EFCOG Best Practice #39

Security Requirements Integration Team

10/08/05

Facility: Los Alamos National Laboratory

Point of Contact: Benito Salazar 505 665 3428 or bsalazar@lanl.gov

Brief Description of Best Practice: The Safeguards and Security Requirements Integration Team (S&S RIT) promotes Integrated Safeguards and Security Management (ISSM) by supporting systematic integration of S&S planning into all Laboratory construction, facility modification/upgrade, mission change, decommission, demolition and operational projects.

The S&S RIT identifies and addresses security interests that need to be included in the project planning and execution phases of the project review process. Security interests include all Laboratory-controlled classified and sensitive unclassified matter, nuclear materials, critical mission assets, biological select agents and toxins, and other government resources associated with accomplishing the Laboratory mission.

The RIT ensures that appropriate S&S subject matter expert(s) engage Laboratory project managers and the owning organization/responsible project authority in designing, developing and implementing cost effective and sustainable security controls.

Why the Best Practice was used: The RIT provides an avenue for the S&S community to join the process of modernizing Laboratory infrastructure and supporting new missions early in their respective life cycles, in sharp contrast to prior approaches where security issues were introduced into many projects in later, less viable and often more expensive stages.

What are the benefits of the Best Practice:
The RIT establishes points of contact to coordinate input from security experts, facilitates resolution of security issues and supports project managers in applying ISSM principles.

By integrating S&S at the beginning of a project during the planning stage, this approach has eliminated re-work and costly retrofits that were sometimes necessary in the past to accommodate security needs that were not recognized until late in a project or mission change lifecycle.

The RIT approach also provides both project-wide and Laboratory-wide perspectives on security needs and controls, allowing identification of interdependencies among and

between projects and functions across the Laboratory and integration with site planning that can create efficiencies on an institutional level by standardizing S&S approaches.

Another benefit of the S&S RIT process has been the improved ability to plan and manage risk and vulnerability analysis efforts. Through the integration process, the security needs for a project or mission change are determined in a planning venue that gives the project (customer) and S&S organizations an opportunity to proactively identify and negotiate deliverables. This has significantly reduced the number of requests for unscheduled analysis and allowed management to plan for resource needs.

What problems/issues were associated with the Best Practice:
Ensuring that the RIT was notified of projects when they were initiated was a challenge. For example, a parking structure was planned next to a major nuclear facility and the project had reached the point of requesting approval from the Infrastructure and Facilities Committee before security considerations were raised. Identification and assessment of S&S issues resulted in relocation of the parking structure to conform with site protection strategies. Cost and schedule impacts resulting from this necessary change would have been substantially reduced had initial project discussions included consideration of security needs.

To support timely communication and coordination between the RIT and project personnel, the Laboratory took action to modify the institutional construction management requirements to require project managers to have a security representative assigned at project initiation for all projects over $500K. Additionally, the RIT participates in various site planning and long-range institutional planning committees and working groups to improve S&S integration.

How the success of the Best Practice was measured:
Unplanned scope, schedule and cost impacts have been reduced through inclusion of realistic security-related project needs into project baselines.

Additionally, customer perceptions of S&S resulting from unfulfilled obligations, inconsistent products and lack of uniform policy implementation have been reduced/managed through more consistent service delivery and standardized application of security requirements.

Description of process experience using the Best Practice:
Since its inception in 2001, the RIT has coordinated with over 400 projects using a three-level graded approach. Low S&S consequence/value projects receive basic communications and point of contact information for support as needed with the majority of coordination handled by deployed security representatives within the owning organizations. For medium and high S&S consequence/value projects, RIT members provide support and coordination throughout the project as necessary to ensure effective security integration.

The RIT creates and maintains project files for each project in a centralized database. Each project file is updated throughout the lifecycle of the project. Project files may include Preliminary S&S Questionnaires, which can be used to collect security needs information from project personnel in conjunction with formal integration meetings facilitated by the RIT. Based on the project overview and discussion of project security needs presented at the integration meeting, the RIT determines if an S&S Project Team is necessary. If so, Security Program managers are asked to designate subject matter experts who are then identified in a formal S&S Project Appointment Letter that defines their roles and responsibilities. If a project team is not necessary, security integration support is provided by the RIT and deployed security personnel.

Information copies of security-related decisions, reviews, reports, guidance and requirements are provided to the RIT by project management and/or the owning organization for inclusion in the project file. The accumulated history of each project can be used to develop lessons learned and to support development of Laboratory S&S standards.

This best practice relates to the following ISSM guiding principles and core functions.

- Principle 5: Balanced Priorities
- Principle 6: Identification of Security Standards and Requirements
- Principle 7: Work-Tailored Security Controls
- Core Function 1: Define Scope of Work
- Core Function 2: Analysis of Hazards
- Core Function 3: Develop and Implement Hazard Controls