and Targets</b>			<ul style="list-style-type: none"> <li>✓ Establish specific goals, targets and objectives</li> <li>✓ Notify all employees of goals, targets and objectives.</li> </ul>			
<b>Communications/ Security Awareness</b>	<ul style="list-style-type: none"> <li>✓ Issue ISSM Pamphlet</li> <li>✓ Article in new electronic AL News</li> </ul>	<ul style="list-style-type: none"> <li>✓ Design and populate Security/ISSM Website</li> <li>✓ Security Fact Sheet</li> </ul>	<ul style="list-style-type: none"> <li>✓ Article in new electronic AL News</li> <li>✓ Launch Security/ISSM Website</li> <li>✓ Develop security rules for the desktop for all AL employees.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Push electronic Security Fact Sheet by e-mail to all AL employees.</li> <li>✓ Update website</li> <li>✓ Print and issue security rules for the desktop.</li> <li>✓ Post desktop guide(s) on website.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Article in new electronic AL News.</li> <li>✓ Update website</li> <li>✓ Publish Fact Sheet on Security Tips for the Home during the Holiday Season.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Push electronic Security Fact Sheet by e-mail to all AL employees.</li> <li>✓ Update website.</li> </ul>
<b>Measurement and Feedback</b>	<ul style="list-style-type: none"> <li>✓ Review input from employees suggestion box on the AL Internet.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Review input from employees suggestion box on the AL Internet.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Review input from employees suggestion box on the AL Internet.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Publish article in Website progress made in implementing ISSM.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Review input from employees suggestion box on the AL Internet.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Review input from employees suggestion box on the AL Internet.</li> </ul>
<b>Reporting</b>			Quarterly report to AL management on progress of ISSM implementation.			Quarterly report to AL management on ISSM implementation progress.
<b>Management Feedback</b>	<ul style="list-style-type: none"> <li>✓ Appoint ISSM POC &amp; Technical Champion for AL.</li> </ul>			<ul style="list-style-type: none"> <li>✓ Review ISSM Quarterly Report and provide</li> </ul>		

	✓ Provide input to focus group and interviews.			feedback to employees and Implementation Team.		
--	--	--	--	--	--	--