Best Practice #153

Best Practice Title: *Best Practice: Process for Reporting Security Incidents and Concerns*

Facility: Pacific Northwest National Laboratory, operated by Battelle.

Point of Contact: Sharon Wilder, 509-375-6747; wilder@pnnl.gov.

Brief Description of Best Practice: PNNL developed a program for promptly reviewing incidents of security concern (IOSCs), defining procedures for categorizing, reporting and closing out these incidents, and delineating the actions required by Safeguards and Security Services Division staff members. PNNL worked closely with DOE's Pacific Northwest Site Office—our Cognizant Site Office (CSO)—and the Laboratory's issues management staff. The result is a plan that meets DOE criteria and has been approved by our CSO. The plan also meshes with PNNL's existing processes and uses them for causal analysis, corrective action planning, effectiveness reviews, and a risk matrix that categorizes IOSCs according to the Lab's existing low-, medium-, and high-risk categories. Other DOE Office of Science sites, and National Nuclear Security Administration sites have begun to implement the new order and some have inquired at PNNL for assistance in developing their own programs. A key element of PNNL's success is our partnership with our CSO and the informal processes that has been established to keep them informed of our progress, thus building trust and avoiding surprises. The CSPO helped define the scope of the program and they approved the final product. This collaborative effort builds a positive, ongoing rapport why helping maintain an open, honest communications between the two organizations.

Why the best practice was used: After the Department of Energy created a new order (DOE O 470.4b attachment 5), changing its entire security incident reporting system, DOE contractors began determining how to comply. PNNL took the change as an opportunity to redesign and implement a number of improvements in its program. The result is a cradle-to-grave system that achieves greater consistency in reporting, analyzing causes, and determining risks.

What are the benefits of the best practice: By complying with the new DOE order, PNNL's program focuses more attention on serious issues, as opposed to treating all incidents equally. In the past, both high- and low-risk incidents received a similar, equally rigorous response. Now, by using a graded approach and using the risk ranking sheet on all incidents, PNNL management allocates more resources toward reporting and addressing concerns that pose the greatest risks. The system also allows for more realistic deadlines for initial inquiry and categorization before initial reporting is required. Prior to the new order, security organizations had eight hours to categorize the risk of an IOSC and submit a preliminary report to the DOE, leaving little time to validate their decision. If an incident was determined to be Level 1, the initial report was due in just one hour. The new order grants a five-day window to study potentially compromised information and to make a more informed, thorough and accurate determination of risk before submitting a report. If the risk can be mitigated and classified as Category B, the rigor needed for response is more appropriate and less time consuming, giving security personnel more time to focus on Category A incidents that pose higher risks.

What problems/issues were associated with the best practice: The two central issues in implementing an effective process for reporting security incidents were: First, establishing and agreeing upon appropriate criteria for assigning Category A or Category B status to IOSCs; and, second, building a close working relationship with our CSO. When we reached agreement on the appropriate criteria for categorizing incidents, our relationship with the CSO became important in making sure each incident was clearly understood and correctly assigned to its appropriate category. Working and communicating closely with the CSO to make accurate category assignments helps us verify that we agree on the incident that deserves our greatest attention and remedial efforts. We stay focused on our mission, avoid spending unnecessary time and effort on incidents of lesser concern, and don't waste time on something DOE did not intend us to do. It is important to remain calibrated with the CSO through annual reviews. When the site security plan is up for review, the CSO has an opportunity to make suggestions. Each stakeholder comes back to the table, to refresh the A/B reporting requirements, and renews our common agreement on what will be reported as and IOSC and how it will be categorized. The CSO will be able to approve and review all Category A reports and can negotiate and review B reports. This process has helped build a positive rapport with our CSO. This open and honest communication helps to maintain a high-caliber program. It is much better for us to apprise our CSO counterpart informally when there is an incident than for them to hear it from another source. Informal communication builds trust and can help us make sure there are no surprises for our CSO or PNNL management. We are true partners in the process.

How the success of the Best Practice was measured: PNNL's program is being used as a template for other DOE sites. We assess our security incident reporting system internally with independent self-assessments and peer reviews conducted by parties at the Lab, comparing our system to DOE requirements we must satisfy. DOE has conducted program-assist visits to PNNL where they reviewed not only our reporting system but also our classified holdings, making sure we are categorizing and handling all incidents as we should. Our performance assurance plan includes collecting incident related data and tracking performance and compliance trends in our system from cradle to grave to make certain we are targeting the right things at every stage. Using our trend data as a predictive indicator helps us define the need to participate in PNNL's educational and security awareness activities. This type of forecasting helps us make sure a more proactive approach is taken in keeping incidents from occurring. We have communicated our findings to staff members via brown bag meetings and short articles on specific preventive measures in PNNL's e-newsletter, *Inside PNNL*. We have also created several human performance videos that allow staff members to refresh their memories regarding security issues when it is convenient for them.

Description of process experience using the Best Practice: Our program has proved to be effective in several ways:

- We have seen more consistency in reporting and have a better working relationship with our DOE counterpart.
- We have enhanced our understanding and ability to apply the appropriate degree of rigor to each incident we report, doing so in a graded fashion that matches the degree of risk posed by each incident.
- We are not spending time on an issue simply because it was deemed serious in the past.
- We are producing more thorough and accurate initial reports.
- We continue to apply the same rigor to monitoring trends as we always have.
- We have not noted a reduction in the number of incidents, but this program has helped us do a better job of accurately and appropriately categorizing them.
- In some ways, we are reporting more incidents because DOE's requirements have become stricter than in the past.