Department of Energy
Germantown, MD 20874-1290

October 13, 1999

Secretary of the Commission
U.S. Nuclear Regulatory Commission
Attention: Rulemakings and Adjudications Staff
Washington, D.C. 20555-0001

Dear Sir/Madam:

In reference to the Comments on Proposed Rule 10 CFR 70: Domestic Licensing of Special Nuclear Material; Possession of a Critical mass of Special Nuclear Material (Federal Register Vol. 64, No. 146, pp. 41338-41357 dated July 30, 1999. The Department of Energy submits the attached comments on the proposed revisions lo 10 CFR 70 in response to a request for public input in the July 30, 1999 Federal Register notice.

Please contact Dr. Jacques Read, of my staff, if you have any questions on this. He can be reached at (301) 903-2535, e-mail: jacques.read@eh.doe.gov.

Sincerely,

Richard L. Black, Director
Office of Nuclear Safety
Policy and Standards

Attachments:

cc:
The Honorable Greta Joy Dicus, Chairman. NRC
The Honorable Nils J. Diaz, Commissioner, NRC
The Honorable Edward McGatligan. Jr., Commissioner, NRC
The Honorable Jeffrey S. Merrifield, Commission, NRC
Dr. William D. Travers. EDO/NRC
Dr. Carl A. Paperiello, NMSS, NRC
Mr. Frank Miragila. EDO, NRC

DOE Comments on Proposed 10CFR 70 Rule Published in the Federal Register July 30, 1999

1. Section 70.4, "Worker" "individual whose assigned duties in the course of employment involve exposure to radiation and/or radioactive material from licensed and unlicensed sources of radiation (i.e., an individual who is subject to an occupational dose as in 10 CFR 20.1003)".

   The following change should be made to the definition provided: ".... from licensed sources of radiation, and radiation from man-made non-regulated sources (e.g., an individual .....). As originally defined, persons who are subject to occupational doses from natural sources of radiation, for example airline pilots and astronauts subject to high cosmic background might be included, whereas workers involved with the manipulations of unlicensed radioactive materials might not be. The proposed change removes this source of confusion.

2. Section 70.11 should be revised to reflect the applicability of the NRC authority over a MOX fuel fabrication facility owned by DOE, pursuant to changes in law last year.

3. Section 70.22 (f) should be coordinated with 70.65. As written, it is not clear whether the requirements are collateral, complementary, or redundant.

4. Section 70.23 (b) should be examined to clarify the need for this requirement in light of similar information being submitted pursuant to 70.65. Irrespective of 70.65, 70.23 (b) appears to be an unnecessary step and should be considered for deletion by NRC. If NRC chooses to retain 70.23 (b), NRC should clarify how the authorization process would be conducted, given that the procedural step has never been exercised to the knowledge of DOE. Furthermore, NRC should identify how the "design basis" authorization is defined, why it is necessary, and how it relates to the ISA.

5. Section 70.61, Performance Requirements:

   This section of the rule sets the dose limits only for high-consequence and intermediate-consequence events with the likelihood of highly unlikely and unlikely and does not set the limits for anticipated occurrences similar to that in 10CFR72, parts 104 and 106. The dose limit for anticipated occurrences is much less than the limits for high-consequence and intermediate-consequence events and the anticipated occurrences, when analyzed unmitigated, could result in doses that potentially exceed the limits for high-consequence and intermediate-consequence events. The NRC should specify the dose limits for potential anticipated occurrences at the nuclear fuel cycle facilities. This part of the rule then will cover the range of likelihood (anticipated, likely, unlikely, and highly unlikely) of potential accidents that could occur at nuclear cycle facilities. This could result in an increase in the number of structures, systems, and components relied on for safety and will impact the design, operation, and licensing of the MOX facility.

   a) Section 70.61(d) is not related to 70.61(b) or 70.61(c) yet the three conditionals are all linked together. Subpart (d) should be segregated from (b) and (c) if (d) is

preserved as an independent entry (as would seem preferable). Otherwise, (d) should be subsumed under (b) and/or (c), and the regulatory basis for criticality prevention should be predicated on the risks and/or consequences of the accidents, rather than the presence of initiator precursor per se. (editorial)

b) Section 70.61(f), Each licensee must establish a controlled area, as defined in section 10 CFR 10.1003, in which the licensee retains the authority to determine all activities, including exclusion or removal of personnel and property from the area. For the purpose of complying with performance requirements of this section, individuals who are not workers, as defined in sec. 70.4 may be permitted to perform ongoing activities (e.g., at a facility not related to the licensed activities) in the controlled area, if the licensee demonstrates compliance with 70.61(f)(1) or (2).

