No. S-99-02

"Exterminating the Bug:

Governmental and Industrial Challenges in the Face of the Year 2000 Problem"

by

Dr. Shirley Ann Jackson, Chairman

U.S. Nuclear Regulatory Commission

OECD/NEA Committee on Nuclear Regulatory Activities

International Workshop on the Impact of the Year 2000 on the Nuclear Industry

Ottawa, Canada, February 9, 1999

Introduction

Good evening, ladies and gentlemen. First and foremost I would like to thank our host, the Atomic Energy Control Board (AECB), and our sponsor, the Organization for Economic Cooperation and Development/Nuclear Energy Agency (OECD/NEA), for organizing and conducting this workshop. Ottawa is a lovely city-a bit cold this time of the year-but very lovely.

The world has come to rely on computers in its day-to-day operations, and people have accepted computers as part of everyday life. We have built a web of interconnected computer systems on which we rely for virtually every need, including energy, communication, transportation, and banking, among others, making our world increasingly interconnected and interdependent. There also is a reliance, however unrealized, on embedded systems that include chips and firmware, which are in virtually every electronic appliance we use at home. These computers and embedded chips also are found in electrical transmission and distribution systems, communication systems, and equipment and components in electrical generating stations, including nuclear power stations. Just after the stroke of midnight on December 31, 1999, these systems have the potential to fail.

Particular concerns within the U.S. electric power industry include the reliability of voice and data communications needed for monitoring and control of power systems, and the use of embedded chips in communications and numerous power system device controllers. While it is estimated that only 1 to 2 percent of these devices uses a time/date function in a manner that could result in a Y2K malfunction, the interconnected nature of electric systems make them sensitive to the failure of any equipment.

As you know, the Year 2000 (Y2K) problem concerns the use of a two-digit year element, usually within a six-digit date representation (MM/DD/YY or variations), with the twentieth century not explicitly stated but implied. Many of the computer-based systems we depend upon could experience operational difficulties at the turn of the century due to their inability to recognize and accommodate the change from the year 1999 to the year 2000. The degree to which such difficulties impact society is a function of the type of component experiencing the problem, the degree to which the problem impacts the component, and the nature and number of interrelationships between the affected component and other components and systems.

The Y2K problem is not without solutions. Businesses and governments know how to fix non-compliant systems, and are devoting significant financial and human resources toward

doing so. Identifying, categorizing, repairing, or replacing systems, components, and equipment and their interconnections takes time, however, and January 1, 2000, is an immovable deadline. Ensuring that critical systems and equipment are ready for the Year 2000 is a matter of prioritizing what needs to be fixed, devoting adequate human and financial resources to the project, and developing contingency plans to be used in the event that systems, either internal or external, fail.

Electrical Grid Instability and Loss of Offsite Power

The Y2K problem has significant implications for the management of electrical distribution networks (grids). Individual susceptibilities may exist in software controlling a particular portion of the grid itself or telecommunications systems supporting grid management. Moving downward to the electrical generation level, Y2K problems can affect individual components involved in the production of electricity, such as digital process controllers. When one considers a nuclear power plant, a concern exists that not only power generation problems may arise, but that problems may extend to the safety systems of a facility and create challenges to these systems.

When one considers the myriad of possible situations in which the Y2K problem can manifest itself, it soon becomes obvious why the issue demands our prompt attention. In an admittedly pessimistic scenario, what starts as a Y2K-related electrical grid instability, for a particular nuclear plant, could cascade into a loss of offsite power which, in turn, would challenge plant safety systems. Can such a cascade occur? In 1996, two electrical disturbances (within a five-week period) on the Western U.S. Grid caused 190 plants to trip off-line, including several nuclear units. In particular, on July 2, 1996, a transmission line sagged into a tree in Idaho, creating a ground fault which progressed into a major fault on the Western Interconnection. The affected nuclear plants saw a frequency transient, but did not scram or lose offsite power. A similar event occurred the next day but did not propagate outside Idaho. On August 10, 1996, again a line sagged into a tree, this time in Oregon. The subsequent transient resulted in the loss of over 30,000 MW(e) of load, 25,000 MW(e) of generation, which is 17 percent of the total western U.S.-Canada generation. Among the 190 generating units that tripped were 4 nuclear units at Diablo Canyon in California and Palo Verde in Arizona.

