NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: COMMISSIONER DIAZ

SUBJECT: **SECY-02-0057 - UPDATE TO SECY-01-0133, "FOURTH STATUS REPORT ON STUDY OF RISK-INFORMED CHANGES TO THE TECHNICAL REQUIREMENTS OF 10 CFR PART 50 (OPTION 3) AND RECOMMENDATIONS ON RISK-INFORMED CHANGES TO 10 CFR 50.46 (ECCS ACCEPTANCE CRITERIA)"**

Approved xx Disapproved _____ Abstain _____
Subject to the attached comments.
Not Participating _____

COMMENTS:

SIGNATURE

Oct. 30, 02
DATE

Entered on "STARS" Yes xx No ____

COMMISSIONER DIAZ' COMMENTS ON SECY-02-0057 AND THE LOCA

The Commission's vote on SECY-02-0057 is a decision that transcends the regulation of the reliability and availability of core cooling for the management and mitigation of reactor transients and accidents. This decision will reflect on our capability and our commitment to be a risk-informed agency utilizing present regulatory tools, technology and operational safety experience.

The Commission's decision to risk-inform our regulations was based on two simple principles: *if it is not risk-significant, it is not important to safety*; and, *the focus of our regulations and resources will be on the issues more important to safety*. In this regard, the low risk-significant Large Break Loss-of-Coolant-Accident (LBLOCA) is a true anachronism in today's safety construct, consuming resources that should be directed to the more risk-significant issues. The LBLOCA is a very small component of the Loss-of-Coolant-Accident (LOCA) contribution to risk, and the LOCAs are a small contributor to the total risk. Therefore, the LBLOCA is using resources disproportionate to its importance to safety, taking attention and resources from what we know is much more important. The LBLOCA was good in 1970, was so-so in 1978, but it is absurd now as a dominant Light-Water Reactor (LWR) safety criterion; it has been rendered obsolete by improvements in safety performance and analysis. Thus, I support a risk-informed alternative within the definition of a LOCA as a voluntary option for licensees.

Before I vote on the specifics, I will present an overall justification for such a change and, on the way, some recommendations on "how-to". The NRC has been using four major performance goals to direct and measure the agency's achievements: maintain safety, increase effectiveness and efficiency, increase public confidence and reduce unnecessary burden. I am convinced that only three of these goals (safety, effectiveness and efficiency, and unnecessary burden reduction) are "vectors" amenable to regulatory control, and that increasing public confidence should be the result of the good performance of those three, as well as our ability to communicate the performance well. Safety is not determined by public confidence; public confidence should be established and grow from safety performance that is factually established and is well communicated. I also believe that major changes to our regulations need to *improve* safety, not just to maintain safety.

While the decision on this SECY impacts on increasing effectiveness and reducing unnecessary burden, my vote is based on *improving the safety* of the nuclear power plants. Yet, whatever direction is set by the Commission, it will be necessary, indeed indispensable, to properly communicate the supporting safety criteria and performance expectations. A very clear statement of the results of the Commission's decision regarding the ECCS and LOCAs will be needed, presenting the safety case and the benefits of implementation. Thus, I believe that providing rule language now, allowing for a risk-informed alternative to the present LBLOCA requirements that focuses on the appropriate LOCA events and other risk-significant issues will actually improve safety,

demonstrate the Commission's commitment to risk-informed regulation and allow for early public participation. The path towards rulemaking will provide many opportunities for participation by all stakeholders and should be conducive to enhancing public confidence in our stewardship of nuclear safety issues.

There is a significant, although not always well utilized, body of knowledge regarding LOCAs and LBLOCAs. I will start with the regulatory definition of a LOCA. The term LOCA is often used quite loosely, but it is very clearly defined in our regulations as "those postulated accidents that result from the loss of reactor coolant *at a rate in excess of the capability of the reactor coolant make up system from breaks in the reactor coolant pressure boundary*, up to and including a break equivalent in size to the double ended rupture of the largest pipe of the reactor coolant system" (emphasis added).[1] So a loss of reactor coolant is only a LOCA, under NRC regulation, if the cause is a break in the reactor coolant pressure boundary, with the maximum size limited to the largest pipe of the reactor coolant system. Thus, a LOCA is a subset of possible losses of reactor coolant. Furthermore, it is only a full-fledge regulatory LOCA if the loss of coolant *exceeds the capability of the reactor coolant make up system*. Again, the set of possible loss of coolant accidents that are dealt with in regulatory space are narrowed to those losses well beyond the ordinary. The reason for repeating the obvious is to emphasize that the regulatory definition of a LOCA does not include all possible leaks or breaks. Moreover, the original selection of the break size was not based on a well-established analysis, an analysis that is now possible.