These requirements consider the individuals working in the nearby facilities as public when performing an accident analysis to determine the consequences of the accidents that may occur at the facility. This would result in a more stringent application of safety requirements for the protection of workers (e.g., additional items relied on for safety) at the Mixed Oxide (MOX) Fuel Fabrication Facility (FFF), Pit Disassembly, Conversion Facility, Immobilization Facility, and any other nearby DOE facilities. This also would have a substantial impact on the cost of the MOX facility. The workers in the nearby DOE facilities are protected under DOE Code of Federal Regulations 10 CFR 835, "Occupational Radiation Protection" and DOE Order 5400.5, “Radiation Protection of the Public and the Environment," and potentially by draft 10 CFR 834, "Radiation Protection of Public and the Environment," which are comparable to the protection afforded the workers under NRC 10 CFR 20.

Therefore, the NRC should consider changing Section 70.60(f)(1) to read as follows: Demonstrates and documents, in the integrated safety analysis, that those individuals at the location of their activities do not exceed the performance requirements of paragraphs (b)(1), (b)(3), (b)(4)(ii), (c)(1) and (c)(4)(i) of this section, including the Section 70.60(f)(2) requirement in Section 70.22 (h)(2)(ii)(3). Accordingly, the paragraph could be rewritten as follows: "Each licensee must ensure that a controlled area can be established as defined in Sec 20.1003 in which the licensee has the authority to enable control over all activities.

6. Section 70.62(d) Management Measures. Second sentence: "The measures applied to a particular engineered or administrative control or control system may be commensurate with the reduction of risk attributable to that control and control system."

The management measures.are to be applied to items relied on for safety based on their contribution to a reduction in risk. The failure data for most fuel facility equipment are not well documented. The frequency of failure of equipment is a major factor in determining the reduction of risk. Therefore, the NRC should consider the graded approach to management measures, using risk as one of the factors in applying the management measures to items relied on for safety. Other factors should include consequences, life cycle, and magnitude of hazard involved. Balanced and integrated criteria for determining the appropriate management measures can ensure the safety and integrity of the facility.

7. Section 70.64a(4) Environmental and dynamic effects. The design must provide for adequate protection from environmental conditions and dynamic effects associated with normal operation, maintenance, testing and postulated accidents that could lead to loss of safety functions.

   This requirement is unclear. What does it mean? Is formal Equipment Environmental Qualification Program required similar to that required under 10 CFR 50.49 and Regulatory, Guide 1.89? The NRC should clarify this requirement and should not impose requirements that may not be appropriate or necessary because of the nature of the processes at non-reactor nuclear facilities.

8. Section 70.64(b). Facility and systems design and layout must be based on defense-in-depth practices. The defense-in-depth definition as used in Section 70.64 does not reflect the defense-in-depth design philosophy as defined in WASH-1250, "The Safety of Power Reactor and Related facilities," which outlined three levels of safety concepts in the design of a nuclear Facility. The three levels concern different design considerations in the facility; however, these design considerations intermesh and overlap so that distinctions as to whether certain design features belong to one or the other of these levels are somewhat arbitrary.

   The definition in the rule oversimplifies the concept of defense in depth, to where it loses its basic purpose. For example, Sections 70.64(b)(1) and (2) do not adequately represent the implementation of defense-in-depth philosophy in the design. The selection of engineered controls over administrative controls and features that reduce challenges to items relied on for safety are partially implemented in the concept.

   For non-reactor nuclear facilities, one level of safety by itself may not be sufficient to protect against the release of radioactive materials. However, a combination of any of these levels should provide a sufficient level of protection to the public, workers, and environment. The NRC should reexamine the definition and the application of the defense-in-depth philosophy to be commensurate with the level of hazard and associated consequences and risk. NRC should clarify how defense-in-depth philosophy applies to the regulation of facility types stated in section 70.60.

9. Section 70.65(9). A description of the definitions of likely, unlikely, highly unlikely, and credible as used in the evaluations in the integrated safety analysis.

   The NRC should define the terms likely, unlikely, highly unlikely, and credible in the rule so that there will be one set of definitions applied to all nuclear fuel facilities. This will minimize the interpretation and application of these terms in the integrated safety analysis.

10. Section 70.73 states that a description of changes made to structures, systems, components, etc., should be sent periodically by the licensee to the NRC. The term "periodically" should be defined.

11. On the ISA update summary, the 90 day period appears to be too cumbersome. An annual update (similar to the annual FSAR updates for reactors per 10CFR50.71(e)) should suffice. If the spirit of the regulation is not being met based on experience, the licensee should face enforcement action.

