

## Enclosure

### Defense Nuclear Facilities Safety Board Fourth Public Meeting Questions on Safety-in-Design

#### *Meeting Objectives:*

- (1) Review the Department of Energy's (DOE) and National Nuclear Security Administration's (NNSA) ongoing efforts to integrate safety earlier into the design process;*
- (2) Review implementation of DOE's and NNSA's policies related to the integration of safety earlier into the design process;*
- (3) Review DOE and NNSA current practices regarding the identification, management, and timely resolution of safety-related design issues; and*
- (4) Review the efficacy of actions described in the July 19, 2007, Joint Report to Congress, to improve the timeliness of identification and resolution of technical issues raised by the Defense Nuclear Facilities Safety Board (Board).*

#### *This includes:*

- Implementation of DOE Order 413.3A, Program and Project Management for the Acquisition of Capital Assets, guidance documents supporting DOE Order 413.3A, and DOE-STD-1189, Integration of Safety into the Design Process;*
- Establishment of headquarters and field office level policies and practices associated with the integration of safety into the design process;*
- Training of key personnel to implement policies and practices associated with the integration of safety into the design process; and*
- Implementation of the actions described in the July 19, 2007, Joint Report to Congress, to improve the timeliness of identification and resolution of technical issues raised by the Board.*

I. Objective: (Note: These questions apply separately to NNSA and DOE's Office of Environmental Management (EM)). Discuss the actions taken or being considered by NNSA/EM to fully implement DOE Order 413.3A and DOE-STD-1189 within your respective organizations.

A. What is the status of implementation for DOE Order 413.3A and DOE-STD-1189 within NNSA/EM?

1. What NNSA/EM direction was provided to facilitate implementation of these directives?

2. What organization(s) within NNSA/EM, at the headquarters level, is (are) responsible for implementation of these directives? Describe each organization's responsibilities.

a) Are Technical Independent Project Reviews completed consistent with the expectations in DOE-STD-1189?

(1) If yes, how was this determined?

(2) If not, when will Technical Independent Project Reviews be conducted consistent with DOE-STD-1189?

b) What actions are being taken to ensure the federal staff assigned as nuclear safety and design experts on Integrated Project Teams are properly qualified?

c) What is the involvement of federal staff in project technical reviews? For a hazard category 2 nuclear facility, describe the expected level of involvement for the nuclear safety expert during project technical reviews, e.g., personally reviews and provides comments on all safety-related documentation regarding adequacy of technical content, limits involvement to supervision of contractor personnel, etc.

3. What field elements are responsible for implementation of these directives? Describe all roles and responsibilities.

4. What resources, including staff, are or were devoted to implementing these directives?

a) Did NNSA/EM perform a staffing capability and capacity assessment to determine whether DOE Order 413.3A and DOE-STD-1189 can be implemented as intended?

b) Describe the results of any assessment(s).

5. What resource shortages, if any, have hampered implementation of these directives? What was done to address resource shortages?

6. What role does the Chief, Defense Nuclear Safety (CDNS)/Chief, Nuclear Safety (CNS) play in the implementation of these directives?

a) Is the CDNS/CNS performing the duties required by DOE Order 413.3A, and DOE-STD-1189 related to safety in design?

b) How was this determined?

c) Describe the procedures in place to ensure that the required duties are performed. Provide examples of reviews or other activities performed by the CDNS/CNS to meet the requirements of DOE Order 413.3A and DOE-STD-1189.

7. Have DOE Order 413.3A and DOE-STD-1189 been incorporated into existing contracts? If not, which contracts remain to be modified and when will this occur?

8. During implementation at the field office and project levels, were the directives tailored? Describe how tailoring of requirements was accomplished and how it has been documented.

a) What limits, if any, were placed on tailoring safety-related requirements at the field office level? At the project level?

b) If tailoring was allowed, what was done to ensure that the objectives outlined in the Deputy Secretary's memorandum of December 5, 2005, and discussed in subsequent testimony before this Board have not been compromised?

B. Were supplemental NNSA/EM headquarters or field element policies developed to facilitate implementation of DOE Order 413.3A and DOE-STD-1189? Describe each policy.

1. If NNSA/EM policies were established to implement or supplement these directives, what was the objective of each policy?