Why are these events significant? Let me explain. First, such cascading transients, in causing reactor scrams, can challenge plant safety systems directly. Second, they can lead to Station Blackout events. In 1988, the NRC initiated Individual Plant Examinations to study the various initiators of reactor core damage events. All U.S. nuclear plants performed probabilistic risk assessments, with detailed modeling of their plant systems, to search for plant-specific vulnerabilities from severe accidents. At many of the nuclear plants these studies showed that a major contributor to core damage frequency was a Station Blackout event. Events of this type are defined as Loss-of-Offsite-Power events, coupled with the inability of the onsite emergency diesel generators to provide power to key plant safety equipment. If a cascading transient brought down multiple generating units at a time that onsite power sources did not exist, or were compromised, a nuclear plant could experience a Station Blackout event.

Depending upon the degree of Y2K readiness in safety systems, the result of a Loss of Offsite Power or Station Blackout could range from an analyzed, expected, plant response to a more significant event. Moreover, if emergency response is required offsite, the degree to which the telecommunications infrastructure is Y2K compliant would dictate the effectiveness of that response. To be sure, we at the NRC do not deem such an outbreak of failures to be probable based upon what we currently know about Y2K. Rather, it is the possibility of such events that motivates our actions.

Tonight, I would like to discuss the activities the United States is undertaking with respect to the Y2K issue, both domestically and internationally; the actions the Nuclear Regulatory Commission (NRC) is taking, both internally and externally; and some of the factors that are driving these activities.

U.S. Government Activity

The importance of addressing the Y2K problem in the U.S. was acknowledged by President Clinton early last year when he established the President's Council on Year 2000 Conversion on February 4, 1998. The Council is made up of representatives from more than 30 major U.S. Federal executive and regulatory agencies, including the U.S. Nuclear Regulatory Commission. The Council Chair is Mr. John Koskinen, Assistant to the President for Year 2000 Conversion. Each agency on the U.S. Council is responsible for oversight of the Y2K efforts necessary for ensuring availability of the infrastructure sector for which they have statutory responsibility. These "sector coordinators" promote action on the Y2K problem and offer support to public and private sector organizations-both domestically and internationally-within their policy areas. In particular, agencies are working with industry trade associations (which have unique capabilities for communicating with their members about the Y2K problem); individual companies; and U.S. State and local governments. The nine major sector areas covering the provision of critical services are: benefits/payments, communications, electrical power, emergency services, financial services, oil and gas, solid waste, transportation, and water supply.

On January 7, 1999, the U.S. Council issued its first quarterly report, which summarizes information about the level of preparedness among key industries as follows:

- Virtually all of the industry areas report high awareness of the problem and its potential consequences.
- Participants in several areas are mounting aggressive efforts to combat the Y2K problem, and to ensure that critical systems will be able to process the date change to the Year 2000. Financial institutions, including banks and securities firms, are most notable for their coordination and progress.
- We increasingly are confident that there will not be large-scale disruptions among banks, and in the power and telecommunications industries. Disruptions that do occur most likely will be of a more localized nature.
- Large organizations often have a better grasp on the problem than some of their smaller counterparts. While many small and medium-sized U.S. businesses and government organizations are focused on solving the Y2K problem and have made significant progress, some continue to believe the problem will not affect them or are delaying action until failures occur. Lack of preparedness among these organizations increases the risk for localized Y2K disruptions.

At the Federal level, U.S. agencies are working to prepare mission-critical systems for the Year 2000, and have mounted aggressive efforts to ensure that critical services will not be disrupted by the transition to the new millennium. Agencies are working to develop contingency plans in the event of internal or external Y2K related failures.