12. A backfit process similar to that in 10 CFR 50.109 or 10 CFR 76.76 should be incorporated into the revisions to Part 70 and should apply to the current proposed changes to the extent they apply to existing facilities.

13. Because DOE facilities do not have the uncertainty of continued corporate sponsorship inherent in commercial facilities, the timeliness and schedule requirements in the decommissioning requirements of § 70.38 should be revised to include separate requirements for DOE facilities.

14. The criticality requirements of § 70.24 should be revised to permit alternate criticality control provisions to be accepted for DOE tacilities without requiring an exemption.

15. As additional DOE facilities are licensed by the NRC under the provisions of Part 70. NRC should ensure that the requirements address the full range of fissionable and fissile materials at these facilities.

Comments on NUREG 1513, Integraled Safety Analysis Guidance Document

Guidance on the quality assurance of the ISA process itself should be supplied.

Comments on NUREG 1520, Standard Review Plan (SRP)

This review focuses on the Integrated Safety Analysis (ISA) Chapter 3 of the SRP, since most of remaining SRP Chapters are dependent on the ISA results. The comments only address Chapter 3, ISA, and Appendix A.

Quantitative and non-quantitative determination of likelihood of accidents:

The quantitative determination of event likelihood is dependent on several factors, such as the equipment failure rate; operator error rate; and surveillance, inspection, maintenance, and testing intervals. These factors must be known to determine the frequency of occurrence of an event. The non-quantitative determination of the likelihood imposes design criteria such as redundancy, independence, concurrency, and assurance measures for reliability and availability of items relied on for safety. The likelihood index, which is a summation of preventive and mitigation controls failures, does not consider the interdependency of these controls, nor does it reflect the actual performance of these controls under the expected operating conditions. For example, the integration of failure rates over a range of potential failures for controls that are independent and the summation of failure rates for dependent controls would be more likely to represent the actual performance and likelihood of failure of these controls.

The criteria are subjective and open to arbitrary interpretation by a reviewer. The risk for potential disagreement on appropriate assigned accident likelihood, duration index, and failure rates is extremely high and could render the results of the integrated safety analysis (ISA) unacceptable. (This could jeopardize the chances of obtaining a facility license and impact the cost and schedule of the project.) See the comment on the SRP risk matrix in our response to Section 70.65 above.

Failure rate of components credited for prevention and mitigation of accidents and reduction of risk and/or likelihood:

The fuel fabrication facilities in the US do not maintain a failure-rate database on their equipment, and failure-rate data for structures, systems, and components for a MOX fuel fabrication facility do not exist. The available failure-rate data in the US are geared more toward the commercial nuclear power industry. In addition, the type of equipment used in reactors is significantly different from that used in the fuel fabrication facilities. The Europeans may maintain failure-rate data on their equipment. However, the use of this data will depend on the basis and quality of the data, e.g., collection and control of the data. The European data may have to be validated under US quality assurance practices.

The use of failure data for specific equipment without consideration of the total systems integration failure (i.e., system interactions, support system failures, etc.) may not reflect the effectiveness of these engineered features in mitigating the risk from the potential hazards. The ISA attempts to implement the performance-based, risk-informed approach but fails to recognize that without comprehensive and valid equipment failure data, the approach cannot be implemented in a meaningful fashion.

Summation of frequencies of all accident sequences:

The two performance safety measures established as part of the Nuclear Regulatory Commission (NRC) Strategic Plan are (1) no inadvertent criticality and (2) no increase in reportable radiation releases. The argument used to justify using the summation of frequencies of all potential accident sequences that could occur at the facility during its service life is not supported by any technical justifications. It is unrealistic to take the 5-year average of reportable radiation exposures, allocate 10% of the average, and divide by the number of currently operating fuel facilities to establish a safety performance goal for the facility. There will be only one mixed oxide (MOX) fuel facility; therefore, the performance safety goal for MOX could be set at a much higher level. For example, the performance safety goal for accidents with immediate consequences at the MOX Fuel Fabrication Facility (FFF) could be 4E-2 and for high consequences could be 1E-2, whereas for low-enriched uranium (LEU) facilities, the goal would be set at 4E-3 and 1E-3, respectively, a factor of 10 lower.

The summation of frequencies of all accidents and comparison of the result to a set of quantitative goals may or may not reflect the actual risk from the facility because these goals are set without sufficient basis or adequate data. The data used to set the safety performance goal numbers are insufficient and statistically insignificant. In addition, the number of operating facilities should not be considered as a significant factor in determining the safety performance goal. The 10% of the average of reportable increase in radiation exposure is an arbitrary number. Why not 15% or 20%? Clarification should be requested to ensure that MOX and LEU facilities are judged on the same scale of risk to the health and safety of the public, workers, and environment.

