QUALITY ASSURANCE EXCHANGE

Volume 1, Issue 2
September 2005

U.S. Department of Energy, Office of Corporate Performance Assessment
Office of Quality Assurance Programs (EH-31)

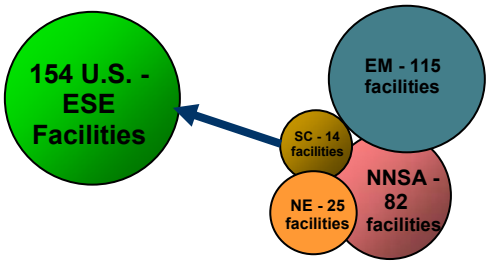
IN THE SPOTLIGHT: INTERVIEW WITH CHIP LAGDON

ACTING CHIEF OF NUCLEAR SAFETY
ENERGY, SCIENCE AND ENVIRONMENT

In a recent interview, Chip Lagdon, Acting Chief of Nuclear Safety for Energy, Science and Environment (ESE) briefly discussed the role of the Central Technical Authority (CTA) and his role in the new organization. In addition, he highlighted the challenges for and the benefits to DOE as a result of the recently issued DOE Order 414.1C, *Quality Assurance.*

Q: Tell us about the role of the (CTA) and more specifically about your role as Chief of ESE Nuclear Safety (CENS).

A: "The Under Secretary is the CTA for ESE's nuclear activities and is responsible for the proper implementation of DOE nuclear safety policy and requirements at ESE facilities (See Diagram 1). I am responsible for providing independent expert technical advice to the Under Secretary to make sure that function is being carried out by his line managers. I intend to accomplish this through maintaining operational awareness of nuclear activities through reinvigoration of Integrated Safety Management (ISM) by the line and implementation of the new oversight order, strengthening the process



	HC1	2	3	Total # of facilities
Environmental Management (EM)	0	85	30	115
Nuclear Energy (NE)	2	17	6	25
Science (SC)	0	5	9	14
	2	107	45	154

Diagram 1 **CTA Nuclear Facility Portfolio**

(Continued on page 5)

DOE ORDER 414.1C ROLLOUT

The Quality Assurance Order Rollout Video Conferences were held July 25th and August 4th , 2005, at the DOE Forrestal Building, Washington, D.C. Over 20 DOE sites nationwide participated in the video conferences. The primary objectives of the video conferences were to exchange information on the Order, which was issued on June 17, 2005, and the associated DOE Guides, DOE G 414.1-4 and DOE G 414.1-2A; to establish clear and uniform understanding on the new requirements in the Order; and to outline DOE expectations as well as available support and assistance in the implementation.

The conference focused on the Order implementation roles and responsibilities and the significant changes to the Order includ-

(Continued on page 6)

INSIDE THIS ISSUE:

LESSONS LEARNED FROM SQA ASSESSMENTS

The Department's Implementation Plan for DNFSB Recommendation 2002-1 required that assessments of safety system software and firmware be conducted at defense nuclear facilities. As a result of the initial assessments, the following software quality assurance lessons learned were developed and utilized in the new requirements and guidance.

- ***Software Requirement Document (SRD) and Software Design Document (SDD) are essential for developing quality software and life cycle maintenance.***

  The information for SRDs and SDDs is typically extracted from system design documents that provide the process system design and operation details. System design documents generally do not address software application, its functionality and performance requirements that are essential for the software design and development. Success of a software development project relies heavily on how well the software requirements are defined. In the absence of SRD and SDD, the software developer must rely on good communication with the system design engineer and understanding of the system design document.

  Observations: It is evident from site assessments that the majority of software projects did not have SRDs and SDDs. The sites using the SRDs and SDDs were found to have clear understanding of what was needed to develop and maintain the quality of the software. The sites without the benefit of the SRDs and SDDs appeared to be relying heavily on the available experts on the projects and also on the process system engineers to ensure that the software developed or procured would meet the project needs. This is particularly important for the software used for the process system controls.