To help companies, associations, and other groups collect and share information on the status of Y2K efforts, the President worked with the Congress to enact the "Year 2000 Information and Readiness Disclosure Act." On Oct. 19, 1998, President Clinton signed this act into law and stated: "The Y2K problem is an enormous challenge, and we must meet it. Enactment of this legislation is a significant achievement toward allowing all of us to take a successful step into the new millennium." This Act placed limits on financial liability for entities that disclose

Y2K readiness information, thereby encouraging U.S. companies to share information about fixing computers and systems at risk because of the Year 2000 date problem.

With respect to electric power distribution, in May 1998, the U.S. Secretary of Energy requested that the North American Electric Reliability Council (NERC) coordinate efforts within the electric power industry to assure a smooth Year 2000 transition. The NERC is a voluntary industry reliability group, made up of 10 regional councils, whose membership includes nearly every major provider of electricity generation and transmission within the Eastern, Western, and Texas interconnections that form the backbone of the electricity supply system for the United States, Canada, and a small portion of Mexico.

The NERC has established recommended industry-wide milestones for ensuring that U.S. electric systems are ready for the Year 2000. The recommended completion date for the remediation/testing phase of Y2K preparations is May 1999. Mission-critical systems and components (e.g., power production, energy management systems, telecommunications, substation controls and system protection, and distribution systems) are to be made Y2K ready by June 30, 1999.

The NERC has worked in partnership with trade associations representing investor-owned utilities (Edison Electric Institute), municipal utilities (American Public Power Association), rural electric cooperatives (National Rural Electric Cooperatives Association), nuclear power plant operators (Nuclear Energy Institute), and the Canadian electric power industry (Canadian Electricity Association) to ensure the most complete coverage of the industry in the surveys and assessments of Y2K readiness.

The U.S. electric power industry is placing considerable emphasis on contingency planning for the Year 2000 transition. The NERC is targeting June 1999 as the date for completion of contingency plans.

Activities of the U.S. Nuclear Regulatory Commission for Y2K Readiness

U.S. Nuclear Regulatory Commission (NRC) preparations, both internal and external, have been underway for some time.

Internal Preparations

Internally, the Year 2000 problem potentially affects the NRC in the areas of computer information systems hardware and software, embedded chip systems, data exchanges with outside entities, telecommunications hardware infrastructure, and building environmental, fire protection, security access, and other control systems.

The NRC adopted a strategy, in accordance with best practices published by the Office of Management and Budget (OMB), and developed a schedule closely aligned to the milestone dates recommended by the OMB for assessment, renovation, validation, and implementation of remediation for key systems. The NRC made the decision to spend additional time on assessment so that the full scope of our remediation efforts were understood. Having an understanding of this scope enabled us to schedule resources more accurately to correct identified system problems within established schedules.

At the request of the OMB, all U.S. agencies were asked to identify their mission-critical systems. The NRC identified seven computer and telecommunications systems as having high importance related to accomplishing the NRC mission and requiring a high level of reliability, because any delay in access to the system for any reason could adversely affect the ability of the agency to fulfill its mission of protecting public health and safety, promoting the common defense and security, and protecting the environment.

The NRC grouped its remaining systems into two categories (business-essential and non-critical) in order to make explicit decisions about establishing their priority for repair. Business-essential systems are described as any system that is integral to agency processes and required for meeting agency statutory, programmatic, legal, or financial obligations. Typically, the agency could function without any major impact on its operations if any of these systems malfunctioned and was unavailable for up to 3 or 4 weeks while being repaired. Non-critical systems are those that are not considered mission-critical or business-essential and whose unavailability would represent only an inconvenience to the agency. Typically, these systems can be unavailable for extended periods (1 to 2 months or more) while they are being repaired, and manual processes can be used readily in their place, if necessary.

Of the total number of systems identified as requiring review for Y2K vulnerabilities, the NRC ultimately identified 88 systems with Y2K problems that had to be addressed. Seven were mission-critical, 51 were business-essential, and 30 were non-critical.

Our testing or validation of system repairs has been very rigorous. Systems repaired by Year 2000 program contractors are being verified and validated independently, using a three-level approach. The first level, unit testing, is performed by personnel who actually repair the system code. The second and third levels are performed by personnel who are not involved with system repairs. The second level of testing is performed by personnel assigned to a permanent quality assurance group, using an established test plan. Third-level testing is performed by the NRC personnel who use the system, also using an established test plan. Only when written approval is received from all three testing levels do we consider the system validated and report it as such.