Risk index evaluation:

The risk index evaluation includes factors such as frequency of the initiating event, duration of vulnerability, and frequency of the preceding system/control failure. In Table 5 of the ISA, a duration index is assigned to the duration of the vulnerable state. For example, a duration index of -2 is assigned for an average failure of a few days and a duration in years of 0.001, and a -5

duration index is assigned for a 5-minutes-average failure and a 1E-5 duration in years. What does a few days mean? Does it mean 2, 4, or 6 days? How does a 5-minute-average failure result in an index of -5?

The bases for duration index numbers appear to be selected arbitrarily. The duration of a control/system failure is important in determining the overall risk index; however, these numbers should be based on credible data and properly factored in the index. The data and the methodology for assigning a duration index number should be referenced, and bases for the assigning of index numbers also should be provided.

ISA process:

The ISA process includes the use of several tables to assess the risk from potential accidents and the acceptability of an item relied on for safety to prevent or mitigate the consequences of an accident. The process steps are complex and very hard to follow. A complex process may not produce results that reflect the conditions analyzed. The ISA process should be tailored to accommodate the complexity and uniqueness of the operation to be analyzed and simple enough that it can be easily understood and applied. A logic diagram or procedure should be included to describe the process better.

Determination of assurance measures for safety controls:

The ISA calls for every item relied on for safety in accident sequence categories 2 or 3 (high and intermediate consequences) to be assigned at least a minimal set of measures to defend against a common mode failure of all controls. In addition, it specifies this minimal set as configuration management, regular auditing, adequate labeling and training, written procedures, surveillance, and corrective and preventive maintenance.

The minimal set of assurance measures for items relied on for safety appears to be selected arbitrarily, and there is no logic or basis to support it. The rule calls for the assurance measures to be selected based on the importance of the item to safety and the level of risk associated with its failure. This could have a substantial impact on the design, construction, testing, operation, and maintenance of the facility.

In summary, the ISA process is too prescriptive. This has made the process very complex and confusing. Continued attention should be given to the process as it evolves. (A clear and well-defined ISA process will minimize the risk to the MOX project.)

Appendix A - Example Procedure

The discussion appearing in this section contains virtually no firm guidance as to how to quantitatively justify category assignments. It does, however, contain logical flaws, and must be rewritten.

In the early days of nuclear power plant regulation, a British authority named Farmer proposed a method of judging the acceptability of risk from accidents. This method involved estimating a consequence measure, such as calculated dose at the site boundary, and a likelihood for the accident yielding that consequence, given in the units of per year. If all identified accidents were given as points on a log-log plot of consequence versus likelihood, then Farmer postulated that

there would be a line or curve on that plot such that if all points had consequences and likelihoods less than the curve, then the overall risk could be accepted. He was shown to be wrong; while providing a possible method of graphically presenting comparative risks, the plot cannot be used to assign acceptable areas of risk.

This "Farmer's curve" cannot be a straight line, because the acceptable risk of an accident does not remain constant as the accident consequences increase -- i.e., higher consequence accidents must be more than proportionally less likely than lower consequence accidents. This is because no measure of consequence is applicable over a broad spectrum of accidents. For example, worker doses of less than 1 Sievert can be acceptable at very much higher probabilities than worker doses over 10 Sievert, since the first consequence is unlikely to be fatal, while the second is likely to be fatal. The risk of death is an additional risk that 10 Sv doses have that is above and beyond ten times the health risk of 1 Sv doses. Similarly, the risk to people off-site from a catastrophe is entirely different from the risk associated with a precautionary evacuation. Mortality and morbidity are two entirely separate hazards, and the acceptable likelihood often deaths is not just simply one tenth that of one death.

The proposed guidance for judging the acceptability of consequences replaces the fallacy of Farmer's curve with that of a histogram.

This view of risk is not new, it was first described by D. Bernoulli in the eighteenth century (the "St. Petersburg Paradox"), and was extensively investigated by L.J. Savage in the decade following the second World War (the "Sure Thing" principle). These principles state that risk management cannot be the acceptance of a likelihood, but of a consequence. If a consequence is too large to be accepted, then the design must reduce its likelihood such that its occurrence can be viewed as virtually impossible. If a consequence is acceptable, then its risk can be managed by control of likelihood.

In practice, this means that unacceptably high consequence accidents must be both prevented and mitigated, i.e., in addition to design features to interrupt accident scenarios leading to the unacceptable consequences, there must be design features to mitigate the consequences to humans sufficient to render them acceptable.