RL/REG-98-08
Revision 2

Regulatory Unit Position On Selected Hazards Control Strategy Issues

August 14, 1998

Office of Radiological, Nuclear and Process Safety Regulation of TWRS Privatization Contractors

Richland Operations Office
PO Box 550
Richland, WA 99352

Approved: _____

Date: _____

This page intentionally left blank

PREFACE

The Department of Energy's (DOE) Richland Operations Office (RL) issued the *TWRS Privatization Request for Proposal* (RFP) for Hanford Tank Waste Remediation System (TWRS) Privatization in February 1996. Offerors were requested to submit proposals for the initial processing of the tank waste at Hanford. Some of this radioactive waste has been stored in large underground storage tanks at the Hanford Site since 1944. Currently, approximately 56 million gallons of waste containing approximately 240,000 metric tons of processed chemicals and 250 mega-curies of radionuclides are being stored in 177 tanks. These caustic wastes are in the form of liquids, slurries, saltcakes, and sludges. The wastes stored in the tanks are defined as high-level radioactive waste (10 CFR Part 50, Appendix F) and hazardous waste (Resource Conservation and Recovery Act).

Under the privatization concept, DOE will purchase waste treatment services from a contractor-owned, contractor-operated facility under a fixed-price contract. DOE will provide the waste feedstock to be processed but maintain ownership of the waste. The contractor must: a) provide private financing; b) design the equipment and facility; c) apply for and receive required permits and licenses; d) construct the facility and bring it on-line; e) operate the facility to treat the waste according to DOE specifications; and f) deactivate the facility.

The TWRS Privatization Program is divided into two phases, Phase I and Phase II. Phase I is a proof-of-concept/commercial demonstration-scale effort the objectives of which are to a) demonstrate the technical and business viability of using privatized contractors to treat Hanford tank waste; b) define and maintain adequate levels of radiological, nuclear, process, and occupational safety; c) maintain environmental protection and compliance; and d) substantially reduce life-cycle costs and time required to treat the tank waste. The Phase I effort consists of two parts: Part A and Part B.

Part A consists of a twenty-month development period to establish appropriate and necessary technical, operational, regulatory, business, and financial elements. This will include identification by the TWRS Privatization Contractors and approval by DOE of appropriate safety standards, formulation by the Contractors and approval by DOE of integrated safety management plans, and preparation by the Contractors and evaluation by DOE of initial safety assessments. Of the twenty-month period, sixteen months will be used by the Contractors to develop the Part-A products and four months will be used by DOE to evaluate the products.

Part B consists of a demonstration period to provide tank waste treatment services by one or more of the TWRS Privatization Contractors who successfully complete Part A. Demonstration will address a range of wastes representative of those in the Hanford tanks. Part B will be 10 to 14 years in duration. Within Part B, wastes will be processed during a 5- to 9-year period and will result in treatment of 6 to 13 percent of the Hanford tank waste.

Phase II will be a full-scale production phase in which the remaining tank waste will be processed on a schedule that will accomplish removal from all single-shelled tanks by the year 2018. The objectives of Phase II are to a) implement the lessons learned from Phase I; and b) process all tank waste into forms suitable for final disposal.

A key element of the TWRS Privatization Contracts is DOE regulation of radiological, nuclear, and process safety through the establishment of a specifically chartered, dedicated Regulatory Unit (RU) at RL. This regulation by the RU is authorized by the document entitled *Policy for Radiological, Nuclear, and Process Safety Regulation of TWRS Privatization Contractors* (referred to as the Policy) and implemented through the document entitled *Memorandum of Agreement for the Execution of Radiological, Nuclear, and Process Safety Regulation of the TWRS Privatization Contractors* (referred to as the MOA). The Policy is signed by the Under Secretary of Energy; the Manager, RL; the Assistant Secretary for Environment, Safety and Health (ASEH); and the Assistant Secretary for Environmental Management (ASEM). The MOA is signed by the Manager, RL; the ASEH; and the ASEM. The nature and characteristics of this regulation are also specified in these documents. The MOA details certain interactions among RL, the ASEH, and the ASEM as well as their respective roles and responsibilities for implementation of this regulation.

