EFCOG Joint Meeting

4/24/18

SRS = 300 sq. Mile footprint

ISM O updated in 2017 (DOE O 450.4A?) - workers encouraged to have questioning attitude free of fear of reprisal

David Weitzman (for Pat Worthingon):

- Safety Culture Improvement Panel (SCIP) meeting in May in NLV: top goal is to find ways for feds and contractors to better work together to improve safety culture across DOE complex
- Amendment to Worker Health and Safety Order (10CFR851) - requires sites to update consensus standards to most recent versions - you have until 1/17/19 to implement

Gary Staffo - Accident Investigation and Prevention Program:

- Recruiting new members and offering training to replace retiring members. Have much fewer accidents in recent years due to increase in Safety Culture and awareness.
- DOE O 225.1B and companion Handbook
- Question employee's fitness for duty if something doesn't seem right or if the employee appears to be at risk due to health concerns
- Formal accident investigation can be required if one or more of the following occurs:
  - Death
  - Hospitalization of more than 5 days
  - Multiple employees losing workdays due to injury• other extenuating circumstances
- EIP-120DE, Accident Investigation Overview (online) - see if I can take this• Gary.staffo@hq.doe.gov (202) 586-9577

Christian Palay - AU-32, QA & Nuclear Safety Management Programs:

- 414 Guide will be submitted to Defense Review Board very soon (released within next 2-3months)
- CGD Handbook goals - into RevCom by July, published by next March
- Will reconvene DOE Quality Council
- Developing training for: S/CI, CGD, and Graded Approach
- Assessing need to revise 414.1D (recognizing Non-830 SW is also important) - within next3 years
- Looking to NNSA and EM to find a replacement for Subir. Must be DOE SQA SME qualified• 202-586-7877
- Sonja Barnette and Duli Agarwal are part of his group

Jan Preston - Safety Working Group:

- 7 Best Practices (BP) published by the ISM & QA EFCOG group last year
- SQA Auditing Protocols White Paper BP
- Question if any of our BPs should have training associated with them (Auditing, SW CGD, etc.)
- Where are our pain points/struggles?
- Strong push for all sites to participate in the single supplier list (MASL)
- Looking into reducing regulations

- Once you start a supplier evaluation, freeze requirement set; don't "update" during audit or three+ year blessed period even if DOE O or requirement is changed during that time

Mike Sheraton - QA P&P Group:
- Graded Approach has been used in the past as an excuse to not do quality

Bill Wingfield - Supply Chain:
- Lots of work on MASL and audit checklists

Chuck Ramsey - HPI:
- Gather Lessons learned and positive practices
- developing HPI training - already has a firm 5-year funded budget for this
- Can't just use your own successes (or feeling of success) as a barometer or how well you are doing. Need to benchmark with others and share approaches and struggles to stay fresh and continuously improving.
- "Things that don't get measured, don't get managed" - Deming

Darlene Murdoch - Contractor Assurance System:
- Tools developed by the group include a Maturity Model; LOIs for CAS Effectiveness validation; Assessment Plan template(?)
- Working on Best Practices on how to solve CAS issues

EFCOG SQA Group

NOTE: Email group requesting information on their site's mission and cohesiveness of SQA SME groups

Supplier Audit Checklists (MASL):
- Must include Req. 3, (7?), 11, and Subparts 2.7 and 2.14
- Action Item (Vicki) – Get update of matrix from Steve O
- Contract with vendors must specifically invoke 2.7
- Approaches to audits:
  - Compliance matrix with objective evidence that they are following it
  - Process audit (procedures showing they are following NQA-1)
  - JSEP had a lot of detailed info; MASL and NIAC do not - not enough info to determine if the audit can be used.
  - Steve Gauthier (ANL) received an audit LANL did with a lot of good detail - maybe use this as a starting point
  - Sid - starts with NQA-1 requirement checklist, then look at what procedures they are using to implement the requirements
- Paula D (LANL) - if objective is to have confidence in MASL, it is disturbing that the MASL auditors don't recognize importance of SQA-specific questions; need a SQA SME on the audit team (not just the detailed checklist)
- Question really boils down to the execution of the audit itself - right team asking right questions, getting right evidence
- MASL needs enough detail to make an evaluation of sufficiency
- MASL - does it include qualifications of team members?

- Action Item (entire SQA group) – Each site should ask their internal supply chain group if they've done an SQA-related audit; review reports for detail; was a checklist used? Can it be shared?
- Action Item (Vicki) – Talk to Bill about details captured in MASL, including auditor qualifications
- Action Item (Vicki) – Add NQA-1 Subpart 2.7 checklist from Steve Gauthier (ANL) on the Box site (EFCOG Share Folder → Spring 2018 Meeting at Savannah River → MASL Checklists)
-

Toolbox Codes:

- Christian Palay wants to expand the Toolbox to include more titles; however, individual sites must do diligence that ensure they are using the code correctly and it is meeting individual needs
- Action Item (Vicki) – send Christian the history of the Audit Task Force and feelings around Toolbox codes
- Could we help qualify titles and new versions?
- Could we leverage MASL? What would we need to add to MASL audits so that we could
  - leverage them? (JSEP had things like auditor qualifications)
- Action Item (entire SQA group) – gather list of software titles and version numbers we would like to see in Toolbox - prioritized and with reasoning why it is needed (what the qualification limitations would be)
- Checklist with requirements/LOI/acceptable objective evidence