- ***Software procurement specifications should specify details of software requirements, not just catalog data.***

  Software procurement should be a key component of the SQA program to ensure clear requirements and responsibilities for planning and executing procurement of software related items and services. Appropriate interface with Engineering and Information Technology departments should be established and proceduralized. Proper evaluation and qualification of suppliers in accordance with the AMSE NQA-1 standard and follow up surveys and re-evaluation are crucial to SQA. Absence of technical requirements in the procurement specification could contribute to poor quality products, or products with limitations. Vendors typically provide many features, and without appropriate specifications selection of the features could be limited. The procurement specification should also specify quality and documentation requirements commensurate with software applications.

  Observations: The sites procuring programmable logic controllers for the process systems only specified the vendors' catalog model information for procurement specifications without any supporting documentation for the suitability and applicability of the technical requirements.

- ***Formal procedures for software problem reporting and corrective actions for software errors and failures need to be rigorously maintained and implemented.***

(Continued on page 4)

DID YOU KNOW?

Did you know that the Goal/Question/Metric (GQM) paradigm looks at the goals of the customer to better align the measurements and metrics with the customer's business goals? GQM asks questions about the types of information needed to determine whether there is movement towards those goals or if the goals have been achieved. It then selects metrics to provide the information needed to help answer those questions. This method is used to ensure that metrics are selected that align with the goals of the metric customer. Many publications are available for additional detail on the GQM paradigm.

One such paper can be found at http://www.cs.umd.edu/projects/SoftEng/ESEG/papers/gqm.pdf.

SQA—WORK ACTIVITY 1

Software Project Management and Quality Planning and ASME NQA-1-2000

This article is the second in a series that addresses how the software quality assurance (SQA) 10 work activities in the DOE O 414.1C relate to American Society of Mechanical Engineers (ASME) NQA-1-2000 and other consensus standards. DOE G 414.1-4 provides details for implementing the 10 work activities in the DOE O 414.1C.

Work activity #1, Software Project Management and Quality Planning, is the fundamental process that ensures that software quality activities are planned and included in the overall execution of system/software life cycle work.

As with any system, project management and quality planning are key elements to establishing the foundation to ensure a quality product that meets project goals. For software, project management starts with the system level project management and quality planning. Software specific tasks are identified and either included within the overall system planning or in separate software planning documents.

These tasks are documented in a software project management plan (SPMP), an SQA plan (SQAP), a software development plan (SDP), or similar documents. They also may be embedded in the overall system level planning documents. The SPMP, SQAP, and/or SDP are the controlling documents that define and guide the processes necessary to satisfy project requirements, including the software quality requirements. These plans are initiated early in the project life cycle and are maintained throughout the life of the project.

Since the SQAP and SDP are overall quality and software engineering plans, some quality activities, such as software configuration management, risk management, problem reporting and corrective actions, and verification and validation, including software reviews and testing, may be further detailed in separate documents.

Software project management and quality planning activities do not end with the generation of plans. The success of this work activity is measured by how well the tasks are performed, how well the tasks are tracked and monitored for proper implementation and completeness, and how effective the software-related project management and quality planning activities interface with other system-related activities. In most instances, software can not be isolated from the system. The software project management and quality planning activity is the linkage to the system level activities.

The ASME NQA-1-2000, standard specifies that software project management and quality planning include all significant tasks associated with software development and procurement, including procurement of services, estimate of the duration of the tasks, resources allocated to the task, and any dependencies. The software project management and quality planning tasks may require additions or subtasks to be included and tracked to completion as the project progresses and more detailed information is available. A work breakdown structure can provide the flexibility to include additional detail as the project progresses.

In addition to ASME NQA-1-2000, several consensus standards and industry publications identify the importance of software project management and quality planning. These standards offer more detailed information regarding the software development and procurement tasks. As such, they are good resources to assist in the identification and description of the software development and procurement tasks. Some of these standards and publications are listed in the References section below.