The authority of the RU to regulate the TWRS Privatization Contractors is derived solely from the terms of the TWRS Privatization Contracts. Its authority to regulate the Contractors on behalf of DOE is derived from the Policy. The nature and scope of this special regulation (in the sense that it is based on terms of a contract rather than formal regulations) is delineated in the MOA, the TWRS Privatization Contracts, and the four documents (listed below), which are incorporated into the Contracts. This special regulation by the RU in no way replaces any legally established external regulatory authority to regulate in accordance with their duly promulgated regulations nor relieves the Contractors from any obligations to comply with such regulations or to be subject to the enforcement practices contained therein.

The Policy, the MOA, the TWRS Privatization Contracts, and the four documents incorporated in the Contracts define the essential elements of the regulatory program, which will be executed by the RU and to which the TWRS Privatization Contractors must conform. The four documents incorporated in the Contracts (and also incorporated in the MOA) are

> *Concept of the DOE Regulatory Process for Radiological, Nuclear, and Process Safety for TWRS Privatization Contractors*, DOE/RL-96-0005,
>
> *DOE Regulatory Process for Radiological, Nuclear, and Process Safety for TWRS Privatization Contractors*, DOE/RL-96-0003,
>
> *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, DOE/RL-96-0006, and
>
> *Process for Establishing a Set of Radiological, Nuclear, and Process Safety Standards and Requirements for TWRS Privatization*, DOE/RL-96-0004.

In the execution of the regulatory program, the RU will consider not only the relevant approaches and practices of DOE but also those of the Nuclear Regulatory Commission (NRC). The Policy states that

> "It is DOE's policy that TWRS privatized contractor activities be regulated in a manner that assures adequate radiological, nuclear, and process safety by application of regulatory concepts and principles consistent with those of the Nuclear Regulatory Commission."

To this end, the RU will interact with the NRC (under the provisions of a memorandum of understanding with the NRC) during development of regulatory guidance and during execution of the regulatory program to ensure implementation of this policy.

All documents issued by the Office of Radiological, Nuclear, and Process Safety Regulation of TWRS Privatization Contractors are available to the public through the DOE/RL Public Reading Room at the Washington State University, Tri-Cities Campus, 100 Sprout Road, Richland, Washington.

This page intentionally left blank

TABLE OF CONTENTS

REGULATORY UNIT POSITION ON SELECTED HAZARDS CONTROL STRATEGY ISSUES

1.0 PURPOSE

This paper clarifies the RU's expectations for implementation of the required process for establishing safety standards and application of the DOE-stipulated top-level standards and principles. Based upon the Contractors' submittals for Standards Approval and Initial Safety Evaluation, the Regulatory Unit (RU) found that the Contractors had failed to follow the requirements of the Contracts. Specifically, the Contractors made assumptions and identified standards that were not justified based upon the work identification and hazards evaluations contained in their submittals. For example, the Contractors had preemptively distinguished separate hazards control strategies and standards for the worker, co-located worker, and the public without sufficiently precise identification of the work or sound rationale based upon such work identification.

This paper elaborates on the details of the Regulatory Unit's (RU) positions concerning selection of control strategies and standards. The regulatory program referenced in this position paper is the program required by the TWRS Privatization Program Contracts DE-AC06-RL13308 and DE-AC06-RL 13309.

2.0 REQUIREMENTS OF THE REGULATORY PROGRAM

The regulatory program requires the Contractor to follow a structured process to identify a set of subordinate standards that, when properly implemented, will ensure adequate radiological, nuclear, and process safety, compliance with applicable laws and regulations, and conformance to the *Top-Level Radiological, Nuclear, and Process Safety Standards and Principles for TWRS Privatization Contractors*, DOE/RL-96-0006 (*Top Level Standards and Principles*). The required structured process is described in the *Process for Establishing a Set of Radiological, Nuclear, and Process Safety Standards and Requirements for TWRS Privatization*, DOE/RL-96-0004, (*Process for Establishing Standards*).

The top-level standards and principles in DOE/RL-96-0006 are a set of broad statements, independent of the Contractor's waste processing technology, of ways to achieve the expected level of safety for TWRS Privatization. The top-level standards and principles do not provide a blanket waiver to applicable safety regulations, nor do they substitute for the required structured process, rather they are an additional consideration for the identification of standards. The Contractor is required to address and incorporate the top-level standards and principles in the Contractor's set of standards.