I believe that, as a matter of improving safety, the consideration of very low probability Large Break LOCAs should be addressed as severe accident scenarios rather than as the design basis accident. Effectively, the current LBLOCA would not be a design basis accident when utilizing a risk-informed approach. With the alternative definition of the LOCA the really important, risk-significant, accident scenarios would remain within the design basis; in fact, their consideration would be enhanced by a new focus on their risk-importance.

My decision to support a risk-informed alternative definition of a LOCA in the regulatory context is based primarily on several important factors: the data available (or lack thereof), the ability to "learn" from failures or potential failures and take corrective action, the excellent state of current operational safety, and the existing capability of making sound risk-informed decisions that include state-of-the-art Probabilistic Risk Assessments (PRA). Let me address each in turn.

There are many very significant aspects of the data that can be singled out in the existing body of knowledge regarding the occurrence of coolant leaks and their association with

---

[1] 10 CFR Part 50, Appendix A.

LOCAs. The first is the scarcity of actual LOCA data. There are not enough LOCAs to estimate, with confidence, the frequencies of LOCA-type failures from historical data, particularly for medium to large breaks. It is very difficult to predict medium and large break LOCAs from zero occurences. Of course, the lack of data should really be construed as a success story, but it is a curse to analysts seeking to establish failure rates. Thus, all kinds of failure data (cracks, pinholes, leaks or ruptures) are brought in to substitute for actual LOCA data. Much of this failure data can be made useful to provide failure estimates. Piping failures are among the "easiest" -- but not easy -- to estimate since there is at least some reasonable body of knowledge that could be used to predict piping crack growth and potential ruptures. Failures due to human behavior (for example, failure to take corrective action) are much harder to predict. Yet, a Large Break LOCA has not occurred in any nuclear power plant in the world, good plants or bad plants, nada.

Due to the lack of actual data, medium and Large Break LOCA frequencies are very conservatively estimated by calculating the frequency of leaks or through-the-wall cracks that have challenged piping integrity. What about small-break LOCAs? They are about two orders of magnitude more probable. Of course, one very famous "small" LOCA occurred at TMI-2 from the failure of a valve to close, a failure augmented by human error. Indeed, it is in this area where data and PRAs demonstrate the need for regulatory concern. It has been more than 23 years since it has been well known that the LOCA risk is dominated by the small break LOCAs. Therefore, that is where our "attention and resources" should be focused.

Another reason for my decision to support a risk-informed alternative stems from the ability of nuclear regulators, the industry, and the technical infrastructure to learn from and correct actual or potential failures. This is especially true for significant safety-related failures or LOCA-type failures. It is not surprising that these groups have "learned to learn" from failure and lack of failure, and that everyday they should learn more efficiently from errors, because prevention and mitigation, followed by error minimization are fundamental nuclear regulatory and operational safety principles. No other TMI-type LOCA has occurred since the first occurrence, and that is probably to be expected because of the extensive actions taken to prevent another occurrence. Yet, the fact that the system "learns" and "corrects" is significant.

The capability of well-developed industrial systems to "learn" from errors is well documented. I would venture to add that error learning curves are most predictable in industrialized democracies, and that errors - especially those well publicized - are corrected rapidly in order to address the real or perceived risk that society associates with the industrial activity. Errors or failures in nuclear power plants are well publicized. Furthermore, the higher the perception of risk to society from an activity, the quicker and more successful should be the learning process.

The nuclear industry, after a somewhat shaky start --- due mostly to human errors in the design, construction and operation of a complex system new to the marketplace --- learned well after the shock of TMI. When a rare and significant event like the Davis-Besse hole-in-the-head occurs, the industry and the regulator are forced to learn and act quickly. It is highly improbable that another Davis-Besse type failure will occur in the U.S.A. because of the corrective actions that have been and are being taken based on what has been learned. One hole-in-the-head is bad enough. Other new and unknown occurrences will surely take place and, therefore, capabilities to mitigate the more probable and risk-significant spectrum of failures should be given more attention.

The learning has not been limited to major events - a la TMI - but also has included a significant part of operational safety issues. For example, once Intragranular Stress Corrosion Cracking (IGSCC) and Flow-Assisted Corrosion were identified as emergent failure mechanisms, the industry "learned" and the failure rates decreased almost exponentially as a function of accumulated experience. This is neither unique nor laudable: it is normal and expected.