Equally, if not more important than the documents mentioned, is developing and maintaining open communications between the SQA lead, the software project manager and the system project or program manager. Open dialogue that establishes joint expectations of those involved and minimizes unexpected issues is critical to a successful software project. The inclusion of DOE headquarters and site personnel will help establish contractor oversight expectations, again minimizing the amount of unanticipated activities. *Contact: debra.sparkman@eh.doe.gov*

References and Additional Resources

1. ASME NQA-1-2000, *Quality Assurance Program for Nuclear Facilities,* American Society of Mechanical Engineers, 2001
2. Institute of Electrical and Electronic Engineers (IEEE), Std 1058-1998, *IEEE Standard for Software Project Management Plans*, IEEE, 1998.
3. Institute of Electrical and Electronic Engineers (IEEE), Std 730-2002, *IEEE Standard for Software Quality Assurance Plans*, IEEE, 2002.
4. Christensen, Mark J., and Richard H. Thayer, *The Project Manager's Guide to Software Engineering's Best Practices,* Institute of Electrical and Electronics Engineers (IEEE) Computer Society Press, 2001.
5. Pressman, Roger S., *Software Engineering: A Practitioner's Approach,* McGraw Hill, 1992.

"Lessons Learned"... *(Continued from page 2)*

Organizational responsibilities for software problem reporting and corrective action for errors and failures should be clearly identified and implemented through well documented procedures. Completion of corrective action should be documented and reviewed periodically. Without such practices, problem recurrence may not be prevented and lessons from the errors may not be learned. Contractual specifications should require software vendors to notify DOE contractors of newly found errors in the codes.

Observations: Many sites resolve their software errors and corrective action process at a project level and maintain informal coordination with vendors or other affected entities.

- ***Software quality assurance (SQA) program and procedures should be rigorously implemented.***

The SQA program encompasses all the procedures and requirements that are essential to ensure quality of the software product and its life cycle maintenance. A Clear, appropriate, and well documented program and procedures, coupled with qualified and trained personnel and a self-assessment program are the foundation for establishing and maintaining the software quality.

Observations: Site assessments revealed inconsistencies in the requirements contained in the SQA program and procedures and their implementation. Many sites rely on individual expertise and their personal effort and put less importance on the corporate SQA program.

- ***Appropriate qualifications and training on software use is essential for proper use of safety software.***

Software developers and users should have requisite qualifications and be trained in SQA procedures and requirements. Software developers and users should have a thorough understanding of the technology used in the software and should be knowledgeable in software quality assurance, verification and validation, configuration management, and error reporting and corrective action. The qualification and training requirements need to be documented in SQA procedures and an approved user/developer list maintained. Through personnel training the SQA culture needs to be developed for a successful SQA program.

Observations: SQA assessments indicate that very sophisticated and complex software is sometimes used without appropriate training.

- ***Appropriate software control and configuration management is essential for safe use of the software.***

Safety software should be controlled at all times both in terms of its version, distribution, residence and access. An inventory of safety software should be maintained. Configuration management is needed to control utility or calculational type software, such as Excel or Mathcad.

Observations: Lack of proper control had resulted in multiple versions being available at the same time and even some with known errors. Assessments have noted deficiencies with configuration control in terms of software version and documentation.

Contact Subir Sen (301) 903-6571, subir.sen@eh.doe.gov.

DID YOU KNOW?

Did you know that a design constraint limits the choices that software developers have when implementing a software system? Frequently, design constraints are confused with requirements. It is important to distinguish the difference since in most instances a design constraint may be removed without impacting the functional, performance, or other customer requirements. Examples of design constraints include requiring the use of a particular programming language such as ADA or C, requiring the software system be deployed on the Microsoft Windows XP platform, and requiring Oracle as the underlying database management system. Since design constraints limit the software implementation options, they should be thoroughly investigated to ensure the limitations that are imposed on the software system are necessary. Often, decisions made regarding the design, such as choosing a programming language, are made too early and become design constraints that inappropriately limit the software developer's ability to choose a different programming language that would better meet the project's schedule, development and operational costs, and long-term maintenance.

"In the Spotlight"… *(Continued from page 1)*

for approving deviations and waivers of operational and nuclear safety requirements, and providing input on nuclear safety policy in conjunction with the Office of Environment, Safety and Health. I also maintain a forcing function when necessary to ensure nuclear safety requirements are being appropriately addressed. There is a great deal of work needed to strengthen DOE's technical oversight activities and I look forward to supporting the line in achieving better project management and a more systematic approach to our activities.

