

Idaho National Laboratory (INL) Security Improvement Community of Practice

**Rich Panter
SMC Security Manager**

October 5, 2011

www.inl.gov



Security Improvement CoP

- **What is a “Community of Practice”**
- **How did it evolve**
- **Security Improvement CoP Structure**
- **Commitments**
- **Challenges**
- **Advantages**
- **Accomplishments**

Community of Practice

- **What is a “Community of Practice”:**
 - **Interest** - people who share an interest in improvement and work within a strategic context to solve problems.
 - **Independence** - augment the existing INL organizational structure to identify a problem, create a solution, and manage the corrective action.
 - **Management support** - CoPs approved by Laboratory Director and report to Executive Secretariat. CoP participants viewed as leaders.
- **Objectives:**
 - Improve integration and alignment across INL
 - Provide leadership-management opportunities that both develop our people and encourage ownership and initiative
 - Improve the Laboratory.

How did it evolve – Security Incident

- Several common events across the lab
- No extent of condition process for security incidents
 - “Had I known... I would have taken action...”
- Each classified program/area implementing independent controls/processes to prevent recurrence in their area.
- Prevent recurrence across the lab.
- Increase focus on security awareness at the laboratory level.

Security Improvement CoP Structure

- **Purpose:**

- Promote and facilitate integration among the various classified programs across the INL.
- Provide a formal channel to facilitate information exchange on security performance, trends, concerns, issues, and lessons learned.
- Drive process improvements, advise on effective corrective actions, and strengthen the overall security performance for INL.

- **Membership:**

- INL Classified Program Management (SMC, N&HS, NucOps, CI)
- Key Security Management (IOSC, Classification)
- Leadership Management Team (LMT) Sponsor

Commitments

- Establish process for “Extent of Condition” evaluations
- Share ideas, concerns, issues, findings, lessons learned, effective or ineffective corrective actions, and exchange best business practices
- Identify and remove road blocks that constrain efficient and effective work
- Develop an INL Security Improvement Plan to ensure INL’s focus related to security is well defined and documented
- Promote integration among security and classified program organizations across INL

Challenges

- Breaking down security cultures
- Budgets drive what gets implemented
- IOSC – Classification/investigation issues
- “That’s the way we’ve always done it...”
- Security incidents aren’t just classified program issues, they’re INL issues.

Advantages

- Senior INL Management buy-in
- Active participation is the price of membership
- Members are held accountable to contributing to the success of the CoP
- Unified front – better to tackle issues together than separate

Accomplishments

- “Extent of Condition” process established
- Lessons Learned shared with all classified programs
- Revamping security training for classified programs
- Elevated security awareness to LMT level – security shares at LMT
- Best management practices shared/integrated across classified programs and security entities
- Subcommittees Formed:
 - IOSC variance analysis
 - Functionally/mentor driven security training

Questions