Presently, the NRC and licensees are justifiably focused on the cracks found on PWR vessel head penetration nozzles and welds. I expect that this issue, due to the attention it is properly receiving, should not result in changes to the medium or Large Break LOCAs' frequencies. In the realm of reasonable assurance, it is reassuring to observe that in this country no error or failure from the operation of nuclear power plants has come close to breaching the very stringent safety standards established for the protection of public health and safety embodied in the NRC's strategic goals. We are committed to maintaining this record. The point is, the NRC now regulates in a "learned" and "learning" environment, a statement supported by the present operational safety performance of the plants in this mature industry. This fact allows us to conclude that significant new "errors" should be discovered and corrected before progressing to large failures, and more specifically, this environment should further decrease the probability of a LBLOCA.

When estimating failure rates, regulators today should focus not only on the existence of failures or errors --- many of which are due to human performance --- but also on the ability of the learned systems to cope with the failure, to detect deficiencies, to minimize consequences, to prevent --- or decrease significantly --- recurrence, and to properly value success. A truly effective regulatory system should balance the error data with the expected learned-system behavior to estimate future failure rates. This would be directly applicable to potential failures of the reactor coolant pressure boundary, and certainly applicable to LBLOCAs.

Another consideration in my decision to support a risk-informed alternative is the fact that the capability for making risk-informed decisions, based on relevant experience, deterministic models, defense in-depth and state-of-the-art PRA exists today. This

capability is not equally utilized by everyone, but it is here. Selecting a risk-informed alternative to the LOCA rupture size will require this capability at the expert level, with an acceptable - in regulatory space - high quality PRA. It is important to point out that I believe that the precise size of the large break is not a risk determinant issue; there are many other more risk-significant issues.

I now offer the following specific proposal on how to better reduce to practice the "LOCA failure analysis and frequency estimation":

> By December 31, 2003, the staff shall present to the Commission a comprehensive "LOCA failure analysis and frequency estimation" that is realistically conservative and amenable to decision-making. Realistically conservative estimations, with appropriate margins for uncertainty, should be used. Unrealistic extrapolation of estimates to time periods beyond the knowledge base and those requisite time periods used by the industry to inspect, monitor, and correct should not be used. Full understanding of the LOCA frequencies has always been important, but it is time that it becomes a short-term high priority. The goal is to achieve a predictive and well managed safety envelope embodying the best data and the best methods.

To achieve the objective of the above proposal I believe the following must be done:

a. *Use a 10-year period for the estimation of LOCA frequency distributions,* with a rigorous re-estimation conducted every 10 years and a sanity check for new types of failures every 5 years. This periodicity is consistent with the In-Service Inspection (ISI) program required of all reactor licensees. Longer periods do not make sense, neither technically nor from a regulatory perspective.

b. *Conduct a practical reconciliation of LOCA frequency distributions by the 1) expert use of service-data, 2) Probabilistic Fracture Mechanics (PFM) and 3) expert elicitation to converge the results*. Limiting the interval to 10 years will benefit significantly all three methods, using realistic predictability and convergence of results as necessary criteria. I strongly recommend that both service-data and PFM estimates be "reduced" to an appropriate set by "expert discrimination" of what data should be treated. Not all data is "born" equally nor should it be treated equally. For the purpose of LOCA estimation, a better discrimination of failure data is needed before it is used as predictive data. This is an area that needs prompt and expert attention. Service-based LOCA estimates (a statistical analysis of service experience data) are more useful than PFM, especially if the projection is limited to 10 years. PFM (a phenomena-based method using fracture and failure

analysis) can make a contribution, more so if it is used to selectively converge to service data predictions.

c. *Finally, expert elicitation should use the converged (whenever possible) service-data and PFM results to provide the Commission a comprehensive "LOCA failure analysis and frequency estimation" predictive envelope that is realistically conservative*. Expert elicitation is better when the data and analysis methods have first been screened for that purpose, and I believe that this has not yet been done.

In a related matter, in a briefing of Commission Technical Assistants on April 22, 2002, the staff stated that it is possible for some pipes to fail without a precursor leak (no leak-before-break) and that this contribution to the pipe break probability should be included in the analysis. I believe that leak-before-break is an established technological fact for risk-significant failures and the Commission should be informed and kept up-to-date on the staff's efforts in this area. I prefer to deal with actual probabilities and not with all possibilities.