Q: Within your office, do you foresee taking an active role in Quality Assurance (QA) and Software Quality Assurance (SQA) in light of the recently issued DOE O 414.1C?

***A*: "**Yes. The CTA for ESE will be promoting consistency in Quality Assurance Programs (QAPs) and participating in field reviews of QAPs and making sure that there is an appropriate balance between QA and Integrated Safety Management (ISM). The CENS staff will also be reviewing and concurring in the ESE Headquarter QAPs as outlined in the Department's Implementation Plan for DNFSB Recommendation 2004-1. The proposed staffing for my organization reflects significant attention to QA and SQA. This is a direct reflection of where I perceive additional work is needed, particularly in QA. SQA is another area that requires attention for some of our waste processing activities."

Q: What do you see as the biggest challenges facing DOE in the implementation of DOE O 414.1C?

A: "The biggest challenge for DOE in reference to the DOE O 414.1C is implementing the SQA requirements. Implementing SQA requires multiple technical disciplines to be involved and does not lend itself to traditional QA practices. Sites that have had software problems understand this issue; therefore, it will be important to share the lessons learned. DOE needs to continue with the field assessments of SQA and to maintain a thorough understanding of how the contractors are implementing SQA requirements in the field."

Q: In your previous job as Director, Office of Quality Assurance Programs you were responsible for much of the day-to-day implementation of the commitments in the DOE 2002-1 Implementation Plan for SQA. What benefits to DOE do you see as a result of these activities and specifically DOE O 414.1C?

A: "There are several benefits of DOE O 414.1C: 1) Federal Employees with responsibility for overseeing SQA activities at nuclear facilities have been trained and qualified; 2) there is now an understanding of the impacts of SQA, knowing that we can't afford NOT to do SQA; 3) there is a greater confidence and understanding of safety analysis reports and the safety software that support them; 4) there is a greater appreciation of why and how to build SQA into the process upfront, rather than trying to back fit it into a system or piece of software."

Q: Recently the Office of the Deputy Secretary sent out a memo regarding reinvigorating ISM (Integrated Safety Management). What role will your office play in this 2004-1 Implementation Plan commitment?

A: "Right now in DOE, we have a senior management team that is very interested in correcting problems and managing DOE as a corporate entity. It is a very exciting time. The Under Secretary has established an office of dedicated federal staff to support corporate management of the Energy, Science and Environment portfolio. He has also directed the reestablishment of the Field Management Council that has already begun to work on some of the most difficult departmental problems.

"Reinvigorating ISM is one of the challenges we face. As one of the ISM Champions, I am responsible for working with the line programs in the development of ISM systems, ensuring that this is reflected in the QAPs, and establishing consistent methods to ensure Headquarters' awareness of field activities. Many sites have existing ISM systems that are working. The goal is to ensure that Headquarters understands them and does an appropriate amount of oversight that is commensurate with the risk involved.

"There are three levels in the DOE Oversight Model; Headquarters, Field Elements and Contractors. (*see Diagram 2*) Each level has a beneficial role to play and we are going to further define these roles to develop a systematic approach to implementing ISM."

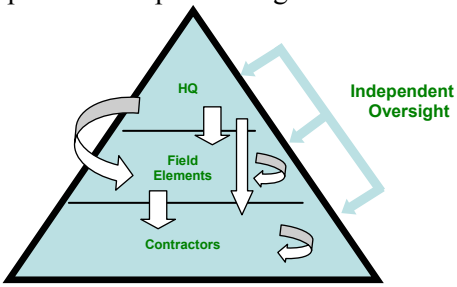


Diagram 2 **DOE Oversight Model**

"DOE Order Rollout…" *(Continued from page 1)*

ing: the revised definition for safety software, the use of ASME (American Society of Mechanical Engineers) NQA-1-2000 supplemented by other consensus standards, applying a graded approach to implementing the 10 SQA (Software Quality Assurance) work activities, and responding to frequently asked questions (FAQs) addressing field implementation.