We also have analyzed and identified embedded chip systems at the NRC. Forward date testing of embedded chip systems can be problematic, since access to embedded chip system control programs is limited. As a result, both the nuclear power industry and the NRC rely on manufacturer certification to establish compliance and, where possible and appropriate, on in-house testing to confirm compliance. We have tested our microcomputers successfully with available testing software to determine compliance.

Additionally, the NRC has assessed all areas of the agency that have the potential to exchange data with other Federal, State, and local governments, as well as with international and commercial entities. We have assessed satisfactorily all agency building systems and our telecommunications infrastructure, and also have contacted our telecommunications service providers to ensure that all systems are compliant or will be compliant by mid-1999.

Our strategy required our business experts to prepare contingency plans in case we were unable to complete repairs in time, or in case factors outside our control (electricity, etc.) rendered the systems unusable. Our contingency plans are commensurate with the nature of our mission-critical systems. In all but one case (our administrative local area network), assuming total automation unavailability, we have an option of reverting to manual methods to continue support of the mission-critical functional area. These manual methods have been used successfully by our business offices in the past when their systems did not exist or were unavailable temporarily.

I am pleased to tell you today that, as of February 5 (54 days ahead of the OMB-established milestone), we have completed the renovation, validation, and implementation of all NRC mission-critical, business essential, and non-critical systems requiring repair.

In terms of program cost, I am pleased to report that our Y2K program was completed under budget. Since we have completed our program for all systems, $600,000 in resources

budgeted for FY 2000 will not be needed, and we expect our actual expenditures for FY 1999 to be less than budgeted.

External Preparations

The NRC also is developing a Y2K contingency plan to enable us to respond rapidly to potential events at licensed U.S. facilities resulting from unanticipated Y2K problems. The plan includes provisions to collect and disseminate information on Y2K-related events that occur in countries in time zones ahead of the U.S. Continued safe operation of nuclear power plants during the transition to the Year 2000 is important to help maintain reliable electrical power supplies. As such, the NRC Y2K contingency plan includes considerations for rapid decision-making under circumstances where a Y2K problem might result in licensee non-compliance, but would not affect continued safe plant operation. The NRC contingency plan will be coordinated with the U.S. nuclear power industry, other Federal agencies (including the Federal Emergency Management Agency), State governments, and international nuclear regulatory organizations.

With respect to external activities, in 1996 the NRC began an evaluation of the impact of the Year 2000 problem (Y2K) on nuclear power plants. To ensure that senior level management at operating U.S. nuclear facilities was aware of the Y2K problem, the NRC issued Information Notice (IN) 96-70, "Year 2000 Effect on Computer System Software," on December 24, 1996. IN 96-70 described the potential problems that nuclear facility computer systems and software might encounter during the transition to the new century. All U.S. nuclear power plants, fuel cycle facilities, and other material licensees were provided with copies of this document.

Since 1996, the NRC has been working with nuclear industry organizations to address the Y2K problem. In 1997, the Nuclear Energy Institute (NEI) agreed to take the lead in developing industry-wide guidance for addressing the Y2K problem at nuclear power reactors. In November 1997, NEI issued a guidance document to all U.S. nuclear power plant licensees, entitled "Nuclear Utility Year 2000 Readiness" (NEI/NUSMG 97-07).

In Generic Letter 98-01, issued May 11, 1998, the NRC requested that all operating U.S. nuclear power plant licensees submit written responses regarding their facility-specific Y2K readiness programs in order to obtain confirmation that licensees are addressing the Y2K problem effectively. Thus far, all licensees have submitted an initial response stating that they have adopted plant-specific programs, similar to that outlined in the NEI guidance document to which I referred, that are intended to make the plants Y2K ready by July 1, 1999. Generic Letter 98-01 also requests a written response, no later than July 1, 1999, confirming that these facilities are Y2K ready. If not Y2K ready by the July deadline, these licensees also must include a status report for the work remaining, including completion schedules, to ensure timely Y2K readiness. Based on these responses, the NRC will determine the need for plant-specific follow-up actions.

