GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

160021

B-279244

March 6, 1998

Mr. David Meyer, Chief
Rules and Directives Branch
Division of Administrative Services
Nuclear Regulatory Commission

Subject: Year 2000 Readiness: NRC's Proposed Approach Regarding Nuclear Powerplants

Dear Mr. Meyer:

We appreciate the opportunity to comment on the Nuclear Regulatory Commission's (NRC) January 29, 1998, Federal Register notice, "Proposed Generic Communication; Year 2000 Readiness of Computer Systems at Nuclear Power Plants (MA0138)." We are providing this letter to document the substance of the oral comments we presented to NRC officials on February 27, 1998.

In order to gain assurance that nuclear powerplant licensees are effectively dealing with Year 2000 problems that could affect safety-related systems, NRC's proposed generic letter requires licensees to submit (1) a brief description of their Year 2000 programs, if they are not following Year 2000 guidance developed jointly by two industry organizations–the Nuclear Energy Institute (NEI) and the Nuclear Utilities Software Management Group (NUSMG),[1] (2) written confirmation that they are implementing their programs, and (3) written certification that their facilities are "Year 2000 ready" and in compliance with the terms and conditions of their licenses and NRC regulations, together with a status report on any work remaining to be done to complete their Year 2000 programs.

[1]The NEI is a policy organization of the nuclear industry that fosters and encourages the safe utilization of nuclear energy. NUSMG is a nonprofit organization that provides a forum for nuclear utilities to obtain concensus on software control issues.

160021

We commend NRC for acting on this issue. Although it is our understanding that, to date, no safety-related Year 2000 problems have come to NRC's attention, we agree that special steps are warranted to provide assurance of continued safety at nuclear facilities during the Year 2000 transition. Our comments, therefore, are directed at clarifying and strengthening NRC's regulatory authority to address safety-related Year 2000 problems, particularly in these areas:

- specifying a more complete Year 2000 program for licensees,
- monitoring licensees' progress on Year 2000 readiness,
- clarifying the "Year 2000 ready" certification, and
- addressing future Year 2000 maintenance requirements.

Our comments on each of these areas are discussed below, along with suggestions for how NRC might improve its effectiveness in this important effort.

SPECIFYING A MORE COMPLETE YEAR 2000 PROGRAM FOR LICENSEES

The proposed generic letter would require licensees to indicate whether they are pursuing a Year 2000 readiness program at their facilities. As a benchmark of program effectiveness, NRC is relying heavily on Year 2000 guidance developed jointly by NEI and NUSMG, entitled Nuclear Utility Year 2000 Readiness (NEI/NUSMG 97-07, October 1997). NRC's proposed generic letter states that NRC staff "believes that the guidance in NEI/NUSMG 97-07, when properly implemented, will present an appropriate approach for licensees to address the Y2K [Year 2000] problem at nuclear power plant facilities." Accordingly, the proposed generic letter would require licensees to state in writing whether they are pursuing a Year 2000 program as outlined in the NEI/NUSMG guidance.

We agree on the importance of requiring licensees to provide NRC with assurance that they are implementing a program that effectively addresses the Year 2000 issue. However, we believe that NRC should be aware that the NEI/NUSMG document has several significant shortcomings.

Shortcomings in the NEI/NUSMG Guidance

The NEI/NUSMG Guidance does not include all the elements of a comprehensive Year 2000 program. In particular, the guidance does not deal adequately with risk management, business and contingency planning, or remediation of embedded systems.

- *Risk Management:* The NEI/NUSMG guidance does not include adequate discussion of risk management in Year 2000 programs. Risk management is an ongoing activity through which top management (1) identifies and tracks internal and external risks to the organization and outside parties resulting from Year 2000-related problems, (2) assesses Year 2000 project and program progress, and (3) develops contingency plans for mitigating the impact of potential Year 2000-related failures.

- *Business Continuity and Contingency Planning:* The NEI/NUSMG guidance does not cover business continuity and contingency planning in any detail.[2] Organizations need to have plans to ensure business continuity since computer failures may occur despite conscientiously implemented Year 2000 programs. Business continuity planning focuses on reducing the risk of Year 2000-induced business failures and safeguarding an organization's ability to produce a minimum acceptable level of outputs and services in the event of failures with internal or external systems. It also links risk management and mitigation efforts to an organization's Year 2000 program.

- *Embedded Systems:* The stated scope of the NEI/NUSMG document ("software, or software based system or interface") is too narrow, since date dependencies can also occur in computer hardware, firmware (software instructions stored in read-only memory), or data. While the NEI/NUSMG guidance mentions the importance of dealing with Year 2000 problems in embedded systems (e.g., in appendix F), it does not provide sufficient detail to assist utilities. Referencing existing work by others could help provide this needed detail.[3]

Vendor Warranties

Section C of the NEI/NUSMG guidance specifies that vendors should provide Year 2000 compliance warranties to licensees, even for work previously completed. This approach is premised on the assumption that vendors would (1) agree to amend existing contracts for hardware, software or firmware to

---

[2] GAO's forthcoming exposure draft, Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19) provides a framework that can help the utilities develop these plans. This document builds on GAO's previous Year 2000 guidance, Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997), and draws on a variety of research and publications of the Gartner Group, the Disaster Recovery Institute of Canada, the Department of Information Resources for the State of Texas, and others.

[3]See, for example, Embedded Systems and the Year 2000 Problem: Guidance Notes (IEE Technical Guidelines 9:1997) by the Institution of Electrical Engineers (IEE). Further information and guidance on embedded systems is available within IEE's web site at <http://www.iee.org.uk/2000risk>.

warrant that the product is Year 2000 compliant, as defined in the "Technical Criteria for Year 2000 Compliance" in the NEI/NUSMG document, (2) agree to forgo existing provisions of valid contract or license agreements that limit the vendors' liability, and (3) accept without time limitation the liability for any costs or damages incurred by the licensee that are caused by a breach of the warranty. NRC appears to endorse contract language included in the NEI/NUSMG document as an effective approach to the Year 2000 problem. We suggest that NRC reconsider any apparent endorsement of contract language for use by private parties.