Russell Shearer, Principle Deputy Assistant Secretary Office for Environment, Safety and Health, and Frank Russo, Deputy Assistant Secretary, for Corporate Performance Assessment (EH-3) emphasized DOE's commitment to quality and DOE's expectations for an integrated ISM and QA program. Chip Lagdon, Acting Chief of Nuclear Safety, Energy, Safety and Environment presented lessons learned from site experiences related to safety systems. Representatives of DOE Program Secretarial Offices discussed their expectations, current and future activities for the implementation of DOE O 414.1C, and the new safety software requirements.

After the conference, a short reception was held in the DOE Forrestal Building where Frank Russo, gave special thanks and presented Award Certificates to the DOE G 414.1-2A and DOE G 414.1-4 writing teams.

Upcoming activities to continue the Order rollout will involve presentations at industry standards committee meetings, regional training sessions, and responding to requests for site visits. The Quality Assurance Exchange newsletter will also be used to provide communication of lessons learned and share information on SQA implementation.

More information on these activities and FAQs is available on the QA and SQA Web Sites at
http://www.eh.doe.gov/qa/ and
http://www.eh.doe.gov/sqa/

DOE-wide Suspect/Counterfeit Items Video Conference Conducted

The Office of Corporate Performance Assessment (EH-3) sponsored a Suspect/Counterfeit Items (S/CI) video conference on September 15, 2005. The purpose of the video conference was to share new S/CI identification information across the Department and to share S/CI investigation results since the last video conference in 2003.

DOE and contractor employees concerned with quality assurance, procurement, and worker and community safety participated in the two hour video conference. Video conference topics included: General S/CI Program updates; Office of Inspector General Litigation/Investigation resolutions; Procurement Enhancements at Brookhaven; Reporting S/CI through ORPS and Lessons Learned; and Manufacturer Insignias/Grademarks and Foreign Manufacturers.

For further information, please contact:

Rick Green: (301) 903-7709
Rick.Green@eh.doe.gov or
Tom Williams: (301) 903-4859
Thomas.E.Williams@eh.doe.gov

DID YOU KNOW?

Did you know that prior to propagating a corrective action throughout the organization, the effectiveness and applicability of the corrective action should be verified through implementing a pilot? A small pilot that implements the corrective action(s) should be used to "test" the corrective action and ensure that all issues associated with the reason for the corrective action have been addressed.

ANNOUNCEMENTS, UPDATES AND ACTIVITIES

EH Continues DOE Rollout Activities

EH is planning the following activities to continue to assist the DOE and its contractors in their effort to comply with the requirements of DOE O 414.1C:

SQA Regional Orientation Activities

- ASME NQA Committee Meeting
  Oct 10-12, 2005 in San Francisco
- EFCOG ISM Working Group Meeting
  Oct 31-Nov 4, 2005 in Albuquerque
- Southeast Region
  Nov/Dec 2005, location TBD
- Mid-Atlantic Region
  Nov/Dec 2005 in Washington, D.C.
- Northwest Region
  Feb. 2006 in Richland
- Mid-West Region
  March 2006 in Chicago

- ***Continue ongoing communication:***
  - FAQs on SQA Knowledge Portal
  - Online Discussion Forum
  - Articles and information exchanges in this Newsletter

EH is working with the PSOs to define additional site specific needs. Look for additional information on the QA and SQA websites and future issues of this Newsletter.

DOE Organizations are Developing Quality Assurance Programs

Pursuant to the requirements of DOE O 414.1C and in response to DNFSB 2004-1 Recommendations, DOE organizations (EH, EM, SC, NE, and NA) are developing their respective HQ Quality Assurance Programs. Some of these QAPs are due to be completed by November 2005. These QAPs are intended to govern DOE HQ activities including oversight responsibilities with primary focus on nuclear safety functions and activities.