In NRC Generic Letter 98-01, it was noted that despite the best of efforts to achieve Y2K readiness, unanticipated problems (particularly events external to a plant) could occur and disrupt continued plant operation. Therefore, contingency plans were needed to address potential unanticipated Y2K problems. To address this need, in August 1998 NEI issued another guidance document, "Nuclear Utility Year 2000 Readiness Contingency Planning," (NEI/NUSMG 98-07) which is being incorporated into Y2K readiness programs by all U.S. nuclear power plant licensees. The detailed plant-specific contingency plans also are scheduled to be completed by July 1, 1999.

Although the primary focus of the NRC with our licensees has been on public health and safety, related to reactor operations, we recognize the concern that the Year 2000 problem

could affect the reliability of electrical grids. Our regulatory focus on electrical grid reliability has related primarily to the challenges to plant safety systems that might result from a grid transient, such as a Loss of Offsite Power.

However, the Y2K problem has presented the NRC with a unique challenge. NRC regulatory oversight and authority does not extend to the U.S. offsite electrical grid system. Nonetheless, we recognize the national importance of a broader focus that helps to ensure that potential concerns with electrical grid reliability are identified and resolved. As mentioned earlier, the NRC supports the efforts of the President's Council on Year 2000 Conversion. As members of the Energy/Electric Power Sector Working Group, we understand the importance not only of maintaining nuclear power plant safety, but of enhancing safe grid operation in the face of the Y2K problem as well.

In addition to the exchange of information between the NRC and power reactor licensees, we have recognized the importance of seeing, first-hand, how Y2K preparations are being pursued at the nuclear power plants. In 1998, the NRC began a series of audits at 12 power reactor licensees. The individual licensees were chosen to reflect a cross-section of ages, reactor types, locations, vendors, and utility sizes. From these audits, the NRC concluded that, by employing the NEI guidance I previously described, licensees could address the Y2K problem effectively. The audits also concluded that, in general, licensees began to develop contingency plans late in the Y2K preparation process. Consequently, the NRC concluded that six additional, differently focused reviews, involving licensees other than those that comprised the original 12, were in order to determine the effectiveness of licensee contingency planning. We will be performing these audits in the March/April time frame, focusing on this area.

International Activities

The President's Council stated, in its first quarterly report, that international failures are likely. Despite recent increased efforts, a number of countries have done little thus far to remediate critical systems. These failures could have a significant impact upon the U.S. and other countries, especially in areas that rely heavily upon cross-border operations. International Y2K activity is the area about which we have the least information. The U.S. State Department and other agencies on the Council's International Relations Working Group have been working with U.S. embassies and other organizations around the world in an effort to gather Y2K information on a country-by-country basis.

The U.S. is working to encourage other nations to take action on the problem and to facilitate coordination of country Y2K efforts on a regional and international basis. We worked closely with the President's Council to support the United Nations meeting of national Y2K coordinators. Coordinators from over 120 countries attended the December 1998 meeting. Delegates to the meeting discussed Y2K challenges in key infrastructure areas and agreed to work together regionally to share information on their Y2K remediation and contingency planning. The U.S., along with several other nations that helped to organize the meeting, will work to create an international coordinating center to support these efforts in the coming months.

In preparation for the 42nd IAEA General Conference in September 1998, the NRC took the lead in drafting a resolution on the Year 2000 (Y2K) as it applies to the safety of nuclear power plants, fuel cycle facilities, and other enterprises using radioactive materials. That resolution urged, among other things, that: Member States submit information to the IAEA on activities underway to inventory and remediate Y2K problems at their nuclear facilities; and that the IAEA act as a central coordination point in disseminating information about Member State Y2K activities.

During its numerous bilateral side meetings with countries such as Argentina, Lithuania, Russia and Ukraine, the NRC presented the draft resolution and urged their support. Ultimately, 28 Member States co-sponsored the resolution, including a number of countries that have nuclear facilities whose safety are of great concern to the U.S. government.