3.0 CONSIDERATIONS

The Regulatory Plan[1] states, as one basis for TWRS Privatization planning, that "Regulation would not rely on the DOE Order-based system but would apply the concept of 'tailoring' of controls to the work to be performed and associated hazards, and would be exercised through DOE nuclear safety rules and contract commitments to agreed upon standards." Rather than specifying prescriptive rules, standards, and design approaches, the DOE stipulated that top-level standards and principles are to be satisfied in addition to adherence to applicable Federal and state laws when selecting those standards needed to assure adequate safety based upon the Contractor's specific work identification and hazards evaluation. It is the Contractor's responsibility to recommend the specific set of subordinate standards and requirements applicable to the design, construction, pre-operational testing, operation and deactivation of the Contractor's facilities. The RU reviews and approves the Contractor's recommended set of standards based upon the soundness of the rationale documented in the Contractor's regulatory submittals.

The Contractor's set of standards should address the preparation of safety analyses. Safety analyses of the design should identify and evaluate the hazards and resulting potential accidents arising from the proposed facility design and operations. It is expected that these analyses will be performed using industry-accepted techniques including consideration of design and process uncertainties. These analyses should identify the safety functions, and the relative degree of reliability needed, of structures, systems, and components that are intended to mitigate or prevent accidents. The potential need for redundant and diverse structures, systems and components in those areas of the design susceptible to common-mode or common-cause failures should be identified and evaluated.

The estimated frequency of process or facility system failure is dependent on many factors: e.g., quality of components, operating and maintenance procedures, design features, redundancy, diversity, and physical protection from external and internal events. These impacts on system reliability must be considered, to determine the likelihood of postulated events, when this information is known. Also, the allowable dose consequences of a postulated event are dependent on the affected population (public, worker, or co-located worker), the likelihood of the event, and the cost-benefit of accident prevention or mitigation.

It is expected that there will be features of the design that will be required to be more demanding than others in order to satisfy those top-level standards and principles specifically applicable to the worker, co-located worker, public, and the environment. For example, it is important that confinement systems be designed to fully satisfy the Radiation Protection Objective[2] and the Defense in Depth Principle[3] for all affected populations.

It would be shortsighted for the vitrification plant(s) to rely on the area between the Hanford site boundary and the plant boundary as a location for airborne contamination to fall out from the vitrification plant. Such a design approach overlooks the larger goals of DOE to maintain public acceptance of Hanford, and eventually return large portions of the site to the public for unrestricted use. The vitrification plant(s) should be designed and operated consistent with DOE planning to remediate the site. The Radiation Protection Objective includes mitigation of the extent of environmental impact due to accidents. The Mitigation Principle[4] states that the facility should be designed to retain radioactive material. Consistent with both this objective and principle, control strategies that mitigate the consequences of releases of hazardous material by retention are to be preferred over control strategies that mitigate by dispersion.

The RU recognizes that development of performance requirements that will determine reliability of systems,

[1] *Radiological, Nuclear, and Process Safety Regulation of TWRS Privatization Contractors REGULATORY PLAN*, RL/REG-97-10, Revision 1, 1/7/98.

[2] DOE/RL-96-0006, Section 3.2
[3] DOE/RL-96-0006, Section 4.1.1.1
[4] DOE/RL-96-0006, Section 4.1.1.4

structures and components that are important to safety will occur iteratively. However, mitigation should not be initially assumed in estimating potential event consequences. Failure to consider higher consequence events at an early stage of design, based on unsubstantiated assumptions of low probability is inappropriate. Unmitigated consequences of a wide spectrum of possible events, including common-cause and common-mode failures, should be considered when assessing the need for preventive and mitigative features in the design. Notwithstanding the need for consideration of unmitigated consequences, assumptions, estimated consequences, preventive and mitigative features based upon previous similar designs may be used, and should be used, provided the rationale for the previous design and its applicability to TWRS Privatization is made clear in the regulatory submittals.

The top-level radiological safety objectives establish goals for allowable risk for the facility. These goals, if accomplished, should ensure protection of public and worker health and safety. "The Contractor should use these objectives to determine 1) the effectiveness in achieving the expected level of safety and 2) the need for additional measures[5]." Consequence analyses should be confirmatory, and should not be the primary basis of the design.

