** Best Business Practice **

Title: Establishment of a Strategic Information Security Working Group

Points of Contact:

Marcia L. Baird, Consolidated Nuclear Security, LLC, (Y12)

Brief Description of Best Practice:

This Best Practice describes steps to promote a collaborative and strategic Information Security partnership within Safeguards & Security, the Y-12 site and the federal customer. From 2013 to 2017, after transitioning from the NNSA Policy Letter back to DOE Orders, the Y-12 site faced many Information Security challenges. In addition, in 2017 the site experienced two significant 10 CFR 824 events relating to the protection of classified matter. With several years of impactful events and in desperate need of resolution to classified matter issues, Consolidated Nuclear Security (CNS), in partnership with our Nuclear Production Office (NPO) federal customer, formed the Information Security Working Group. Members included NPO Deputy Director S&S, NPO managers for Classification, Information Protection (CMPC, TSCM, OPSEC), Vulnerability Assessment, Nuclear Material Control & Accountability, Physical Security (including systems), Performance Assurance, Protective Force, and IOSC as well as CNS S&S Sr. Leaders and managers/representatives representing the same disciplines. In addition, CNS also included Cyber Security, the Uranium Processing Facility, and organizational Division Security Officers. This working group met every 5 weeks to brainstorm solutions to problems, share problems with implementing solutions, and celebrate successes. Actions tracked, milestones discussed and managed, and ultimately problems were solved. In 2020, after a successful Enterprise Assessment, this effort has grown into what is now an even more expanded and collaborative team adding representatives from both sites as well as representatives from Counterintelligence, Export Control, Information Release, and Nuclear Enterprise Assurance.

Why the Best Practice was used?

This Best Practice was used to achieve a multi-disciplinary, unconventional, collaborative approach to understanding, sharing, and collaborating on Information Security issues, successes, and future endeavors. The formation of this working group allowed the once stove piped thinking and communication barriers to be broken down and blossom into a collaborative effort in which all of the members played a role in problem solving some of the sites biggest issues related to Information Security. The group continues to be the conduit for information sharing both solutions to problems and opportunities for awareness/additional training.

What are the benefits of the Best Practice?

The benefits of this Best Practice include:

- Increases buy-in from multiple areas when information security changes are necessary..
- Assures appropriate level of understanding, input and outcome for information security activities.
- Serves as lessons learned for issues, awareness, incidents, and other information security related problems/successes.
- Validates thorough analysis and perspective from other security disciplines as well as garners buy-in from NPO customer for corrective actions prior to submittal and implementation.
- Break-down barriers and ensures there are enough people with all perspectives involved prior to making costly modifications or implementing unrealistic/unachievable requirements.
- Serves as the catalyst for an Information Protection Governance Counsel made up of Vice Presidents and Site Sr. Leaders.

What problems/issues were associated with the Best Practice?

Problems/issues associated with the Best Practice include:

- A number of good ideas for solution, but with hesitation on leading the change.
- Managing meetings in the appropriate environment.
- Maintaining the Sr. Management presence which is a must. Their engagement ensures everyone remains engaged and understands the priorities.

How the success of the Best Practice was measured:

This Best Practice was demonstrated by:

- Improved communication and collaboration, resulting in longstanding information security issues resolution.
- Reduced IOSCs related to Information Protection.
- Smoother/more expeditious security plan approval for nonconforming storage plans.
- Approval of the Limited Nonconforming Storage practice.
- Reduction of cost associated with compliant classified matter storage.

Description of process experience using the Best Practice:

Establishment of a small team is usually easy, especially when there is one common goal, and establishing this working group was at first challenging. The challenges included making sure you had the right disciplines in the room, to include NPO, working around schedules, and working to ensure the topics to be discussed would have the right environment (classified vs unclassified) to be presented in. As the team grew, side meetings would need to be held on various topics, but that allowed the smaller teams with the most interest to break off and get to work, much like the committees within the EFCOG. Due to the number of complicated issues, the first year was often spent just trying to solve problems and gain buy-in. The most amazing thing is that it wasn't always the CMPC or Information Security person solving the problem, other SMEs began to provide their thoughts and perspectives. NPO was right in the middle of the discussion and we had real time feedback on whether a proposed solution would be accepted by the risk acceptors. Opportunities to try new approaches and explore unique options to age old problems were available and often accepted, at least to pilot, by the customer. While working through the problems, lessons learned across security and other organizations was understood almost in real time. Meeting every 5 weeks allowed time to work through possible solutions and bring data back information to the larger team. Training and awareness for information security grew. In 2020, the team was officially chartered, additional members added and the expansion of information security awareness at the Y-12 and Pantex Site continue to soar.