POSSIBLE NEW TASK: LIST OF NEW SW TITLES AND VERSIONS FOR DOE TOOLBOX (DUE FALL 2018)

EFCOG SQA Group

4/25/18

CRADS:

- Carol Olijar's (ANL) CRADs were created by Debbie Sparkman (DOE HQ) and based on NQA-1-2000. Two examples - straight CRADs (smaller handout) and Objective/WA 1 filled out (larger handout)
- Two columns:
  - Column 1: Criteria statements
  - Column 2: Documents and Records = objective evidence to meet each criterion (this can be filled out by auditee prior to the audit)
- Row below row with objective's criteria/records is a row of approach and lines of inquiry to be asked by auditor during the face-to-face part of the audit
- The auditee fills out the form at least two weeks prior to on-site visit and creates folders to house all referenced documents and records, giving auditor access to the folder/sub folders (sub folders might be by objectives with a general folder for umbrella documents)
- The audit team would interview project members during on-site visit using the LOIs
- This is a more formal internal independent assessment or even an external assessment
- LLNL's CRADs were shown. More practice based; not tied directly to NQA-1 statements; divided up by 10 Safety Software Work Activities; LOI are broken out by individual criterion, making writing of final report easier.
- Copies of the NQA-1-2000 and LLNL CRADS are on the Box site (EFCOG Share Folder → Spring 2018 Meeting at Savannah River → SQA CRADs)

R&D = rip-off and duplicate

Acquired SW Updates:

- INL - has a team that does all testing; hosted on controlled servers
- ANL - IT group controls the downloads and does testing. Control downloads to once a quarter, at the most
  - A JIRA ticket is created,
  - IT evaluates changes in new version and recommends whether or not to update,
  - RI makes final determination
  - Only IT can install software and/or updates;
  - For minor changes, just do "smoke tests" to make sure major functionality is working as expected
- PNNL - evaluate updates on a case by case basis; perform some type of tests based on impact of change (e.g., minor updates would not require full acceptance testing)
- SRS and INL - SSW titles are only hosted on a stand-alone, separate set of servers that are better controlled as far as updates to titles and updates to underlying platforms; also have list of applications with exclusions (e.g., app xyz can only work on Windows XP); these are behind firewalls to better control / eliminate outside access
- Not all Labs have separate computers / servers for their safety software, which is not in compliance with NQA-1.
- The ASME NQA-1 committee are currently working on a white paper about rapid changes in technology and how to accommodate the way technology is changing

Graded Approach:

- Lance Presentation (SRS):
  - SRS revised their graded approach in 2017 - waiting for final DOE approval
  - Partnering with DOE oversight to make sure everyone is on-board
  - Key for table on slide 4: SC = safety class; SS = safety significant; PS = production support; GS = general software; R = required; G = graded - this table represents the old program. An updated table does not yet exist (will be created once the new procedure has been approved)
  - S1 = DOE 414 Guide's Level A, etc.
  - If software is part of waste affecting (WA) software there are specific requirements for that software similar to Safety software
  - Defines what falls under S1, S2, and S3 in slides 7 and 8
- For Non-safety software - all apps must have a SQAP, that tells classification level and what practices are graded and how. Non-safety, unless non-nuclear safety-related, grading is a business decision
- Table on slide 12: level of rigor is low, medium and high
- If something falls into two rows, must follow the higher level of rigor
- Once the new approach (QAP) is signed by DOE, there will be at least a 1-year implementation plan to bring everything into compliance
- Design authority and application "owner" classify the software (SC, SS, PS, etc)
- If an app is categorized as one thing (e.g., SS), but will then be used by someone else as another, higher thing (SC), then the software must be classified /qualified a second time at the higher level (if originally classified as a higher level and used at a lower level, a second qualification is not needed).
- At INL, classification/level needs to be reviewed and revised (if appropriate) any time the baseline changes (based on usage)
- When the safety basis plan changes (e.g., new usage of existing software), that triggers reclassification/requalification and updates to documents and procedures based on the change in rigor levels
- ACTION ITEM: VP - Upload Lance's presentation on to Box site (EFCOG Share Folder → Spring 2018 Meeting at Savannah River → Graded Approach)

EFCOG SQA

4/26/18

Firmware:

- If you *cannot* change the functionality of the software, treat it as a whole system; controls are still there, but less than the whole SQA practices
- If you *can* change the functionality, more control and SQA is applied
- Just selecting devices and naming relays does not count as programming
- **Do not open a box to read the chip number** if that will break the warranty of the device. Just keep it under configuration control in the M&TE program.
- If a vendor comes in to change hardware, make sure they do not change the software at that time. If they do, treat this as a new version of the firmware.
- Just because you cannot modify firmware, does not mean that it is not safety software or important
- There is some level of the 10 WA that are applicable to different levels of firmware
- See paper for examples of the different levels based on how modifiable the firmware is (Box site → EFCOG Share Folder → Spring 2018 Meeting at Savannah River → Firmware)