U.S. Department of Energy Office of Safety and Emergency Management Evaluations Criteria and Review Approach Document	Subject: Review of Documented Safety Analysis Development for the Hanford Site Waste Treatment and Immobilization Plant (LBL Facilities) – Criteria and Review Approach Document Acting Director, Office of Safety and Emergency Management Evaluations Date: April 23, 2013 Lead, James Low Date: April 23, 2013	HS: HSS CRAD 45-58 Rev: 0 Eff. Date: April 23, 2013

1.0 PURPOSE

Within the Office of Health, Safety and Security (HSS), the Office of Enforcement and Oversight, Office of Safety and Emergency Management Evaluations (HS-45) mission is to assess the effectiveness of the environment, safety, health, and emergency management systems and practices used by line and contractor organizations in implementing Integrated Safety Management; and to provide clear, concise, and independent evaluations of performance in protecting our workers, the public, and the environment from the hazards associated with Department of Energy (DOE) activities and sites.

In addition to the general independent oversight requirements specified in DOE O 227.1, *Independent Oversight Program*, Section 11.h of Appendix B to DOE O 413.3B, *Program and Project Management for the Acquisition of Capital Assets,* assigns responsibility to the Office of Health, Safety and Security to perform targeted reviews of technical processes and products associated with the design and construction of nuclear facilities.

A key to success is the rigor and comprehensiveness of our process; and, as with any process, we continually strive to improve and provide additional value and insight to field operations. Integral to this is our commitment to enhance our program. We continue to make Criteria and Review Approach Documents (CRADs) available for use by DOE line and contractor assessment personnel in developing and implementing effective DOE oversight, contractor self-assessment, and corrective action processes; the current revision of each CRAD is available at http://www.hss.doe.gov/indepoversight/safety_emergencymgt/guidance.html.

2.0 APPLICABILITY

The following Criteria and Review Approach Document is approved for use by the Office of Safety and Emergency Management Evaluations.

3.0 FEEDBACK

Comments and suggestions for improvements on the Criteria and Review Approach Document can be directed to the Acting Director of the Office of Safety and Emergency Management Evaluations on (301) 903-5392.

Review of Documented Safety Analysis Development for the Hanford Site Waste Treatment and Immobilization Plant (LBL Facilities)

OBJECTIVES AND SCOPE

The review will consider selected aspects of the development of the Documented Safety Analysis (DSA) for the Waste Treatment and Immobilization Plant (WTP); Low Activity Waste (LAW) facility, Balance of Facilities and Analytical Laboratory (LAB) (collectively identified as LBL) to assess the extent to which nuclear safety is integrated into the design of the LBL facilities in accordance with DOE directives; in particular, DOE Order 420.1B and DOE-STD-3009-94.

The present safety basis for the LBL is the collection of Preliminary Documented Safety Analysis (PDSA) for the specific facilities. These PDSAs were not prepared using a standard safe harbor methodology such as DOE-STD-3009-94. Therefore, to implement DOE-STD-3009, the WTP project is in the process of developing a DSA that is scheduled to be completed and submitted to the DOE Office of River Protection (ORP) in mid-2015. As part of the DOE-STD-3009 implementation, WTP started in fall 2012 performing new hazards analysis for LAW and LAB systems. The PDSA and development of the draft DSA are supported by the WTP Basis of Design documents, design descriptions, process & instrumentation diagrams, structures, systems, and components (SSC) failure modes and effects analysis, accident analyses, consequence studies, and various other design and analysis documents.

The review will focus on a few selected SSCs, such as the LAW melter processing system (LMP), Primary Off-gas Processing System (LOP) and LAW Secondary Off-gas/Vessel Vent Process (LVP) System, and associated supporting/interfacing systems. The review will sample information from the safety basis and supporting documents in the following broad areas, as they relate to the selected systems:

- Hazard identification and evaluation using hazard and operability analysis HAZOP and accident analyses; identification of hazard controls, including safety SSCs, safety management programs (SMP) and specific administrative controls (SACs).
- Translation of hazard controls into safety SSC design and functional requirements and performance criteria, and administrative or programmatic commitments.
- Safety basis development process controls to assure protection of safety basis commitments, safety margins, safety SSC characteristics and assumptions.