New Corrective Action Program Guide for DOE O 414.1C

The new draft guide (DOE G 414.1-5) will be released for review and comment through the Department's directive system. (www.directives.doe.gov)

QA Fundamentals Tutorial Update

An updated version of Quality Assurance training materials will be made available on the QA and SQA websites. Readers are encouraged to review the material and modify it as necessary to fit their specific needs for use in providing basic training on the requirements of the DOE O 414.1C and 10 CFR 830. The material will be available online by October 15, 2005. For additional information, please contact bud.danielson@eh.doe.gov

Standard Updates

NNSA - Y-12 and Kansas City are now registered as compliant with ISO 9001:2000 quality standard. These sites are responsible for overseeing major production facilities of the nation's nuclear weapons complex.

ANS 10.4 - As part of the normal standards maintenance cycle, the American Nuclear Society (ANS) has established a working group to update the ANS 10.4, *Criteria for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry*. The updated standard will be enhanced to include a more global SQA standard to address high integrity software. The working group held its second meeting September 14-15, 2005, in San Francisco. The next working group meeting is planned for mid-November 2005, in Washington, D.C.

ASME NQA-1 - The ASME NQA Committee is actively working on the next version of NQA-1. Hot issues include resolving open issues to gain full endorsement of the standard by the NRC for commercial nuclear power plants (10 CFR 50 Appendix B). NQA has also just published a two-part paper and tutorial (free to the public) on the continuing evolution of nuclear QA principles, practices, and requirements. For more information visit www.ASME.org.

On Going Activities

EH is currently analyzing the following issues regarding Quality Assurance:

- ***Welding***
  Contact: charlie.thayer@eh.doe.gov
- ***Respirator Events Analysis***
  Contact: bud.danielson@eh.doe.gov

U.S. Department of Energy, Office of Corporate Performance Assessment
Office of Quality Assurance Programs (EH-31)
Washington, D.C.

QA Contact:
Bud Danielson
Phone:
(301)-903-2954
E-mail: bud.danielson@eh.doe.gov

SQA Contact:
Debra Sparkman
Phone:
(301)-903-6888
E-mail: debra.sparkman@eh.doe.gov

EDITORIAL NOTE:

DOE QA and SQA Newsletters Combined

To date, the *Quality Assurance Exchange* newsletter and the *Software Quality Assurance* newsletter were published separately. Starting with this issue, the *Quality Assurance Exchange* will cover both QA and SQA related issues. Combining these two newsletters is expected to provide a more efficient and focused forum. All readers are again encouraged to contribute articles on all QA related issues to this newsletter.

We're on the Web!

See us at:

www.eh.doe.gov/QA
www.eh.doe.gov/SQA

UPCOMING MEETINGS & WORKSHOPS

DOE Briefs DNFSB on QA and SQA

The next DOE briefing to the DNFSB is scheduled for ***September 26, 2005.*** The briefing will cover both QA and SQA. Presentations by EH, EM, and NNSA will include key accomplishments as well as ongoing and planned activities.

MELCOR User Workshop

When: September 26-30
Where: Albuquerque, New Mexico
Topic: MELCOR Version 1.8.6
http://melcor.sandia.gov

ASME Nuclear Quality Assurance Committee

When: October 10-12, 2005
Where: San Francisco, CA
Topic: NQA-1-XXXX Revision, Special sessions on NQA –1 for

- DOE Safety Software
- Next generation nuclear reactor task group
- NRC endorsement task group

Note: visitors welcome. This meeting also serves as SQA regional orientation
For more Information: www.ASME.org

NWC Software Quality Assurance Committee

When: October 25-27, 2005
Where: Aiken, S.C.
Information: www.lanl.gov/sqas

EFCOG ISM Working Group Semi-Annual Meeting

When: October 31-November 4, 2005
Where: Albuquerque, NM
For more information: http://www.efcog.org/wg/ism/index.htm

ANS Winter Meeting

When: November 13-17, 2005
Where: Omni Shoreham Hotel, Washington, D.C.
Information: www.ans.org/meeting/winter

Newsletter Articles Needed

The *Quality Assurance Exchange* is intended to be a forum for the exchange of ideas and the sharing of experience among DOE field offices, contractors, and DOE headquarters in the effort to meet quality assurance requirements. Readers are strongly encouraged to contribute articles on the implementation of QA requirements, on lessons learned and to offer suggestions. Please forward your input to: *bud.danielson@eh.doe.gov*