Standards should be selected that provide safety design criteria for systems that are important to safety. However, the application of these standards should be tailored commensurate with work identification and hazards evaluation. Design standards should be based on the performance requirements of the system, rather than on an arbitrary pre-selection of design codes assigned to the public, workers, or co-located workers. The design criteria selected should be commensurate with ensuring compliance with applicable laws and regulations, and conformance to the *Top Level Standards and Principles*. Arbitrary application of pre-specified design standards or control strategies without clear rationale connecting the standards to the facility hazards does not defensibly ensure that the standards selected are commensurate with work identification and hazards evaluation.

Certain existing DOE guidance, such as DOE Order 420.1, *Facility Safety*, distinguishes between the design requirements applicable to the public, on one hand, and those required for the worker or for defense in depth, on the other. NRC guidance makes different, but still predetermined distinctions, and does not recognize the specific distinction of a co-located worker population. Importantly, such conventions are not adopted in the TWRS-P Contracts. Therefore, the rationale for distinctions in standards selected by the Contractors based on specific populations must be documented in regulatory submittals. There is no *a priori* reason for assuming that different codes and standards may be applied to different populations without a defensible justification. Rather, control strategies, including design codes, must be chosen commensurate with work identification and hazards evaluation; that is, they must be tailored.

Finally, the use of "pre-selected" standards, that is, standards that are selected without following the required structured process described in the *Process for Establishing Standards*, is not consistent with the integrated safety management approach embedded in the TWRS Privatization Program Contracts. "The tailoring of safety control measures to the specifics of the work and the hazards involved is an important feature built into the Integrated Safety Management concept. As the word tailoring implies, the concept emphasizes the need the fit the safety measures to the specifics of the work. This is an intellectual engineering exercise, not a preconfigured one-size-fits-all method.[6]"

4.0 SUMMARY

1. In accordance with the *Process for Establishing a Set of Radiological, Nuclear, and Process Safety*

[5] DOE/RL-96-0006, Section 3.0.

[6] DNFSB/TECH-16, "Integrated Safety Management," Defense Nuclear Facilities Safety Board Technical Report, June 1997, section 4, page 4-1.

Standards and Requirements for TWRS Privatization, DOE/RL-96-0004, hazards control strategies are to be selected based on work identification and hazards evaluation. Standards are to be selected based on work identification, hazards evaluation, and the hazards control strategies. Distinguishing separate control strategies for the worker, co-located worker, or public populations, must be justified based upon work identification and hazards evaluation. Selection of standards, based upon arbitrarily distinguishing control strategies for particular populations, is not consistent with the requirements of DOE/RL-96-0004.

The process described in DOE/RL-96-0004 relies on an adequate identification of the work. In many instances, the Part A work identification was not precise enough to develop sound rationale for tailoring design requirements to particular populations. Efforts to tailor design requirements to particular populations, without a sufficiently precise identification of the work and resulting sound rationale, are premature. Control strategies (including design requirements) should be tailored commensurate with the work identification and hazards evaluation.

2. Revisions of the set of standards selected must use the process described in DOE/RL-96-0004 iteratively, as work is more precisely identified. In accordance with DOE/RL-96-0004, the standards set must ensure adequate safety, compliance with applicable laws and regulations, and conformance to DOE-stipulated top-level standards and principles. However, the individual top-level standards and principles, e.g., dose standards, should not be used independently for tailoring accident mitigation and prevention features, such as the confinement system, during design. The dose standards should be used to confirm the adequacy of the designs of structures, systems and components, and are not sufficient to comprise the design bases. The design bases should be a combination of functional considerations, conformance to the Radiation Protection Objective, defense in depth, and the other *Top Level Standards and Principles*, and application of the *Process for Establishing Standards*.

3. The bases for assumptions used in hazard assessments, design basis event determinations, categorizations of structures, systems and components that are important to safety, and the selections of standards, should be documented in the regulatory submittals in which they are used. Unsupported or unsubstantiated reliability assumptions should not be used. As the certainty of the design increases over the life of the project, the assumptions should be refined to reflect more precise identification of work. Commitments that are later found to be unnecessary to ensure 1) adequate safety; 2) compliance with applicable laws and regulations; and 3) conformance to DOE-stipulated top-level standards and principles, should be withdrawn or modified as part of the tailoring process. This can be achieved in the PSAR and FSAR submittals or by formal change to the authorization basis using the procedures established in the ISMP.