2. If a policy was aimed at improving the early identification, management, and resolution of safety-related issues, what actions were taken at the headquarters, field office, and project levels to implement the policies? If implemented, how effective have the policies been at achieving their objective(s) and how was this measured?

C. DOE Order 413.3A mandates, and DOE-STD-1189 describes a set of deliverables, e.g., Conceptual Safety Design Report, designed to provide decision makers better safety-related information prior to critical decisions. For this objective to be realized, the availability of design detail(s) may be required sooner than has traditionally been the practice within DOE, e.g., completion of geotechnical studies during conceptual design. To meet this objective, what action(s) has NNSA/EM taken or planned to take, to enhance the design development process, particularly during conceptual design, to improve DOE's ability to identify and resolve safety-related issues earlier?

1. How were these actions promulgated?

2. Were changes made to the budgeting process to ensure adequate funding is available to develop design information earlier?
3. If no action has been taken to develop design detail earlier, what is being done at the project level, to identify and resolve safety-related issues earlier in the design process? Provide examples.
4. Which projects fully implemented these directives during conceptual design? Discuss lessons-learned pertaining to achieving greater design detail.
5. During conceptual design, what are the expectations for development of the design (design maturity) for each alternative when several alternatives are being considered?
  - a) Is each alternative developed to the same degree of design maturity before a preferred alternative is selected or is the preferred alternative developed further?
  - b) If multiple design alternatives are being evaluated, how are the expectations described in DOE-STD-1189 regarding design maturity at Critical Decision-1 achieved?
  - c) How has this been promulgated?

D. What issues, if any, have complicated implementation of the safety-related portions of DOE Order 413.3A and DOE-STD-1189? Describe these issues and provide examples?

1. Is the traditional framework for the critical decision process sufficient to support meeting safety-in-design objectives? If so, how?
  - a) Over the past 5-years, how many new defense nuclear facility design projects have rigorously conformed to an unaltered critical decision process as defined in DOE Order 413.3A? Identify these projects.
    - (1) For each of these projects, have significant safety-related issues been identified, subsequent to Critical Decision-1, that resulted in considerable cost and schedule impact(s), e.g., greater than 5 percent of total project cost?
    - (2) For each of these projects, have significant safety-related issues been identified, subsequent to Critical Decision-2, that resulted in considerable cost and schedule impact(s), e.g., greater than 5 percent of total project cost?

- (3) For each of these projects, have significant safety-related issues been identified, subsequent to Critical Decision-3, that resulted in considerable cost and schedule impact(s), e.g., greater than 5 percent of total project cost?
  - b) Over the past 5-years, how many defense nuclear facility design projects have combined critical decisions, or otherwise altered the traditional critical decision process?
    - (1) What were the primary reasons for altering the critical decision process?
    - (2) To what degree have safety-related issues impacted projects where critical decisions were combined or otherwise altered, e.g., did not conform to the traditional critical decision process? If so, when were these issues: (1) identified and (2) resolved, e.g., during conceptual, preliminary, or final design?
- 2. If the critical decision process was altered, was the design process modified, e.g., more detailed design information developed during conceptual design, to mitigate the potential technical risk(s) resulting from combining critical decisions?
  - a) What were the objectives for the design process modifications and how successful was each at meeting its objectives?
  - b) Has NNSA/EM provided guidance on how to appropriately address safety-related requirements from DOE Order 413.3A and DOE-STD-1189, when combining critical decisions? Describe the guidance.
- 3. When the critical decision process has been altered, was the NNSA/EM oversight strategy modified to mitigate potential technical risk(s) resulting from combining of critical decisions?
  - a) Were any special action(s) taken to identify and resolve technical issues early in the design process, e.g., increased use of external technical reviews, technical readiness assessments? What were these actions and how successful was each? How was this measured?
  - b) Were the reviews typically planned for the end of each design stage completed, regardless of combining of critical decisions, e.g., for the case where a combined Critical Decision-2/3 decisions is contemplated, were the safety-related deliverables listed in Table 2, DOE Order 413.3A, applicable at Critical Decision-2, completed prior to commencing final design?