Since the General Conference, the NRC likewise has worked with the IAEA to formulate a Y2K program that would address nuclear safety aspects of the Y2K problem. We requested that State Department funds be allocated, under the FY98 Voluntary Contribution, to fund a Cost-Free Expert (an individual who would work at the IAEA for one year at no cost to the IAEA) to work specifically on Y2K nuclear safety matters in the Department of Nuclear Safety. The Cost-Free Expert assumed his post in December 1998, and the Department of Nuclear Safety is now developing and implementing a comprehensive program to help Member States address Y2K inventories and contingency planning.

The U.S. also has forged bilateral cooperative agreements on the Y2K challenge with several nations, including Japan, South Korea, Canada, and Mexico. Under these agreements, U.S. authorities are working with their counterparts in other countries to exchange information on Y2K efforts in key areas such as power, transportation, customs, telecommunications, finance, and health care.

The U.S. Council Chair has met with numerous international organizations such as the Organization of American States, the OECD, the World Bank, and the International Monetary Fund to enlist their support in encouraging their members to take action on the Y2K problem. To assist developing countries, the U.S. is working with the World Bank to support its program of increasing awareness of the problem among developing countries through a series of international conferences.

In the international arena, my understanding is that the nuclear power industry and its regulators in Canada, Western Europe, and the Far East have undertaken similar efforts and readiness schedules to that of the NRC for addressing the Y2K problem at nuclear power plants. However, some countries have started only recently to focus on the Y2K problem. Last month, at a meeting of the International Nuclear Regulators Association (INRA), which I chair, a statement was drafted on the Y2K problem, expressing concern that the results of the recent United Nations Conference indicated that few countries will be Y2K ready, and that few have adopted expert guidance regarding remediation and contingency planning. Contingency planning, while important in itself to all countries, takes on new importance in late-starting countries, due to the short time remaining before the year 2000. In its statement, the INRA urged governments and their regulatory authorities to take urgent action to diagnose the extent of the Y2K problem in nuclear facilities (including nuclear power plants, fuel cycle facilities, and medical facilities), and to formulate and implement effective remediation programs and contingency planning in the near term for this pre-eminent concern. I understand that contingency planning was the subject of discussion at a session here today. This is a key aspect to effective Y2K readiness.

<u>There Are No Islands</u>

We have come to recognize that nuclear power plants are not islands. The plants rely upon stable electrical distribution systems to support steady-state operations. Symbiotically, stable distribution systems rely on the collective output of generating facilities. In a very real sense then, we all are dependent on the stability of one another. An extension of this concept applies to emergency planning. The ability of both onsite personnel and civic responders to act will be tied directly to the state of Y2K preparedness in each of the participating organizations. In the same way that each generating plant on a grid can be affected by the other plants on the grid, the emergency response capabilities associated with one plant can be impacted in responding to other potential eventualities, such as events at neighboring plants or other Y2K-

related emergencies outside of the electricity industry. For this reason, ensuring continuity at the interfaces of regulator-to-licensee, regulator-to-public, and regulator-to-government is crucial, as such continuity is required to buttress emergency response, our last line of defense in protecting public health and safety. It is the recognition of these facts that has driven many of the actions I have described tonight--the recognition that, despite our best efforts, something still could go awry. I might point out that, just within the past several weeks, at the initiative of the NRC, the NEA Committee on Nuclear Regulatory Activities (CNRA) and its member countries are planning an international exercise to assist in world-wide contingency planning.

Summary

I hope I have been able to convey a sense of the activities being conducted by the United States, and by the NRC in particular, to prepare for the impending turn of the century. Due to the intensity of the activities being conducted in this area, the actions I have described do not represent an exhaustive compilation. For this reason, I encourage you to optimize the use of this conference and similar venues to explore both the possibilities and the solutions for this problem. As I have stated, the U.S. and the NRC stand ready to provide technical information and support in whatever way we can. I have made copies of the generic NRC communications to which I have referred available to this conference. These documents, as well as additional information on NRC Y2K activities, also can be accessed on the NRC worldwide web page.

Thank you for your attention. I wish all of you every success in this very important endeavor.