The DOE ORP Safety Basis Review Team (SBRT) for the LBL DSA has developed DSA/Technical Safety Requirements (TSR) chapter specific review criteria. The following criteria and review approach will supplement, as appropriate, the SBRT review criteria in certain selected areas.

CRITERIA AND REVIEW APPROACH

1. Hazards and Accident Analyses

Criteria:
Hazards analyses are consistent with the DOE safe harbor methodologies; and they provide systematic and complete results for the selected hazards/accidents, consistent with the current design stage, to facilitate developing controls and their design and functional requirements.

Sample Lines of Inquiry:

- Does the hazards analysis include explicit description or reference to the material at risk (MAR), chemical or radiological, potentially affected in the selected hazard scenarios?
- Does the hazard scenario description appropriately describe the mechanisms that lead to the release of hazardous material?
- Does the hazards analysis describe the effect of postulated events on major facility SSCs that could release energy or radioactive/hazardous material?
- Are the selected hazards/accidents conservatively assigned likelihood and consequence?
- Does the hazards analysis comprehensively identify and address hazards associated with facility processes and work activities, as well as natural phenomena and man-made external hazards?
- Are potential beyond design basis accidents identified and the need for their evaluation considered?
- Is the postulated hazardous material release described with respect to each type of potential receptor: facility worker, collocated worker, and offsite individuals?
- Does the hazards analysis identify preventive and mitigative features/controls for the spectrum of events examined using a proper hierarchy?
- Are the results of hazards evaluation summarized to identify significant defense-in-depth and worker safety features, hazard controls, including safety-significant SSCs, SACs, and key elements of safety management programs?
- Does the selection of hazard controls appropriately follow the principles associated with the hierarchy of controls?
- Does the hazard analysis identify dominant accident scenarios through ranking or an equivalent structure?
- Does the hazards analysis use appropriate parameters to establish and evaluate representative, bounding, and unique accidents?
- Is the accident analysis methodology adequate to conservatively assess dose or exposure at receptor locations representing onsite workers and the public?
- Are all pertinent assumptions (e.g., hazardous material inventory, airborne release fraction, and damage ratio) established as part of consequence determination so that technical basis exists for parameters of interest?
- Are the consequences of postulated accidents appropriately compared with the Evaluation Guideline and evaluated to classify safety SSCs and SACs?

2. Safety SSCs

Criteria:
The bases for the design, functional, and performance requirements of the selected safety SSCs to prevent or mitigate the postulated accidents are adequately defined and described.

Sample Lines of Inquiry:

- Are the safety-class and safety-significant SSCs identified and described consistent with the logic presented in the hazard and accident analyses?

- Is the required functional classification of an SSC (e.g., safety-class or safety-significant) based on a proper assessment of the unmitigated accident consequence?

- Are the general requirements for safety SSCs (e.g., conservative design features, design against single-point failure, environmental qualification, safe failure modes) appropriately specified?

- Are codes and standards appropriately specified and tailored, as necessary, based on functional classification and safety function?

- Are safety functions and the design and functional requirements for safety SSCs defined with clarity, and are they consistent with the bases derived in the hazard and accident analyses? Specifically, for each safety SSC, does the safety basis document:

  - Identify safety functions to be performed or maintained by safety SSCs, consistent with the hazard and accident analyses, in the normal, abnormal, or accident conditions postulated?
  - Identify functional and design requirements (e.g., to address non-ambient environmental stresses, or to withstand seismic and other natural phenomena)?
  - Identify the performance criteria necessary to provide reasonable assurance that SSC functional requirements will be met (e.g., surveillance, maintenance, specific operational response, requisite operator training and qualifications)?
  - Evaluate the safety SSC capabilities to ensure that the performance criteria are satisfied?
  - Identify and designate as safety SSC the support systems on which safety SSCs rely to perform or maintain safety functions?
  - Provide for requiring TSR coverage for safety SSCs/SACs?

- Are the boundaries and interface points of safety SSCs (relevant to their safety function), including the support systems, clearly defined?

- Do system evaluations provide evidence that the safety functions can be performed when called upon?

3. SACs

Criteria:
The SACs are adequate to prevent or mitigate the hazards/accidents for which they were identified; and the safety document satisfactorily provides the rationale and basis for determining the safety SACs and their required functions.