4. What is the current NNSA/EM position regarding combining of critical decisions in view of the desire to identify and resolve safety-related issues earlier in the design process? Describe these positions and provide examples.

a) Given the desire to identify and resolve issues earlier in the design process, why would NNSA/EM allow a large, one-of-a-kind, or complicated hazard category 2 or 3 defense nuclear facility projects to combine critical decisions? Provide examples.

b) Describe the specific actions that a large, one-of-a-kind, or complicated hazard category 2 or 3 defense nuclear facility project, would take to ensure that safety issues are identified and resolved early in the design process, prior combining critical decisions.

c) Has NNSA/EM reviewed projects that combined critical decisions to understand if any issues related to combining critical decisions have common causes or drivers? If so, what changes to the existing budgeting and project management practices would address the issues?

II. Objective: (Note: These questions apply separately to NNSA and EM). Discuss the progress and impact the actions described in the July 19, 2007, Joint Report to Congress, have had on improving the timeliness of identification and resolution of technical issues raised by the Board.

A. What policies has NNSA/EM developed to address unresolved safety issues identify by the Board in response to project letters?

B. What policies has NNSA/EM developed to address unresolved safety issues identified by the Board in Quarterly Reports to Congress?

C. What NNSA/EM headquarters organization(s) are currently responsible for addressing unresolved safety issues identified by the Board in project letters and the Quarterly Reports to Congress?

D. NNSA/EM staff met with Board's staff on a quarterly basis to discuss the status of issues resulting from the Board's reviews of projects. How have these discussions contributed to the resolution of outstanding issues? Provide examples.

E. For projects in the conceptual design stage, DOE committed to implementation of DOE-STD-1189 based on a specific evaluation of each project.

1. For each project in this category, who performed the evaluation, what criteria were utilized, and what were the results?

2. For projects in the conceptual design stage that did not adopt DOE-STD-1189, except for the format and content guidance related to preparation of safety documentation, why was it deemed adequate to continue using existing design and project management practices, given the objectives outlined in the Deputy Secretary's memorandum of December 5, 2005, and discussed in subsequent testimony before this Board? Provide a response for each instance.

F. What lessons-learned were developed regarding implementation of DOE Order 413.3A and DOE-STD-1189 requirements for the demonstration projects identified in the July 19, 2007, Joint Report to Congress?

1. How were lessons-learned communicated to other elements within NNSA/EM?

2. How were lessons-learned communicated to ongoing design and construction projects?

3. How were lessons-learned reflected in the decision(s) to adopt or not to adopt DOE-STD-1189 for ongoing projects? Provide examples.

III. Office of Management (MA)/Office of Engineering and Construction Management (OECM). Objective: Discuss the implementation of DOE Order 413.3A and related guidance documents.

A. What mechanism(s) has OECM utilized to measure successful implementation of DOE Order 413.3A across the complex? Discuss the results.

B. Is DOE Order 413.3A, sufficiently well implemented within DOE to meet the objectives outlined in the Deputy Secretary's memorandum of December 5, 2005, and discussed in subsequent testimony before this Board?

C. If DOE Order 413.3A has not been fully implemented, what are the impediments to full implementation?

1. What specific action has OECM taken to ensure implementation of the safety-related portions of DOE Order 413.3A?

2. What is the schedule for these actions?

D. What safety-related portions of DOE Order 413.3A, will likely be revised during the anticipated revision of this Order? Describe these changes, including the basis for each change and any drivers?

1. Did any of the likely safety-related changes result from lessons-learned at the demonstration projects identified in the July 19, 2007, Joint Report to Congress?

2. Describe the reason for these changes.

E. Are potential change(s) in the critical decision process, as currently described in DOE Order 413.3A, being contemplated by OECM to aid in early identification and resolution of safety-related issues? Describe these changes.

F. To what degree are the current OECM policies and practices consistent with the recently completed guides supporting DOE Order 413.3A, e.g., conduct of reviews sponsored by OECM for ongoing projects?

G. In July 2008, DOE issued a Corrective Action Plan (CAP) to address issues discovered from a root cause analysis (RCA) for problems with contract and project management.

1. What problems noted in the RCA impact safety-related design aspects of defense nuclear facilities? Describe these problems.

2. What actions described in the CAP were also described in the July 19, 2007, Joint Report to Congress? Describe these actions.