4. All TWRS-P Contractor facilities should be designed such that they will not add significant contamination to the Hanford site or the surrounding area, during normal or emergency operations (including the design basis events).Consistent with the *Top Level Standards and Principles*, all TWRS-P Contractor facilities should be designed to retain hazardous materials during normal and emergency operations (including design basis accidents) to the extent practical."

5. Ensuring adequate safety based upon the specific work identification and hazards evaluation does not mean a loss or lack of conservatism. Adequacy and conservatism are separate concepts. Adequate safety is achieved by following the process in the Contracts, i.e., complying with applicable laws and regulations, conforming to the *Top Level Standards and Principles*, and adhering to the *Process for Establishing Standards*. Ensuring adequate safety does not mean that "adequate," no more and no less, is the absolute level of safety required. In fact, the top-level principle, "Mitigation," specifically refers to "a conservatively designed confinement system." Conservatism, in and of itself, is not the goal of integrated safety management, but it is consistent with integrated safety management. The degree of conservatism present in the design is a product of the tailored selection of strategies to control each of the hazards identified from the specifics of the work, and is under the control of the system designer. The goal is to tailor safety measures to the work and hazards in a cost-effective manner.

5.0 TERMINOLOGY[7]

Common-Cause Failures

Dependent failures that are caused by a condition external to a system or set of components that make system or multiple component failures more probable than multiple independent failures.

Common-Mode Failures

Dependent failures caused by susceptibilities inherent in certain systems or components that make their failures more probable than multiple independent failures due to those components having the same design or design conditions that would result in the same level of degradation.

Defense in Depth

The fundamental principle underlying the safety technology of the facility centered on several levels of protection including successive barriers preventing the release of radioactive materials to the workplace or environment. Human aspects of defense in depth are considered to protect the integrity of the barriers, such as quality assurance, administrative controls, safety reviews, operating limits, personnel qualification and training, and safety program. Design provisions, including both those for normal facility systems and those for systems important to safety help to: 1) prevent undue challenges to the integrity of the physical barriers; 2) prevent failure of a barrier if it is challenged; 3) where it exists, prevent consequential damage to multiple barriers in series; and 4) mitigate the consequences of accidents. Defense in depth helps to assure that two basic safety functions (controlling the process flow and confining the radioactive material) are preserved and that radioactive materials do not reach the worker, public, or the environment.

Defense in Depth Principle

To compensate for potential human and mechanical failures, a defense-in-depth strategy should be applied to the facility commensurate with the hazards such that assured safety is vested in multiple, independent safety provisions, no one of which is to be relied upon excessively to protect the public, the workers, or the environment. This strategy should be applied to the design and operations of the facility.

[7] With the exception of the last term, “Tailoring,” all terms are from DOE/RL-96-0006.

Important to Safety

Structures, systems, and components that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public. It encompasses the broad class of facility features addressed (not necessarily explicitly) in the top-level radiological, nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation).

This definition includes not only those structures, systems, and components that perform safety functions and traditionally have been classified as safety class, safety-related or safety-grade, but also those that place frequent demands on or adversely affect the performance of safety functions if they fail or malfunction, i.e., support systems, subsystems, or components. Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear, and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of important to safety, i.e., safety-related may be practical. However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems, and components should be considered for inclusion within this definition.

Radiation Protection Objective

Ensure that during normal operation radiation exposure within the facility and radiation exposure and environmental impact due to any release of radioactive material from the facility is kept as low as is reasonably achievable (ALARA) and within prescribed limits, and ensure mitigation of the extent of radiation exposure and environmental impact due to accidents.

Tailoring

Adapting something, such as a safety program, practice, or requirement, within the integrated safety management system to suit the need or purposes of a particular operation/activity, taking into account the type of work and associated hazards.[8]

[8] *Integrated Safety Management System Guide*, DOE G 450.4-1, 11/26/97, Volume 2, Appendix A, p. A-7.