Sample Lines of Inquiry:

- Is there adequate rationale for controlling the identified hazard through an SAC instead of an SSC?
- Are the SACs identified and described consistent with the logic presented in the hazard and accident analyses?
- Are SSCs identified whose failure would result in losing the ability to complete the action required by the SAC.
- Are safety functions for SACs defined with clarity and are they consistent with the bases derived in the hazard and accident analyses?
- Do the functional requirements and evaluations of SAC provisions provide evidence that the required safety functions can be performed when called upon?
- Do the SAC evaluations detail appropriate analysis of human performance factors that affect task performance?
- Are the controls of the SACs relevant to future TSR development clearly defined?

4. Derivation of TSRs

Criteria:
The TSR controls derive from the significant preventive and mitigative features identified in the hazard and accident analyses, and the safety basis document provides sufficient bases for determining that these controls for the safety SSCs, SACs or SMP, as appropriate, will ensure that they perform their required functions.

Sample Lines of Inquiry:

- Are identified candidate TSR controls adequate to preserve the functional and administrative requirements necessary to ensure protection of workers, the public, and the environment, as identified in the hazard and accident analyses?
- Is there sufficient information provided to identify what all the safety limits, limiting control settings, and limiting conditions for operation, will be needed to support the facility TSR documentation?
- Have passive SSCs been designated as design features when appropriate?
- Is there adequate documented explanation for any safety SSCs/SACs or other safety features that will not be provided TSR controls coverage?
- Have the facility operational modes (e.g., startup, operation, shutdown) relevant to derivation of TSRs been adequately defined; for example, such that the status of safety SSCs/SACs can be distinctively defined or that multiple structural segments of the facility considered?
- Have the assumptions requiring TSR coverage and the bases for deriving TSRs been identified and described in the safety basis document?

- Is the logic for the derivation consistent with the logic and assumptions presented in the analyses?

- Are the bases for deriving safety limits, limiting control settings, limiting conditions for operation, surveillance requirements, administrative controls, and specific administrative controls provided and technically accurate?

- Are the facility design aspects necessary to implement the identified surveillance requirements (e.g., instrumentation, equipment access) adequately identified?

5. Safety SSC and Safety Basis Configuration Control

Criteria:

- The key design documents, including SSC design basis and supporting documents, are identified and consolidated to support facility safety basis development and documentation. They are kept current using formal change control and work control processes.

- An adequate, DOE-approved change control process has been implemented and criteria established at nuclear facilities under design and construction to determine the need for DOE approval of changes to facility and procedures.

Sample Lines of Inquiry:

- Is there a formal, controlled list of current safety basis documents, including DOE-approved PDSA? Are valid safety basis documents available at the facility?
- Has the completed design been recorded in design output documents, such as drawings, specifications, test/inspection plans, maintenance requirements, and reports?
- Are design output documents (e.g., calculations, drawings, design specifications, procurement specifications, and computer software) associated with safety SSCs prepared, verified, coordinated, approved, tracked, and controlled within a formal process that ensures maintenance of alignment with the design input parameters and safety basis assumptions and commitments?
- Does the established technical baseline (e.g., drawings, procedures, 3D models, and master equipment list) comprise of approved documents and databases? Are controls to manage changes to the baseline established and implemented?
- Is there a facility-specific list of safety and defense-in-depth SSCs (e.g., a master equipment list) readily available? Is guidance established for surveillance, testing, calibration, and maintenance of these SSCs consistent with applicable requirements and standards?
- Are the system design basis and supporting documents identified and consolidated in documentation consistent with DOE-STD-3024 on system design descriptions?
- When design basis information is not available, does the documentation include system requirements, basis for the system requirements, essential performance criteria, and a description of how the current system configuration satisfies the specified requirements and performance criteria?
- Have technical and administrative design interfaces been identified and methods been established for their control?
- Are design input and functional requirements included in technical task requests, facility/system modifications, and safety component procurements?
- Has an adequate DOE-approved change control process for a facility under design and construction been established to screen design modifications and changes and to identify those requiring DOE approval?

- Do the screenings and evaluations using the DOE-approved change control process reflect adequate implementation?
- Is the screening determination being performed by staff knowledgeable of the safety basis? Are they appropriately trained on the DOE approved change control process?