3. What actions are being taken, beyond what is described in the July 19, 2007, Joint Report to Congress, to address problems from the RCA that may adversely impact safety during the design of defense nuclear facilities? Describe these actions and their schedules.

4. What is the urgency being given to resolving issues identified in the RCA? Provide examples and discuss the specific resources being applied.

5. Given the effort to address safety-related issues with design and construction, how has the current schedule identified in the CAP been justified? Provide examples.

H. MA-1 is currently developing a major revision to DOE Order 251.1B, *Departmental Directives Program*. MA-1 has indicated that one explicit driver for this revision is that DOE Order 413.3A has been cited by DOE's Laboratory Directors as being overly burdensome.

1. Describe in what areas DOE Order 413.3A is considered overly burdensome.

2. What actions, if any, are being taken or planned to address these burdens.



3. How are these actions being integrated with the anticipated effort to revise DOE Order 413.3A?

I. How will MA-1's planned changes to DOE Order 251.1 impact DOE Order 413.3A and its supporting guidance documents, including DOE-STD-1189?

IV. Office of Health, Safety and Security (HSS). Objective: Discuss the implementation of DOE-STD-1189.

A. From an HSS perspective has DOE-STD-1189 been fully implemented within NNSA/EM? How was this measured?

B. If DOE-STD-1189 has not been fully implemented, what work remains for HSS to achieve full implementation? How was this determined?

C. What has HSS done to identify and train key personnel to effectively use DOE-STD-1189?

1. How were key NNSA/EM personnel identified?

2. How were key contractor personnel identified?

3. How were the training requirements for key personnel determined?

4. What were the training objectives for key personnel?

5. Were these training objectives met and how was this measured?

6. What work remains to fully train key personnel to effectively use DOE-STD-1189?

7. When will the initial training be completed?

8. What ongoing training requirements will be established to ensure new NNSA/EM and contractor personnel are adequately trained?

9. How will the training be institutionalized?

D. What has been accomplished to address the concerns raised in the Board's letter dated February 22, 2008?

a) What progress has been made in revising the DOE Orders and Standards needed to implement DOE-STD-1189? Is this progress consistent with the schedule outlined in the HSS memorandum dated May 8, 2008?

(1) Were all the DOE directives needed to fully implement DOE's objectives, with respect to the integration of safety into design, identified in the HSS memorandum dated May 8, 2008?

(2) In their current form, are the directives needed to fully integrate safety into design consistent and void of redundant or conflicting requirements?

(3) If not, what is the potential that the presence of redundant or conflicting requirements will result in other problems, e.g., prevent full implementation of DOE's integration of safety into design objectives?

(4) If the current set of directives needed to integrate safety into design has not been incorporated into existing design related contracts, what are the weaknesses resulting from using out-of-date directives?

(a) How has DOE compensated for these weaknesses?

(b) What are the potential long term impacts, if any, from having a less than complete set of directives for ongoing projects, particularly for technically complex projects or those with long design and construction schedules that are currently in the earliest stages of design?

(5) Are the resources devoted to the revision of key DOE directives sufficient to ensure timely completion?

(6) What shortfalls, if any, exist with respect to the availability of the technical expertise needed to support revision of safety-related directives? Describe these shortfalls.

(7) Are these resource shortfalls sufficient to delay completion of key DOE directives?

b) What progress has been made towards developing criteria to ensure safety-related systems protecting the facility worker and addressing chemical hazards are designed with the requisite reliability? Describe these criteria.

(1) What directives will be modified to contain these new criteria?

(2) When will this be accomplished?

c) What projects are voluntarily using Appendices B and C from DOE-STD-1189? Identify each project.

(1) Is the guidance from these appendices being treated as requirements?

(a) If being used, has the guidance been tailored for project application?

(b) Did tailoring result in a technically defensible set of design criteria, e.g., adequate to protect the facility worker and to address chemical hazards? How was this determined?

(2) If projects have not adopted Appendices B and C from DOE-STD-1189, what are the criteria used to classify safety-related systems and components needed for the protection of the facility worker and to address chemical hazards?

(3) Are the design criteria applied to these systems and components sufficient to meet the reliability related objectives outlined in the Board's letter of February 22, 2008?