One final comment on the above recommendations. As a regulator, I want to know, with significant confidence what the failure rate estimates are for next year, and the year after. For both rulemaking and regulatory oversight, 10 year scenarios are very good; furthermore, I know we can do it even better the next time around. Also, for <u>any</u> safety reason, we can and should take any needed action, as the circumstances require. No service-data, no PFM and no expert elicitation can confidently predict beyond 10 years, nor do we need to using a risk-informed approach.

In summary, the re-consideration of the Large Break Loss-of-Coolant Accident has been a long time in the making. I am convinced that we now have the necessary justification to make this fundamental change to the Light-Water Reactor safety regulatory construct now. Therefore, I vote as follows:

1. With regard to the re-definition of the Large Break LOCA:

The staff should prepare a proposed rule change to 10 CFR Part 50 that allows for a risk-informed alternative to the present maximum LOCA break size. I believe the rule should be very specific and leave no doubt that the pertinent risk parameters are addressed and only the non-significant contributions to risk are handled through severe accident risk management. For example, the modified definition of the LOCA, for use throughout Part 50 and wherever applicable, could read:

Loss of coolant accidents (LOCA). Loss of coolant accidents mean those postulated accidents that result from the loss of reactor

> **coolant at a rate in excess of the capability of the reactor coolant makeup system from breaks in the reactor coolant pressure boundary up to and including a break equivalent in size to the double-ended rupture of the largest pipe of the reactor coolant system *or up to an alternate maximum break size determined by including at least XX% [e.g., 95%, 96%...] of the LOCA failure contributors to core damage frequency.***

Thereby, the most significant failures are included. The net effect of this change would not reduce protection or give up risk sequences; rather, the rule will establish a new risk-informed design basis accident. Only those failures smaller than the average by about two orders of magnitude would be removed for severe accident management; i.e., the capability to mitigate the double-ended rupture of the largest pipe in the reactor coolant system will be retained under severe accident management principles and activities.

While I would expect pertinent changes in the design basis and associated analysis to naturally occur, I concur with the staff that changes in hardware and operation "would require that it be demonstrated that the ECCS functional reliability is commensurate with the frequency of accidents in which ECCS success would prevent core damage or a large early release". In other words, I am not supporting changes to functional requirements unless they are fully risk-informed and protective of public health and safety. For example, I would not support actual changes to ECCS coolant flow rates or containment capabilities to mitigate accidents. I would support changes that provide for risk-informed sequencing of equipment with demonstrated functionality and reliability requirements that arise from the alternate criteria.

There is also no doubt that the redefinition of the LBLOCA would also require strict configuration controls, including during Low Power and Shutdown (LPSD) operations. Thus, I support requiring these strict configuration controls and believe that the ROP, the revised Maintenance Rule and Reg. Guide 1.174, are suitable for use in addressing such requirements.

One last point on the alternate break size. The conservative CDF and LERF safety criteria of Option 3, and particularly the capability of Reg. Guide 1.174 to deal both with absolute (CDF) and relative (delta-CDF) changes, are essential to effect an alternative break size with reasonable assurance of adequate protection.

Furthermore, as discussed above in the recommendation for determining LOCA frequency distribution amenable to decision-making, the rulemaking should be supported by a 10 year estimation of LOCA frequencies, to be delivered by December 31, 2003. This should be done in parallel with the rulemaking activities.

2. Regarding the recommendations in SECY-02-0057:

I approve the staff recommendations to proceed with rulemaking changes to 10 CFR 50.46, 10 CFR Part 50, Appendix K, and GDC 35, sooner rather than later, including an option to the Appendix K evaluation model requirement to permit use of a decay heat model based on the 1994 ANS standard. I support the unbundling and pursuing of separate rulemaking for each of the proposed changes. In order to improve the timeliness, I also approve not preparing a separate rulemaking plan for each rulemaking. However, I strongly believe we should seek early public and stakeholder comments on all of these proposals.

The staff proposed allowing the use of a decay heat model based on the 1994 ANS standard and stated that concerns with uncertainties and conservatism associated with the current standard would be addressed separately from any proposed rulemaking. This is a prudent approach. A similar approach could be used to handle issues separate from the rulemaking when pursuing rule changes associated with the redefinition of the Large Break LOCA.

Risk is measurable and manageable, and risk-informed decision-making is a very good tool to improve safety. It is available now, and I strongly recommend we use it for this particular significant issue in a manner protective of public health and safety.