Suggested Alternative

As an alternative to relying on the NEI/NUSMG guidance, we suggest that NRC's generic letter specify the elements of an effective Year 2000 program, particularly as they bear on safety concerns under NRC's regulatory authority. One publication that can help NRC in this regard is our Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997). This guide is a distillation of government and private sector best practices for dealing with the Year 2000 problem, and provides a useful overview of the elements of an effective Year 2000 program.

NRC could require licensees to address the elements of an effective Year 2000 program when they submit the "brief description" of their own programs, as called for in the proposed generic letter. This approach would provide NRC with a better basis for assessing the effectiveness of the licensees' Year 2000 programs in dealing with safety-related issues.

MONITORING THE PROGRESS OF THE LICENSEES' YEAR 2000 PROGRAMS

The proposed generic letter requires the licensees to make only two reports on their Year 2000 programs. The first report, within 90 days of the generic letter's date, provides written confirmation that the licensees are implementing a Year 2000 program. The second report, to be filed upon completing their programs, or in any event no later than July 1, 1999, provides written confirmation that the licensees' facilities are "Year 2000 ready" and in compliance with the terms and conditions of their licenses and NRC regulations. At that time, the licensees would also describe any work remaining to be done to complete their Year 2000 programs.

To effectively monitor licensees' Year 2000 progress on systems under its regulatory authority, NRC will need more substantive and frequent progress reports. These reports should, at a minimum, require (1) a complete inventory of safety systems and other systems that will need to be certified as "Year 2000 ready" under the generic letter, (2) planned actions on these systems, including formulation and testing of contingency plans, and (3) periodic updates on the

status of those actions. Waiting until July 1999 will not leave NRC much time to respond constructively to a licensee's unresolved Year 2000 problems.

CERTIFYING "YEAR 2000 READINESS" FOR SAFETY SYSTEMS

NRC's proposed generic letter requires each licensee to provide a written response confirming that "your facility is Y2K ready and in compliance with the terms and conditions of your license(s) and NRC regulations." While the criteria for "Year 2000 compliance" are clear and amenable to objective testing, the same cannot be said for the term "Year 2000 ready." "Year 2000 ready" is defined in the generic letter as "a computer system or application that has been determined to be suitable for continued use into the year 2000 even though the computer system or application is not fully Y2K compliant." This determination involves making judgments about suitability. The proposed generic letter does not require the licensees to state how and why they determined that a non-compliant system would be suitable for continued use. For those critical safety systems under NRC's purview, we suggest that the generic letter include such a requirement.

It would also be useful if the generic letter included a discussion of how NRC's ongoing inspection activities will be used in the process of certifying Year 2000 readiness. For example, it is not clear whether the inspections will include checks to see if key Year 2000 issues are being addressed, whether key conversion activities are being carried out properly, or whether critical project milestones are being met.

INDEPENDENTLY VERIFYING AND VALIDATING SAFETY SYSTEMS

The generic letter does not discuss the role of independent verification and validation (IV&V) in supporting the licensees' "Year 2000 ready" certifications. We recognize that, under NRC regulations, modifications to certain systems at nuclear facilities must be verified or checked to ensure that the systems will continue to operate properly. However, the unusual challenges posed by the Year 2000 problem may warrant obtaining additional assurances. For example, the problem of an embedded system is not always an implicit or explicit date variable. The counters inside the system may reset themselves at the millennial change and work well, or not at all, or slowly degrade. The "testing" may require a line-by-line trace of the specification and design model (assuming they still exist).

Accordingly, we suggest that the generic letter require licensees to (1) describe their Year 2000 plans for IV&V of systems related to safety and (2) provide the results of IV&V with their written certification of Year 2000 readiness. The IV&V can be done using in-house resources or contractor resources, or both, as

long as the review team is technically qualified. It is, of course, particularly important that IV&V provide assurance that the powerplant's protection system maintains its design capabilities, as required by NRC regulations.

ADDRESSING FUTURE MAINTENANCE REQUIREMENTS OF "YEAR 2000 READY" SYSTEMS

As noted above, NRC's proposed generic letter requires only that computer systems and applications be "Year 2000 ready." However, there may be future maintenance requirements for "Year 2000 ready" systems under NRC's purview. For example, some logic-based techniques used to make systems "Year 2000 ready" have a predetermined time period during which they can function without a date-related failure. The "fixed window" technique, for instance, involves setting date boundaries that can be correctly referenced by a two-digit year. However, these boundaries need to be manually readjusted as the dates being processed approach the boundary limits.

NRC's generic letter does not include a way to identify, track, and follow up on the future maintenance plans for any safety-related "Year 2000 ready" systems that could eventually fail without further modification or replacement. Therefore, we suggest that the letter address the issue of future Year 2000 maintenance requirements. This issue could be made part of the aforementioned status report that licensees would be required to submit no later than July 1, 1999, describing the work that remains to be done to complete their Year 2000 programs.

- - - - -

We are sending copies of this letter to representatives of the Nuclear Energy Institute and the Nuclear Utilities Software Management Group. We will also make copies available to other interested parties upon request. If you have questions or wish to discuss the issues raised in this letter, please contact me or Keith Rhodes, Technical Director. We can be reached at (202) 512-6412.

Sincerely yours,

Dr. Rona B. Stillman
Chief Scientist for Computers
and Telecommunications

(511642)

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested