

# Y2K AND NUCLEAR POWER: WILL THE REACTORS REACT RESPONSIBLY?

---

---

JOINT HEARING  
BEFORE THE  
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,  
INFORMATION, AND TECHNOLOGY  
OF THE  
COMMITTEE ON GOVERNMENT REFORM  
AND THE  
SUBCOMMITTEE ON TECHNOLOGY  
OF THE  
COMMITTEE ON SCIENCE  
HOUSE OF REPRESENTATIVES  
ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

OCTOBER 22, 1999

Committee on Government Reform

**Serial No. 106-58**

Committee on Science

**Serial No. 106-55**

Printed for the use of the Committee on Government Reform and the  
Committee on Science



Available via the World Wide Web: <http://www.house.gov/reform>

U.S. GOVERNMENT PRINTING OFFICE

61-296 CC

WASHINGTON : 1999

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York	HENRY A. WAXMAN, California
CONSTANCE A. MORELLA, Maryland	TOM LANTOS, California
CHRISTOPHER SHAYS, Connecticut	ROBERT E. WISE, JR., West Virginia
ILEANA ROS-LEHTINEN, Florida	MAJOR R. OWENS, New York
JOHN M. McHUGH, New York	EDOLPHUS TOWNS, New York
STEPHEN HORN, California	PAUL E. KANJORSKI, Pennsylvania
JOHN L. MICA, Florida	PATSY T. MINK, Hawaii
THOMAS M. DAVIS, Virginia	CAROLYN B. MALONEY, New York
DAVID M. McINTOSH, Indiana	ELEANOR HOLMES NORTON, Washington, DC
MARK E. SOUDER, Indiana	CHAKA FATTAH, Pennsylvania
JOE SCARBOROUGH, Florida	ELIJAH E. CUMMINGS, Maryland
STEVEN C. LATOURETTE, Ohio	DENNIS J. KUCINICH, Ohio
MARSHALL "MARK" SANFORD, South Carolina	ROD R. BLAGOJEVICH, Illinois
BOB BARR, Georgia	DANNY K. DAVIS, Illinois
DAN MILLER, Florida	JOHN F. TIERNEY, Massachusetts
ASA HUTCHINSON, Arkansas	JIM TURNER, Texas
LEE TERRY, Nebraska	THOMAS H. ALLEN, Maine
JUDY BIGGERT, Illinois	HAROLD E. FORD, JR., Tennessee
GREG WALDEN, Oregon	JANICE D. SCHAKOWSKY, Illinois
DOUG OSE, California	
PAUL RYAN, Wisconsin	BERNARD SANDERS, Vermont (Independent)
HELEN CHENOWETH-HAGE, Idaho	
DAVID VITTER, Louisiana	

KEVIN BINGER, *Staff Director*

DANIEL R. MOLL, *Deputy Staff Director*

DAVID A. KASS, *Deputy Counsel and Parliamentarian*

CARLA J. MARTIN, *Chief Clerk*

PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois	JIM TURNER, Texas
THOMAS M. DAVIS, Virginia	PAUL E. KANJORSKI, Pennsylvania
GREG WALDEN, Oregon	MAJOR R. OWENS, New York
DOUG OSE, California	PATSY T. MINK, Hawaii
PAUL RYAN, Wisconsin	CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*

MATT RYAN, *Senior Policy Director*

BONNIE HEALD, *Communications Director/Professional Staff Member*

CHIP AHLSEWEDE, *Clerk*

TREY HENDERSON, *Minority Counsel*

## COMMITTEE ON SCIENCE

HON. F. JAMES SENSENBRENNER, JR., (R-Wisconsin), *Chairman*

SHERWOOD L. BOEHLERT, New York	RALPH M. HALL, Texas, RMM**
LAMAR SMITH, Texas	BART GORDON, Tennessee
CONSTANCE A. MORELLA, Maryland	JERRY F. COSTELLO, Illinois
CURT WELDON, Pennsylvania	JAMES A. BARCIA, Michigan
DANA ROHRABACHER, California	EDDIE BERNICE JOHNSON, Texas
JOE BARTON, Texas	LYNN C. WOOLSEY, California
KEN CALVERT, California	LYNN N. RIVERS, Michigan
NICK SMITH, Michigan	ZOE LOFGREN, California
ROSCOE G. BARTLETT, Maryland	MICHAEL F. DOYLE, Pennsylvania
VERNON J. EHLERS, Michigan*	SHEILA JACKSON-LEE, Texas
DAVE WELDON, Florida	DEBBIE STABENOW, Michigan
GIL GUTKNECHT, Minnesota	BOB ETHERIDGE, North Carolina
THOMAS W. EWING, Illinois	NICK LAMPSON, Texas
CHRIS CANNON, Utah	JOHN B. LARSON, Connecticut
KEVIN BRADY, Texas	MARK UDALL, Colorado
MERRILL COOK, Utah	DAVID WU, Oregon
GEORGE R. NETHERCUTT, Jr., Washington	ANTHONY D. WEINER, New York
FRANK D. LUCAS, Oklahoma	MICHAEL E. CAPUANO, Massachusetts
MARK GREEN, Wisconsin	BRIAN BAIRD, Washington
STEVEN T. KUYKENDALL, California	JOSEPH M. HOEFFEL, Pennsylvania
GARY G. MILLER, California	DENNIS MOORE, Kansas
JUDY BIGGERT, Illinois	VACANCY
MARSHALL "MARK" SANFORD, South Carolina	
JACK METCALF, Washington	

## SUBCOMMITTEE ON TECHNOLOGY

CONSTANCE A. MORELLA, Maryland, *Chairwoman*

CURT WELDON, Pennsylvania	JAMES A. BARCIA, Michigan**
ROSCOE G. BARTLETT, Maryland	LYNN N. RIVERS, Michigan
GIL GUTKNECHT, Minnesota*	DEBBIE STABENOW, Michigan
THOMAS W. EWING, Illinois	MARK UDALL, Colorado
CHRIS CANNON, Utah	DAVID WU, Oregon
KEVIN BRADY, Texas	ANTHONY D. WEINER, New York
MERRILL COOK, Utah	MICHAEL E. CAPUANO, Massachusetts
MARK GREEN, Wisconsin	BART GORDON, Tennessee
STEVEN T. KUYKENDALL, California	BRIAN BAIRD, Washington
GARY G. MILLER, California	

## EX OFFICIO

F. JAMES SENSENBRENNER, Jr., Wisconsin+	RALPH M. HALL, Texas+
---	-----------------------





## CONTENTS

---

	Page
Hearing held on October 22, 1999 .....	1
Statement of:	
Beedle, Ralph, senior vice president and chief nuclear officer, Nuclear Energy Institute .....	51
Miraglia, Frank, Deputy Executive Director for Reactor Programs, U.S. Nuclear Regulatory Commission .....	30
Rhodes, Keith, Director, Office of Computer and Information Technology Assessment, Office of Management and Budget .....	28
Willemssen, Joel, Director, Civil Agencies Information Systems, U.S. General Accounting Office .....	8
Letters, statements, etc., submitted for the record by:	
Beedle, Ralph, senior vice president and chief nuclear officer, Nuclear Energy Institute:	
Nuclear utility readiness information .....	78
Prepared statement of .....	53
Horn, Hon. Stephen, a Representative in Congress from the State of California:	
Letter dated December 18, 1998 .....	328
Prepared statement of .....	3
Miraglia, Frank, Deputy Executive Director for Reactor Programs, U.S. Nuclear Regulatory Commission, prepared statement of .....	33
Rhodes, Keith, Director, Office of Computer and Information Technology Assessment, Office of Management and Budget, prepared statement of .....	9
Turner, Hon. Jim, a Representative in Congress from the State of Texas, prepared statement of .....	5
Willemssen, Joel, Director, Civil Agencies Information Systems, U.S. General Accounting Office, prepared statement of .....	9



## **Y2K AND NUCLEAR POWER: WILL THE REACTORS REACT RESPONSIBLY?**

**FRIDAY, OCTOBER 22, 1999**

HOUSE OF REPRESENTATIVES, COMMITTEE ON GOVERNMENT REFORM, SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY, JOINT WITH THE COMMITTEE ON SCIENCE, SUBCOMMITTEE ON TECHNOLOGY,

*Washington, DC.*

The subcommittees met, pursuant to notice, at 10:13 a.m. in room 2318, Rayburn House Office Building, Hon. Stephen Horn (chairman of the Subcommittee on Government Management, Information, and Technology) presiding.

Present from the Subcommittee on Government Management, Information, and Technology: Representatives Horn, Turner, Mink, Biggert, Kanjorski, Ryan, Davis, Ose, and Maloney.

Present from the Subcommittee on Technology: Representatives Morella, Bartlett, Capuano, Baird, Gutknecht, Ehlers, and Udall.

Staff present from the Subcommittee on Government Management, Information, and Technology: George Russell, staff director and chief counsel; Matthew Ryan, senior policy director; Bonnie Heald, communications director and professional staff member; Chip Ahlswede, clerk; P.J. Caceres and Deborah Oppenheim, interns; Trey Henderson and Michelle Ash, minority counsels; and Jean Gosa, minority staff assistant.

Staff present from the Subcommittee on Technology: Jeff Grove, staff director; Ben Wu, professional staff member; Joe Sullivan, staff assistant; Michael Quear, professional staff member; and Mary Ralston, staff assistant.

Mr. HORN. A quorum being present, we will begin the hearing.

There are more than 430 nuclear power plants in the world, including 103 in the United States. Domestically, nuclear power plants provide an estimated 20 percent of the Nation's power supply. Regardless of the year 2000 computer challenge, safety has historically been a paramount concern at all U.S. nuclear facilities; however, the risk of even one failure at one plant is one too many.

Today we will hear from a panel of witnesses who will describe the work that has been done to mitigate the risk of a nuclear accident related to the year 2000 computer problem.

In December 1998, I and my colleagues, Congressman Dennis Kucinich, the former ranking member of the Subcommittee on Government Management, Information, and Technology, and Congressman Donald Manzullo wrote to the former chairman of the Nuclear Regulatory Commission expressing our concern over the Nuclear

Regulatory Commission's plan to perform detailed audits on only 10 percent of the Nation's 103 nuclear facilities. Because of the potentially devastating consequences of a nuclear accident, we strongly recommended that the audits be performed on all nuclear facilities. Our recommendation was rejected.

Today we want to be assured that the Nation's nuclear facilities are free of year 2000 risks. We want to provide an accurate portrayal of nuclear year 2000 readiness.

I welcome our panel of expert witnesses and look forward to their testimony.

[The prepared statement of Hon. Stephen Horn follows:]

DAN BURTON, INDIANA  
 CHAIRMAN  
 BENJAMIN A. GILMAN, NEW YORK  
 CONSTANCE A. MORELLA, MARYLAND  
 CHRISTOPHER DAVIS, CONNECTICUT  
 ILIANA ROSS-KHINTEN, FLORIDA  
 JOHN M. MANJOUK, NEW YORK  
 STEPHEN HORN, CALIFORNIA  
 Y. L. MCGA, FLORIDA  
 M. E. DAVIS II, VIRGINIA  
 O. M. MCINTOSH, INDIANA  
 MARK E. SOLDER, INDIANA  
 JOE SCARBOROUGH, FLORIDA  
 STEVEN C. LAYBURNETTE, OHIO  
 MARSHALL "MARK" SAMPFORD, SOUTH CAROLINA  
 BOB BARR, GEORGIA  
 DAN MILES, FLORIDA  
 ADA HUTCHERSON, ARKANSAS  
 LEE TERPIL, ILLINOIS  
 JUDY WIGGERT, ILLINOIS  
 OREG WALKER, OHIO  
 DOUG OSE, CALIFORNIA  
 PAUL BYAM, WISCONSIN  
 JOHN T. DOOLITTLE, CALIFORNIA  
 HELEN CHENOWETH, OHIO

ONE HUNDRED SIXTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
 COMMITTEE ON GOVERNMENT REFORM  
 2157 RAYBURN HOUSE OFFICE BUILDING  
 WASHINGTON, DC 20515-6143

MAJORITY (202) 225-6274  
 MINORITY (202) 225-6661  
 TTY (202) 225-6662

HENRY A. WADSWAL, CALIFORNIA  
 RANDOLPH MORTON, MISSISSIPPI  
 TOM LANTOS, CALIFORNIA  
 ROBERT E. WISE, JR., WEST VIRGINIA  
 MAJON A. OWENS, NEW YORK  
 EDUARD TONER, NEW YORK  
 PAUL E. MANOHARI, PENNSYLVANIA  
 GARY A. COSSETT, CALIFORNIA  
 PATSY T. MINK, HAWAII  
 CAROLYN B. MALONEY, NEW YORK  
 ELEANOR HOLMES NORTON,  
 DISTRICT OF COLUMBIA  
 CHAKA FATTAH, PENNSYLVANIA  
 ELIJAH E. COCHRANE, MARYLAND  
 CENNIS J. JACZONCH, OHIO  
 ROO R. BLAGOVICH, ILLINOIS  
 DANNY E. DAVIS, ILLINOIS  
 JOHN F. TERPNEY, MASSACHUSETTS  
 JIM TURNER, TEXAS  
 THOMAS H. ALLEY, MAINE  
 HAROLD E. FORD, JR., TENNESSEE  
 BERNARD SANDERS, VERMONT,  
 INDEPENDENT

**Opening Statement**  
**Chairman Stephen Horn (R-CA)**  
**Subcommittee on Government Management,**  
**Information, and Technology**  
**October 22, 1999**

There are more than 430 nuclear power plants in the world, including 103 in the United States. Domestically, nuclear power plants provide an estimated 20 percent of the nation's power supply. Regardless of the Year 2000 computer challenge, safety has historically been a paramount concern at all U.S. nuclear facilities. However, the risk of even one failure at one plant, is one too many.

Today, we will hear from a panel of witnesses who will describe the work that has been done to mitigate the risk of a nuclear accident related to the Year 2000 computer problem.

In December, 1998, I and my colleagues – Congressman Dennis Kucinich, the former Ranking member of the Subcommittee on Government Management Information, and Technology and Congressman Donald Manzullo – wrote to the former Chairman of the Nuclear Regulatory Commission, expressing our grave concern over the Nuclear Regulatory Commission's plan to perform detailed audits on only 10 percent of the nation's 103 nuclear facilities.

Because of the potentially devastating consequences of a nuclear accident, we strongly recommended that audits be performed on all nuclear facilities. Our recommendation was rejected. Today, we want to be reassured that all of the nation's nuclear facilities are free of Year 2000 risks, and we want to provide an accurate portrayal of nuclear Year 2000 readiness. I welcome our panel of expert witnesses, and look forward to their testimony.

Mr. HORN. Mr. Turner has official business that he's working on right now, and when he comes back his statement during the question period will be automatically part of the record.

[The prepared statement of Hon. Jim Turner follows:]

**STATEMENT OF THE HONORABLE JIM TURNER  
JOINT OVERSIGHT HEARING ON "Y2K AND NUCLEAR POWER:  
WILL REACTORS REACT RESPONSIBLY?"  
OCTOBER 26, 1999**

Thank you. Mr. Speaker, we know there is no margin for error when it comes to the Y2K problem and nuclear energy. We have an important responsibility to assure adequate protection of the public's health and safety. At each plant in the country, the Nuclear Regulatory Committee (NRC) has stationed resident inspectors who are carefully monitoring Y2K preparations in addition to conducting their regular oversight responsibilities. Also, specially trained NRC inspectors are to conduct formal on-site reviews of Y2K progress at each plant. According to the latest review by inspections, the NRC concluded that all 103 nuclear power plants in the U.S. will not be adversely affected by the Y2K problem.

While things appear to be on schedule here in the U.S., there is little validated information on potential Y2K problems in foreign nuclear facilities, including nuclear weapons facilities. The U.S. has been actively involved in trying to manage the worldwide nuclear weapons arsenal, particularly in Russia. A few weeks ago, the Pentagon, which fears that Y2K glitches could "blind" Moscow's missile-launch detection system or cause false alarms, announced the creation of the joint U.S.-Russia "Center for Year 2000 Strategic Stability" in Colorado Springs, Colorado. The Center will monitor U.S. and Russian early warning systems functions.

The purpose of this hearing is to assess the Y2K readiness of domestic and

international nuclear power plants. This hearing will focus on what issues remain with our domestic reactors to make them Y2K compliant and what risks persist with international Y2K nuclear facilities preparedness. Safety is our number one priority. It is my hope that we will be able to ascertain what we as a Congress can do to completely eliminate the possibility of Y2K malfunction in nuclear facilities, and I thank the Chairman for his focus on this issue.



Mr. HORN. Are there any statements that any of the Members would like to say at this time?

[No response.]

Mr. HORN. None. The vice chairman, Mrs. Biggert, the gentlewoman from Illinois.

Mrs. BIGGERT. Thank you, Mr. Chairman.

We have reached that critical point, with just under 70 days left before the new year, when systems work drills and contingency plans should be complete, but, as we are going to hear today, that might not be exactly true in the case of all the Nation's nuclear power plants, which is why this hearing on year 2000 nuclear power is so timely.

We have discussed Y2K's impact on commerce, government services, transportation, and life at home, but even if we address potential Y2K problems in these areas, none of these systems will work without electricity. By providing 20 percent of this country's electricity without contributing any air pollution, our nuclear power plants are vital to the stability of our electricity supply and the environment.

The issue of Y2K and nuclear power is particularly important to my home State of Illinois. There are about a dozen nuclear reactors located throughout the State, 10 of which serve the northern 20 percent of Illinois, including Chicago.

Commonwealth Edison, the owner of the 10 reactors serving northern Illinois, came before the Government Reform Committee's subcommittee at a field hearing in July in the district that I represent and reported that all nuclear stations were Y2K ready in July. So none of these plants are on the NRC's short list and never were, but we must remain concerned about the nine systems and seven reactors that aren't currently in compliance, and we must also be concerned about other sources of electricity.

American nuclear power plants don't operate in a vacuum. Commonwealth Edison admits that a failure at one of their surrounding utilities could have some impact on their systems.

So I want to thank the panelists for coming here today and updating us on the final preparations for Y2K, and I thank you, Mr. Chairman, for holding this hearing.

Mr. HORN. Thank you very much.

Does any other Member have an opening statement? The gentleman from Pennsylvania, the acting ranking member.

Mr. KANJORSKI. Mr. Chairman, I would like to ask unanimous consent that the statement of Mr. Turner be entered in the record.

Mr. HORN. Without objection, it will be placed in the record between my own opening statement and the vice chairman's opening statement.

Well, no other statements, let me now swear in the witnesses.

[Witnesses respond in the affirmative.]

Mr. HORN. Note that all four witnesses have affirmed.

The way we work is when we introduce you, your full statement is automatically in the hearing record. We'd like you to summarize it, not read it word for word, because we can read—but if you summarize the high points, that will give us more time for a dialog among the panel, as well as between the Members and the panel. So we will start with Mr. Willemssen, who is our regular presenter,

and the first one doing it. The U.S. General Accounting Office does a wonderful job for this subcommittee and all committees in the House.

Mr. Willemsen, it is good to see you. We have seen you all over the country this year, and we are glad to see you here in Washington.

Please give your presentation.

**STATEMENT OF JOEL WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, U.S. GENERAL ACCOUNTING OFFICE**

Mr. WILLEMSSEN. Thank you, Mr. Chairman and members of the subcommittees. Thank you for inviting GAO to testify today. As requested, we will summarize our statement.

Our Nation's nuclear power plants continue to make progress on their readiness for Y2K. Even with this progress, some risks remain. These risks include not knowing the current Y2K status of all 14 decommissioned plants with spent fuel, the lack of information on the consistency and extent of independent reviews of Y2K testing and emergency Y2K exercises, and the lack of requirements for day one planning, which is that series of events that should be planned for the end of December and the beginning of January.

To address these risks, we have developed a set of suggested actions for NRC to consider.

First, it is important that NRC know the status of all 14 decommissioned plants with spent fuel and report their status.

Second, NRC should determine what independent verification and validation efforts have been completed at nuclear power plants and determine whether additional reviews are needed.

Third, NRC should identify whether emergency contingency exercises performed by nuclear power plants have incorporated Y2K scenarios.

And, finally, we think it is especially important that NRC ensure that all facilities have developed day one plans. We have recently issued guidance in this area, which OMB has encouraged Federal agencies to use.

Let me next turn to Mr. Rhodes, GAO's Director for Computer and Information Technology Assessment, who will provide you with some detailed information on the risks of nuclear plants using a Powerpoint presentation.

Mr. Rhodes came to GAO from the Lawrence Livermore National Laboratory, one of two U.S. nuclear design labs. Since joining GAO, he has been heavily involved in nuclear energy issues such as stockpile stewardship, nuclear material tracking, and non-proliferation. So I will turn it over to Mr. Rhodes and we will see if we can have our slide show.

In addition, we have hard copies of the slides if the Members would like to follow along.

Mr. HORN. We would like to have those, and the clerk will get them and pass it out to the Members.

[The prepared statement of Mr. Willemsen and Mr. Rhodes follows:]

United States General Accounting Office

**GAO**

**Testimony**

Before the Subcommittee on Technology, Committee on Science, and the Subcommittee on Government Management, Information, and Technology, Committee on Government Reform, House of Representatives

For Release on Delivery  
Expected at  
10 a.m. EDT  
Friday,  
October 22, 1999

**Y2K COMPUTING  
CHALLENGE**

**Nuclear Power Industry  
Reported Nearly Ready;  
More Risk Reduction  
Measures Can Be Taken**

Statement of Joel C. Willemsen and Keith A. Rhodes  
Directors, Accounting and Information Management Division



Ms. Chairwoman, Mr. Chairman, and Members of the Subcommittees:

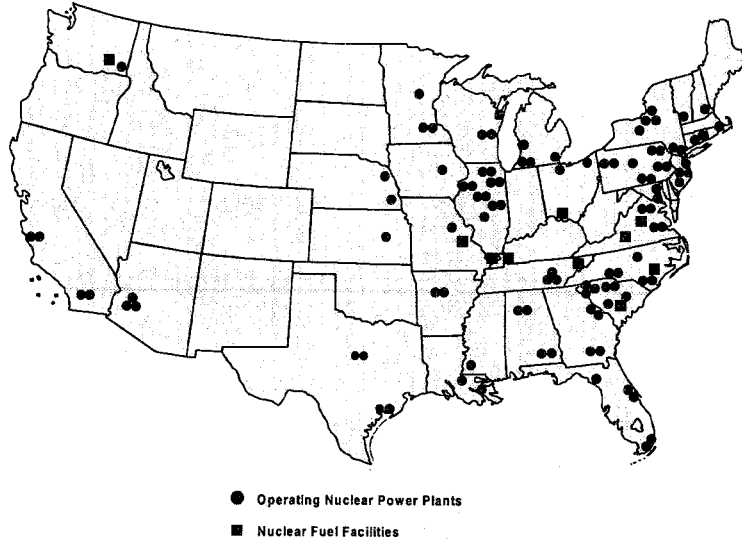
Thank you for inviting us to participate in today's hearing on the Y2K readiness of our nation's nuclear power industry. As with any industry, nuclear power plants must ensure that their systems are Y2K ready so that they can continue to operate and maintain an uninterrupted supply of electrical power. Given the nature of the nuclear power industry, a failure in systems could endanger safety and have potentially serious short- and long-term consequences.

As requested, after a brief background discussion, today we will (1) highlight the Y2K status of the nation's nuclear power industry; (2) discuss the Nuclear Regulatory Commission's (NRC) oversight of the industry's Y2K readiness; (3) provide an overview of the industry's contingency planning; and (4) comment on the international readiness of nuclear power plants.

#### BACKGROUND

Our nation's nuclear power industry currently consists of 103 operating nuclear power plants run by 41 licensees. According to NRC officials, an additional 19 nuclear power plants have been decommissioned and are no longer operating, although 14 of them continue to store highly radioactive spent nuclear fuel. Ten additional facilities fabricate nuclear fuel. As figure 1 shows, most of the 103 currently operating nuclear power plants and the 10 nuclear fuel facilities are located in the eastern part of the country.

Figure 1: Nuclear Power Plants and Nuclear Fuel Facilities in the United States



Source: NRC and the Nuclear Energy Institute.

Similar to other industrial facilities, nuclear power plants face a wide range of internal and external Y2K risks. Internal risks include the potential loss of reactor monitoring and control and the loss of emergency equipment and services, while external risks may include the loss of off-site electric power, water supply, critical consumables, and the loss of emergency equipment and services.

Probably the most serious external risks faced by a nuclear power plant are the potential instability of the electric power grid and the loss of off-site electric power. Such events may cause reactor shutdowns, and result in a loss of power or "station blackout." NRC studies show that a major contributor to reactor core damage occurrences is a station blackout event.

Figure 2: A Typical Nuclear Power Plant

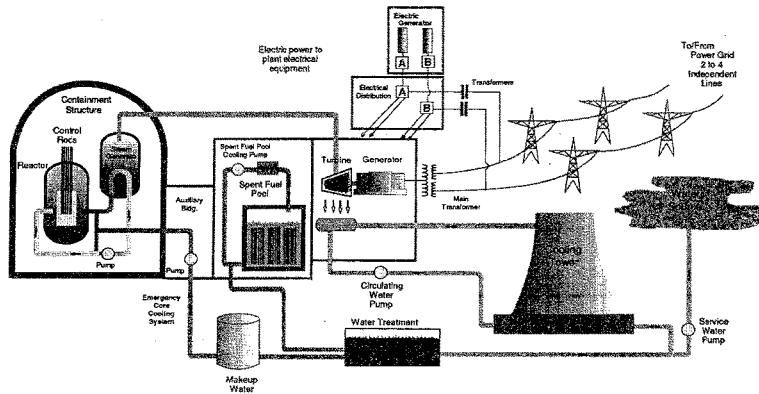


Figure 2 shows the key components of a typical nuclear power plant, and highlights the location of critical safety equipment such as the emergency core cooling pumps. Typically, nuclear power plants have emergency safety systems, including auxiliary feed water (water pumping) systems and standby emergency diesel generators, for cooling the reactors. Normally idle, these systems are designed to be activated during any emergency—such as loss of off-site power—that disrupts the reactor’s primary cooling systems.

Currently, all 103 operating nuclear power plants have active reactor cores and, along with 14 of the decommissioned plants, maintain on-site spent nuclear fuel pools. Both the reactor core and the spent fuel must be cooled to ensure that they are not exposed and release lethal radioactive material.

NRC licenses, regulates, and inspects the design, construction, and operation of domestic power plants and nuclear fuel facilities. It has established regulations for the safe operation of the 103 operational reactors, and requires nuclear reactors to have multiple safety systems to control and contain the radioactive materials used in each plant’s

operation. NRC also requires licensees to test and maintain safety equipment to ensure that this equipment, such as a reactor's emergency cooling system, will operate when needed.

The Nuclear Energy Institute<sup>1</sup> (NEI) has agreed to take the lead in developing industry-wide guidance for addressing the Y2K issue at nuclear power plants. NEI was also tasked by the North American Electric Reliability Council (NERC) with monitoring and reporting on the nuclear power industry's Y2K readiness. The Department of Energy has asked NERC to assess and report on the Y2K readiness of the electric power industry.

#### MOST U.S. NUCLEAR FACILITIES REPORTED TO BE YEAR 2000 READY

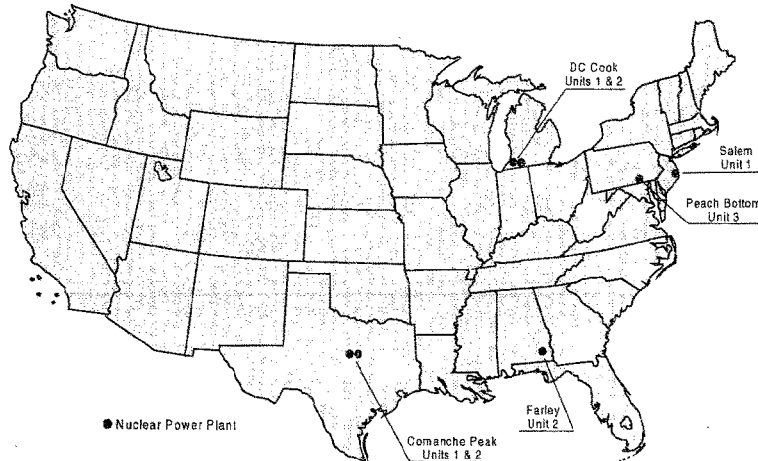
Last month, NRC reported that 75 of the 103 nuclear power plants were Y2K ready, and that all of the 103 operational nuclear power plants had resolved Y2K-related problems that could affect the performance of systems needed to safely shut down the plants. NRC tracks a plant's Y2K status based on the readiness of systems in three categories: (1) safety systems, which can affect plant protection and emergency shutdown; (2) plant operating and plant support systems; and (3) site support systems, such as administrative systems.

On October 4, 1999, NEI updated the industry's Y2K readiness status and reported that 96 of the 103 nuclear power plants were Y2K ready. According to NEI, for the other seven nuclear power plants—shown in figure 3—the safety systems are considered to be Y2K ready. NEI reported that three of these plants (Peach Bottom 3, Salem 1, and Farley 2) still have remediation work to complete on their plant operating and support systems, while another three (Cook 1 & 2, and Comanche Peak 2) have outstanding remediation work on their site support systems. The last plant, Comanche Peak 1, has remediation work to complete on both its plant operating and support systems and site support systems.

---

<sup>1</sup>NEI is a policy organization of the nuclear industry that seeks to foster and encourage the safe utilization of nuclear energy.

Figure 3: Seven Nuclear Power Plants Reported Not Y2K Ready as of October 4, 1999



Source: NEI.

Table 1 summarizes information provided by NEI on the scope of remediation work remaining at the seven plants classified by NRC as not yet Y2K ready. The table shows that all but two plants, Farley Unit 2 in Alabama and Comanche Peak Unit 1 in Texas, are scheduled to complete all remediation within the next 30 days.



Table 1: Scheduled Completion Dates for Non-Y2K-Ready Nuclear Power Plants as of October 4, 1999

Licensee	Plant(s)	Open Items	Scheduled Completion Date (1999)
<b>Plant Operating and Plant Support Systems</b>			
Philadelphia Electric Company	Peach Bottom 3	Digital Feedwater System	October 31
		Turbine Vibration Monitor	October 31
Public Service Electric and Gas	Salem 1	Advanced Digital Feedwater System	November 6
		Plant Computer Monitoring and Alarm System	November 6
		Overhead Annunciator System	November 6
Southern Nuclear Operating Company	Farley 2	Turbine Digital Electro Hydraulic System	December 16
Texas Utilities Electric	Comanche Peak 1	Condensate Polishing Programmable Logic Controller System	November 30
<b>Site Support Systems</b>			
American Electric Power	Cook 1 & 2	Meteorological Information and Dispersion Assessment System	October 30
Texas Utilities Electric	Comanche Peak 1 & 2	Plant Training Simulator	October 30

Source: NEI.

NRC is also responsible for nuclear safety at the decommissioned nuclear power plants operating spent fuel storage facilities. NRC said that it contacted these plants in early 1999, and at that time the plants reported either that their systems were Y2K ready or would be in the near term.

Six of the 10 nuclear fuel facilities reported to NRC that they were Y2K ready by September 1, 1999. The remaining four facilities have all provided NRC with status reports and schedules for remaining work, indicating that they will become Y2K ready by November 1, 1999. All of the nuclear fuel facilities, with the exception of two gaseous diffusion plants, have informed NRC that they plan to be shut down during the year 2000 rollover period.

NRC IS PROVIDING OVERSIGHT OF Y2K ACTIVITIES

Since 1996, NRC has been working with the nuclear power industry—and NEI—to address Y2K in the nuclear power industry. In December 1996, NRC notified all nuclear power plants and fuel facilities about the potential problems that nuclear facility computer systems and software might encounter during the transition from 1999 to 2000. This notification was followed in May 1998 by a letter to all operating nuclear power plant licensees requiring that they submit a written response by July 1999 stating how they planned to address the Y2K problem.

In 1997, NRC asked NEI to take the lead in developing industrywide guidance for addressing the Y2K problems faced by the nation's nuclear power plants. Responding to NRC's request, in October 1997 NEI published its Y2K guide.<sup>2</sup> In our comments<sup>3</sup> on the NRC Y2K approach and on NEI's guide, we noted that they did not adequately address risk management, business continuity and contingency planning, remediation of embedded systems, and independent verification and validation (IV&V) of systems. While NEI did not revise its guide in response to our comments, NRC informed nuclear power plants that the NEI approach and our own Year 2000 assessment guide<sup>4</sup> were approaches that plants might want to follow. NEI later addressed some of the issues we raised regarding its Y2K guide by issuing another guide<sup>5</sup> in August 1998 that focused on contingency planning and risk management.

Regarding reporting of Y2K readiness in 1998, NRC required all plants to report by July 1, 1999, to confirm if their facility was Y2K ready or would be by January 1, 2000. This request covered only the safety-related systems required by the plant license and NRC regulations. In January 1999 NRC expanded this reporting requirement to include plant operating and plant support and site support systems that, while not addressed by NRC

<sup>2</sup>Nuclear Utility Year 2000 Readiness (NEI/NUSMG 97-07, October 1997).

<sup>3</sup>Year 2000 Readiness: NRC's Proposed Approach Regarding Nuclear Powerplants (GAO/AIMD-98-90R, March 6, 1998).

<sup>4</sup>Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997; initially published as an exposure draft in February 1997).

<sup>5</sup>Nuclear Utility Year 2000 Readiness Contingency Planning (NEI/NUSMG 98-07, August 1998).

regulations for safe operation and shut down, are necessary for continuity of plant operations.

In January 1999 NRC completed audits of 12 Y2K programs involving 42 of the 103 operating nuclear power plants. Areas assessed included software applications and embedded systems and components. Information obtained during these assessments indicated that no significant Y2K problems existed in the plants' systems that would affect their ability to safely operate and shutdown.

In March 1999 NRC expanded the scope of its assessments efforts to include all 103 operating nuclear power plant sites. NRC administered to the 103 operational nuclear power plants a 452-question checklist covering items such as assignment of qualified personnel, testing for critical dates, and testing and validation of remediated software applications or embedded components. These assessments, completed by June 30, 1999, found that 14 of the 103 plants required additional follow-up reviews to more fully evaluate their Y2K programs. In the follow-up reviews, completed by August 13, 1999, NRC staff concluded that 13 of the 14 plants' Y2K programs were consistent with industry guidance. The last plant reported to NRC that it made its Y2K program consistent with the guidance in September 1999.

Regarding the decommissioned nuclear power plants, NRC has not issued specific Y2K guidance. However, it has notified the 14 plants with spent fuel on-site that they should follow the NEI Y2K guidance, and report on their Y2K readiness status. In early 1999, NRC also reviewed readiness activities at these 14 decommissioned plants that still have nuclear fuel. Through these reviews, NRC concluded that the licensees are implementing Y2K changes that address equipment and systems important to safety. At that time, the licensees reported that their computer systems were Y2K ready or would be in the near term. However, NRC does not know the current status for those decommissioned plants that previously reported they were not ready. Because of the risk posed by the spent fuel facilities at these sites, we believe that NRC should evaluate and report on the current Y2K status of these plants.

In June 1998 NRC required nuclear fuel facilities to report by December 31, 1998 whether the facility was Y2K ready. For facilities expecting to be ready at some point during 1999, NRC asked for a status report of remaining work, and another report by July 1, 1999. In addition, between September 1997 and October 1998, the major fuel facilities were asked Y2K-related questions during routine inspections. Based on these inspections, NRC concluded that the facilities were aware of the Y2K problem and were taking appropriate steps to address it.

NRC has not required that licensees perform an IV&V of their Y2K programs. Use of IV&V would provide NRC—and nuclear power plants and nuclear fuel facilities managers—with additional assurance that all critical applications and systems are Y2K ready. In March 1998, when commenting on NRC's proposed Y2K approach, we suggested that NRC require licensees to (1) describe their Y2K plans for IV&V of systems related to safety, and (2) provide the results of IV&V with their written certification of Y2K readiness. NRC has not included such a requirement in its Y2K instructions to licensees. In discussing this with NRC officials, they emphasized that a rigorous quality assurance program exists at each nuclear facility to review and validate modifications to safety systems. While we recognize this, such programs do not deal with the broader issue of Y2K testing of safety systems, or systems supporting plant and site operations.

Although we were told by NRC that some licensees obtained independent technical reviews of each nuclear facility's Y2K system test plans and results, NRC did not have specific, current information identifying which nuclear power facilities obtained independent reviews, or what those reviews entailed. NRC noted that the industry had reported in April 1999 that multiple audits were completed at 65 of the 103 nuclear power plants—56 by utility quality assurance departments, 36 by cross-utility audits, and 46 by third parties. However, neither NRC nor the industry issued guidelines establishing criteria to ensure consistency of reviews.

In the few months remaining, an opportunity exists for conducting targeted independent reviews of the licensees' Y2K programs. Since neither NRC nor NEI's guidance defined

the criteria for what constituted an independent review, it would be of value for NRC to survey the plants to gain an understanding of what independent reviews were completed. Based on this information, NRC could then identify plants that may need reviews.

YEAR 2000 CONTINGENCY PLANS DEVELOPED BY ALL FACILITIES,  
BUT COMPLETION OF PLAN TESTING UNCERTAIN

For many years, nuclear power plants have had contingency plans to deal with a wide range of threats, including earthquakes, tornadoes, and blackouts. Licensees have now had to modify these plans to address the Y2K threat and its accompanying risks, both internal and external.

NRC officials told us that nuclear power plants are following the contingency planning process guidance developed by NEI. This NRC-approved guidance recommended management controls, preparation of individual system contingency plans, and development of an integrated contingency plan that allows the utility to manage Y2K-induced risks.

Between May and June 1999, NRC reviewed the contingency planning activities of 12 operating nuclear power plants, looking at the implementation of NEI's guidance. All 12 plants' planning activities were found to be consistent with the guidance, and appropriate management and oversight was being provided. In light of these results and follow-up visits, NRC concluded that plants were acceptably implementing industry guidance, and therefore determined that such detailed reviews focusing specifically on contingency planning were not necessary at additional plants.

Concurrently, NRC had underway its assessment of Y2K readiness at all 103 plants, as previously discussed. The 452-question checklist NRC was using for this assessment included 52 questions covering areas of contingency planning. Such areas included internal and external facility risks and whether an integrated Y2K contingency plan—a compilation of individual contingency plans that included the remediation actions planned for key rollover dates—was developed. Based on these assessments, NRC

reported that all 103 nuclear power plants were using the NRC-approved industry guidance—guidance that included contingency planning—and that only one plant (Cooper Nuclear Station) had not yet completed its integrated contingency plan. NRC verified that this plant has since completed its plan.

While the nuclear power plants have reportedly completed Y2K contingency plans, it is unclear as to whether these facilities have validated their plans. NEI included validation as a step in its contingency planning process guidance to provide confidence that plans can be executed as intended. While NRC's assessment at the 103 plants included questions on whether the nuclear facility validated contingency plans, NRC has not summarized the results of each question from all plants and therefore does not know how many plants responded affirmatively that they had indeed tested their plans. Further, NRC did not assess how the plans were being validated.

The need for additional contingency preparation was also raised by public interest groups, most notably by the Nuclear Information and Resource Service. In December 1998, this group, concerned about the potential impact of Y2K problems on nuclear power plants, submitted three related petitions to NRC.

The first petition requested that all licensed nuclear facilities be shut down by December 1, 1999, if their safety systems were not Y2K compliant, and remain shut down until all repairs were completed. The second petition requested that NRC require nuclear power plant licensees to conduct a successful, full-scale emergency planning exercise involving the failure of computers or digital systems as a result of the Y2K problem, again asking that plants not doing so be shut down. The third petition asked that nuclear facilities have operational emergency diesel generators to provide backup power; that a 60-day supply of fuel for these generators be available; and that the licensees provide alternate means of backup power such as solar panels or wind turbines.

NRC denied all three petitions. While acknowledging the importance of the Y2K-related matters raised by the petitioners, it concluded that actions taken by nuclear plant licensees to address Y2K issues, coupled with NRC oversight, provided reasonable assurance of adequate protection of public health and safety. In responding on August 23, 1999, to the petition that NRC require nuclear power plants to conduct emergency planning exercises that cope with Y2K computer-related failures, NRC stated that this was not necessary because while the cause of computer and equipment failure may be different after December 31, 1999, the result and expected response would be the same as many situations encountered during emergency exercises and drills in the past. For example, NRC said in this response, it is typical in the development of scenarios for exercises and drills to assume that communications links, plant computers, and display and monitoring equipment will be out of service.

Because of the very nature of nuclear facilities, it is true that plants are already required by law to follow and maintain tested emergency plans.<sup>6</sup> These plans are to provide emergency response capabilities that take into account a variety of circumstances and challenges, and the facilities are required to exercise their plans periodically, develop and maintain key skills of involved personnel, identify deficiencies in their emergency plan and personnel, and take appropriate action to correct identified deficiencies. However, it is unknown whether or not each plant has recently tested, through normal emergency exercises, scenarios addressing potential Y2K-induced failures. Therefore, given the known Y2K threat to nuclear facilities, we believe that NRC should obtain information on the scope and extent of nuclear power plants' emergency exercises, and whether these exercises have incorporated Y2K scenarios.

Regarding the nuclear fuel facilities, NRC has not required these facilities to develop specific Y2K contingency plans. However, 8 of the 10 fuel facilities have informed NRC that they plan to be in safe shutdown during the transition to Y2K, and NRC inspections at the other two facilities found their contingency plans to be acceptable. For decommissioned plants, NRC applied the same requirements for the 14 plants with spent

---

<sup>6</sup>10 CFR 50.47, 10 CFR 50.54 paragraphs (q), (s), and (t); and Appendix E to 10 CFR Part 50.

fuel as it did for the 103 operating plants. NRC could not say how many of the decommissioned plants completed contingency plans, as the agency had not reviewed them because NRC staff concluded that Y2K issues were highly unlikely to cause a potential threat to public health and safety at such plants. NRC also noted that decommissioned plants have an extended amount of time to take relatively simple corrective actions should Y2K failures occur.

Another important area that needs to be addressed is Day One planning. Each nuclear facility needs to develop a Day One strategy—a comprehensive set of actions to be executed by nuclear facilities during the last days of 1999 and the first days of 2000. We have recently issued Day One planning guidance that the Office of Management and Budget has encouraged federal agencies to use.<sup>7</sup>

No Day One guidance has currently been issued by the industry on what plants should be doing during the end of December and beginning of January 2000. NRC officials told us that nuclear power plants have taken certain actions to be ready for the Y2K rollover, such as requiring additional staffing and stockpiling consumables (i.e., diesel fuel for emergency diesel generators). However, these do not entail a comprehensive set of actions to be carried out systematically by every operational nuclear power plant. The actions that the nuclear power plants and fuel facilities take during this time will be just as critical as actions already taken to become Y2K ready. Accordingly, we believe that NRC should ensure that all nuclear facilities have developed appropriate Day One plans.

#### LITTLE IS KNOWN ABOUT WORLDWIDE YEAR 2000 READINESS OF NUCLEAR POWER PLANTS

Little current data are available on the Y2K readiness of the 331 nuclear power plants operating outside the United States. Figure 4 shows that 31 other countries besides the United States are operating nuclear power plants. Nine of these countries have more than ten nuclear plants each, for a total of 252 plants. The remaining 22 countries each have

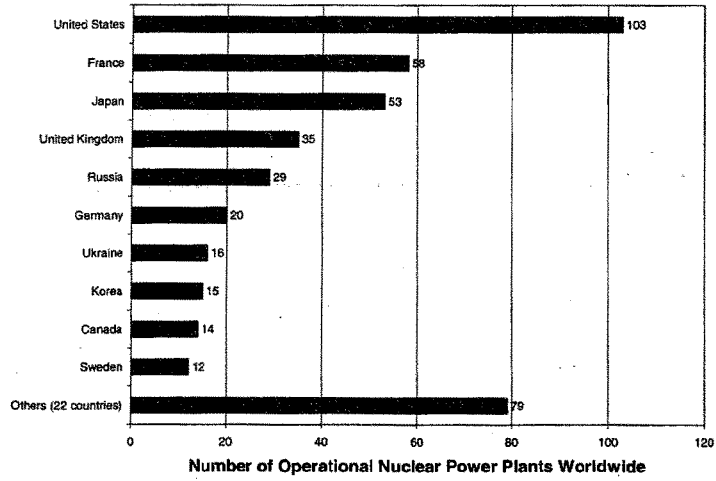
---

<sup>7</sup>Y2K Computing Challenge: Day One Planning and Operations Guide (GAO/AIMD-10.1.22, October 1999).



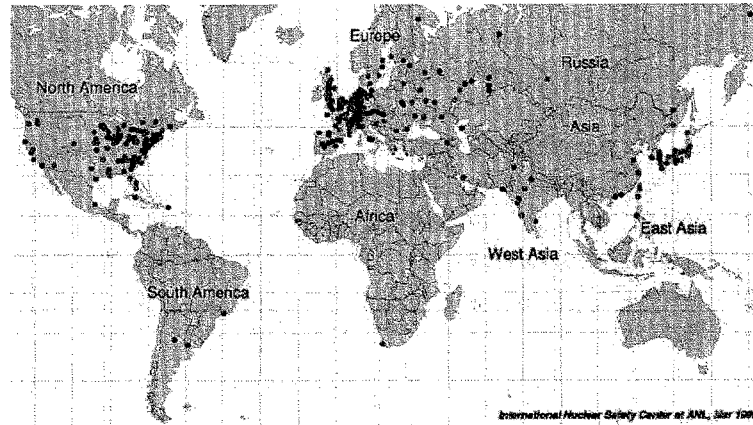
10 or fewer, for a total of 79 plants. Figure 5 shows the location of operational nuclear power plants worldwide.

Figure 4: Ten Largest Nuclear Power Producers Worldwide



Source: International Atomic Energy Agency.

Figure 5: Location of Nuclear Power Plants Worldwide



Source: International Nuclear Safety Center, Argonne National Laboratory.

What information is available suggests that several other countries are taking steps to ready their nuclear power plants for the change of century. For example, the International Atomic Energy Agency (IAEA) has been working with its 128 member states to ensure that they are informed of the Y2K problem. The agency has published guidelines for its members' use in addressing safety and operability concerns, and has sponsored international workshops in January and July of this year to provide assistance to members on the challenge of the Y2K issue. Based on information exchanged at these workshops, several countries reported that they were on their way to readying their nuclear power plants for 2000.

Similarly, the Nuclear Energy Agency (NEA) has been working with its 27 member countries<sup>8</sup>—representing 85 percent of the world's nuclear power capacity—to ensure awareness of nuclear safety during the transition to 2000. In February 1999, during

<sup>8</sup> Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

NEA's workshop on the impact of Y2K on the nuclear industry, some participants—including those from Canada, France, Japan, Spain, and Sweden—reported that most of their plants would be Y2K ready by July 1999.

However, other countries appear to be behind the United States. For example, the Russian representatives at the NEA workshop noted that their State Regulatory Authorities of Nuclear Energy and the Federal Nuclear and Radiation Authority of Russia were still studying the impact of Y2K on the nuclear power industry. They also noted that some facilities and organizations do not probably fully appreciate the impact of Y2K on the nuclear power industry for their nuclear facilities.

Similar concerns were raised by the National Intelligence Officer<sup>9</sup> for Science and Technology during the January 1999 hearing on the Y2K readiness of federal, state, local, and foreign governments before the Subcommittee on Government Management, Information, and Technology, House Committee on Government Reform. Testifying on the intelligence community's assessment of foreign Y2K efforts, he noted that both Russia and the Ukraine had exhibited a low level of Y2K awareness and remediation activity, and that while Russia possessed a talented pool of programmers, they seemed to lack the time, organization, and funding to adequately confront the Y2K problem. He noted that there were concerns about problems with computer-controlled systems and subsystems within power distribution systems and nuclear power generating stations leading to reactor shutdowns, or improper power distribution resulting in loss of heat for indeterminate periods in the dead of winter in Russia.

It should be noted that NRC—with cooperation from NEA and IAEA—is developing a prototype of an international Y2K early warning system. This Internet-based system would be used by NRC and other regulators to share information concerning Y2K problems that affect plant operation, telecommunications, or grid reliability. To date, this effort includes mainly Canada, Europe, Mexico, and Far Eastern countries.

---

<sup>9</sup>Statement of Lawrence K. Gershwin, National Intelligence Officer for Science and Technology, National Intelligence Council, before the Subcommittee on Government Management, Information, and Technology, Committee on Government Reform, January 20, 1999.

In summary, while progress has been made in making the nation's nuclear power plants and fuel processing facilities Y2K ready, some risk remains. At particular risk are the seven plants that do not yet have their non-safety systems ready, especially the two with completion dates scheduled for more than 30 days from now, ever closer to the turn of the century. Similarly, the four nuclear fuel facilities that were not Y2K ready by September 1, 1999, raise concern. Likewise, not knowing the current Y2K status of all 14 decommissioned plants with spent fuel also raises concern. Finally, the lack of information on two key issues—*independent reviews of Y2K testing and emergency Y2K exercises*—and the lack of requirements for Day One planning increases the Y2K risk to the nuclear power industry.

To further reduce risks, NRC and the nuclear power industry can still take specific actions to ensure Y2K-related plant safety. First, NRC should evaluate and report on the Y2K status of all decommissioned plants with spent fuel status that previously reported they were not Y2K ready. Second, NRC should survey the 103 operational nuclear power plants to gain an understanding of what independent reviews were completed. Based on this information, NRC could then identify plants that may need additional reviews. Third, it should obtain information on the scope and extent of nuclear power plants' emergency exercises, and whether these exercises have incorporated Y2K scenarios. Finally, NRC should ensure that all nuclear facilities have developed Day One plans.

Ms. Chairwoman, Mr. Chairman, this concludes our statement. We would be happy to respond to any questions that you or other members of the Subcommittees may have at this time.

**Contact and Acknowledgments**

For information about this testimony, please contact Joel Willemsen at (202) 512-6253 or Keith A. Rhodes at (202) 512-6412, or by e-mail at [willemsenj.aimd@gao.gov](mailto:willemsenj.aimd@gao.gov) or [rhodesk.aimd@gao.gov](mailto:rhodesk.aimd@gao.gov). Individuals making key contributions to this testimony included Mirko Dolak, Troy Hottovy, William Isrin, Janet Jamison, and Michael Tovares.

(511799)

**STATEMENT OF KEITH RHODES, DIRECTOR, OFFICE OF COMPUTER AND INFORMATION TECHNOLOGY ASSESSMENT, OFFICE OF MANAGEMENT AND BUDGET**

Mr. RHODES. Mr. Horn, members of the subcommittee, thank you very much for inviting me here today. I would just briefly like to discuss a few slides that can help illustrate some of the issues we discussed in our testimony.

The first slide shows the distribution of U.S. domestic nuclear power plants and their associated fabrication sites. The blue dots are the plants themselves, and the green squares are the fabrication sites.

The difference is that a nuclear plant generates electricity, while the fabricating plant generates fuel used by the power plant.

As of last Friday, there were only two plants, according to the Nuclear Energy Institute, that are not Y2K ready. One is Peach Bottom and the other is Farley. Peach Bottom is currently going through their final testing. Farley is in an outage now and they are doing their Y2K remediation and should be done by December.

Mr. HORN. Where are those plants located?

Mr. RHODES. Peach Bottom is in Pennsylvania and Farley is in Alabama. If I can point it out on the large board, you see Peach Bottom at the top in Pennsylvania and Farley unit No. 2 is down in Alabama.

The next slide shows a typical nuclear power plant. We are talking about the plant here, as opposed to the reactor, itself. This is actually a pressurized water reactor, but there are also boiling water reactors and other kinds of reactors—light water, heavy water.

The areas that have to be watched under any circumstances, not just Y2K, are as follows.

The grid itself, which brings in offsite power. In nuclear terms, a failure here is called a "LOOP," a loss of offsite power, and is very important because it is the main power source for the plant to keep their systems running.

Backup diesel generators are important, since if a LOOP occurs the generators need to kick in to provide backup power to run the plant. There are typically two diesel generators, although a few plants have hydroelectric sources for backup. This gives a higher degree of assurance that if one generator fails the second one can take over. It is a redundancy in their diesel systems.

There has been much discussion about the reliability of these emergency diesel generators. Some claims are that the generators do not even meet 70 percent reliability, let alone their design requirement of 97.5 percent; however, according to a study by the Idaho National Engineering Laboratory, the generators meet their 97.5 percent requirement, and the lower reliability ratings are due to anomalous conditions occurring during routine maintenance—that is, while you have taken the generator off-line, then you have a power need, and that is why you are getting these lower reliability percentages. Sometimes people will come in and say they are only 70 percent reliability.

Routine maintenance—we have had discussions with both power plants as well as NRC and NEI. Routine maintenance is not going

to occur on the roll-over date, so our assumption is that the 97.5 percent reliability will be met by the diesel generators.

Next in the cycle of importance are the pumps, themselves. The pumps are a key system, since they make certain that the water is flowing throughout the plant to keep the reactor itself cool, as well as the support systems for electricity generation. You see there are pumps throughout the system.

The reactor itself, of course, is a key system, and its security systems are key, since that is the site of the fission reaction that generates the heat. Circulating water that continuously transfers heat from the core to the steam generation system cools the reactor core.

Finally, the spent fuel pools need to have a continuous source of water, since the spent fuel does not cool down immediately and continues to fission at some low level for a long time after it has been removed from the reactor, itself.

Again, to reiterate, the next slide shows those plants that are not yet Y2K ready, and that is as of Friday. NEI reported that D.C. Cook one and two are now ready, and that Farley and Peach Bottom—Peach Bottom, as I stated, is currently going through its testing, and Farley is in an outage and being renovated.

The next slide shows a simple risk assessment box, four quadrants that show the relation between probability of failure and impact of failure. As you can see, the upper right-hand quadrant is rated as high/high—high probability of failure and high impact of failure.

If you have devices that are sitting up in the upper right-hand corner, the objective is to drive those devices down into the lower left-hand corner into a low probability of failure and low impact of failure.

You reduce the probability of failure by doing remediation and replacement of the system, and you reduce the impact by doing contingency and continuity of operations planning, the objective being to move those systems into the low/low quadrant so that there is low impact and low probability of failure.

Any risk assessment and risk management process, not just Y2K, is going to attempt to drive the risk from high to low, both in terms of probability and impact. The probability is reduced, as I said, through remediation and replacement, and the impact is reduced through contingency and continuity planning.

Turning to international nuclear power, as you can see from this chart, if you have very good eyes, the United States leads the world in nuclear power plants, even though we do not get as high a percentage of our domestic power from nuclear as other countries such as France.

The point here is that not just the United States has to be Y2K ready, the world has to be Y2K ready.

Finally, this slide shows the distribution of nuclear power plants worldwide. As you can see, some plants are in rather remote locations, but most are not.

As you are well aware, the former Soviet Union countries are the most worrisome to nuclear power experts, myself included.

That concludes my, unfortunately, a little longer than brief introduction. I would appreciate any questions the committee has.

Mr. HORN. Actually, we will wait until we complete the whole panel and then we will start asking questions.

We now have a key witness from the Nuclear Commission, and that is Mr. Frank Miraglia, Deputy Executive Director for Reactor Programs, U.S. Nuclear Regulatory Commission.

Mr. Miraglia.

**STATEMENT OF FRANK MIRAGLIA, DEPUTY EXECUTIVE DIRECTOR FOR REACTOR PROGRAMS, U.S. NUCLEAR REGULATORY COMMISSION**

Mr. MIRAGLIA. Thank you, Chairman Horn and members of the committee. I'm pleased to be here today on behalf of the Nuclear Regulatory Commission to report the year 2000 readiness of the Nation's nuclear power plants.

Based upon our review of the responses from the nuclear power industry concerning year 2000 readiness, our independent inspection efforts at all 103 operating plants, and our ongoing regulatory oversight activities, we have concluded that the year 2000 problem will not adversely affect the continued safe operation of the Nation's nuclear power plants.

Starting in December 1996, we engaged our industry stakeholders on the development of guidance to deal with the year 2000 problem. The draft guidance was issued for comment. The GAO reviewed the draft guidance and provided comments. Their comments were particularly helpful, many of which were considered in the NRC's endorsement of the final guidance.

These industry guidelines were endorsed and subsequent NRC audits and inspections of our licensees' programs enabled us to independently assess the effectiveness of year 2000 readiness at each nuclear power plant.

Regarding our highest priority, the uninterrupted performance of plant safety systems, all 103 nuclear power plants report that their Y2K readiness efforts are complete.

As of October 20th—there will be some difference in numbers, based upon the dates—99 of these plants also determined that all of their computer systems that support plant operations are Y2K ready and that contingency plans were in place. The remaining four plants have additional work on non-safety-related systems.

As you heard Mr. Rhodes say, NEI has reported that the Cooks units are completed. We haven't formally received a letter, but we understand that is the status of the Cook stations.

These plants are on target to complete the remaining modifications in advance of the year 2000 transition period.

Based on our information as of November 1st, only one plant will have year 2000 readiness work remaining. That station is Farley Two located in Alabama. That plant entered a shut-down on October 15th. It will have the modifications installed and off-line testing completed by mid-November. In order to declare total readiness, it will be waiting startup, which is projected for mid-December.

The work remaining involves non-plant support systems and an outage, as required. These outages are scheduled, the readiness has been planned, and the work has been successfully completed on a sister unit.



During late 1998 and early 1999, the NRC conducted audits of plant-specific Y2K programs and contingency plans at our licensees' facilities. Based upon these audits, we developed an inspection protocol in which all 103 reactors with Y2K programs would be reviewed.

Based on these oversight activities, we have not identified any issues that would preclude licensees from achieving year 2000 readiness. We will continue to monitor nuclear power plant readiness as year 2000 approaches.

Concerns have been expressed about the inability or loss of electrical distribution grid during Y2K critical dates. According to the North American Electric Reliability Council, NERC's latest report, more than 99 percent of the Nation's electricity supply is classified as Y2K ready, or Y2K ready with limited exceptions.

NERC states that the Y2K transition should have minimal impact on electrical systems operations in North America and that widespread, long-term loss of the grid as a result of Y2K-induced events is not likely.

Notwithstanding, the NRC has focused its attention on assuring reliable emergency power would be available to nuclear power plants. The scope of our licensees' Y2K programs, including contingency planning, covers the onsite power and other emergency power systems, such as the electrical diesel generators.

NRC audits and inspections have verified licensees' considerations of those systems, and no associated Y2K issues related to onsite or emergency power systems have been identified.

Regulatory requirements provide high confidence in diesel generator operability, availability, and reliability. Additionally, diesel generator reliability in emergency situations has been high, as demonstrated during weather-related power upsets.

We have also focused on spent fuel cooling systems to assure cooling of spent fuel stored at shut down facilities. The majority of spent fuel cooling systems are based on analog controls, and therefore not subject to Y2K problems.

At the shut down facilities, only 14 have spent fuel remaining onsite. The heat generated by this spent fuel reduces with time, thus increasing the time available for operators to take actions to mitigate any off-normal circumstances.

Existing procedures and operator training at these facilities allow the licensee to deal with normal and off-normal situations such as loss of offsite power, and the plant staff would have time to control these functions.

Notwithstanding these preparations, nuclear power plant licensees have developed contingency plans for each plant to cope with year 2000 problems.

Based upon our inspections and audits, we have determined that all power plants have also developed day one strategies as part of the development of their year 2000 contingency plan.

The NRC has also developed an agency contingency plan to respond to unforeseen events related to year 2000 problems that could potentially affect one or more of our licensees. The plan has been coordinated and communicated with other Federal agencies, as well as provided to the public for comment.

We conducted a full-scale exercise on October 15th involving 11 nuclear power plants and three fuel facilities to further validate the NRC's contingency plan. The exercise was a success, and we gained valuable insights to further improve our readiness for the potential year 2000 transition.

The NRC remains committed to keeping our stakeholders and the general public informed. We have posted our generic communications, audits, and reports on our external-internal website for access by members of the public.

In conclusion, we have been active in addressing the year 2000 problem, both internally and with our licensees. We will continue to work both nationally and internationally to promote awareness of Y2K problems. Our efforts have established a framework that appreciably ensures that the Y2K problem will not have an adverse impact on the ability of the nuclear power plants to safely operate or safely shut down during the year 2000 transition.

Thank you. That completes my statement.

Mr. HORN. Thank you very much. That is a very helpful statement.

[The prepared statement of Mr. Miraglia follows:]

STATEMENT SUBMITTED  
BY THE  
UNITED STATES NUCLEAR REGULATORY COMMISSION  
TO THE  
SUBCOMMITTEE ON TECHNOLOGY  
COMMITTEE ON SCIENCE  
AND THE  
SUBCOMMITTEE ON GOVERNMENT  
MANAGEMENT, INFORMATION, AND TECHNOLOGY  
COMMITTEE ON GOVERNMENT REFORM  
U.S. HOUSE OF REPRESENTATIVES

Y2K AND NUCLEAR POWER:  
WILL REACTORS REACT  
RESPONSIBLY?

SUBMITTED BY  
FRANK J. MIRAGLIA  
DEPUTY EXECUTIVE DIRECTOR FOR REACTOR PROGRAMS

October 22, 1999

U.S. NUCLEAR REGULATORY COMMISSION  
TESTIMONY ON YEAR 2000 AND NUCLEAR POWER PLANTS

**Introduction**

Madame Chairwoman and Mr. Chairman, members of the Committee, I am pleased to submit this testimony on behalf of the Commission regarding the Year 2000 (Y2K) readiness of the U.S. nuclear industry and the NRC's internal Y2K readiness preparations. Based on our review of responses from the nuclear power industry concerning Y2K readiness, our independent inspection efforts at all 103 units, and our ongoing regulatory oversight activities, we conclude that the Y2K problem will not adversely affect the continued safe operation of U.S. nuclear power plants.

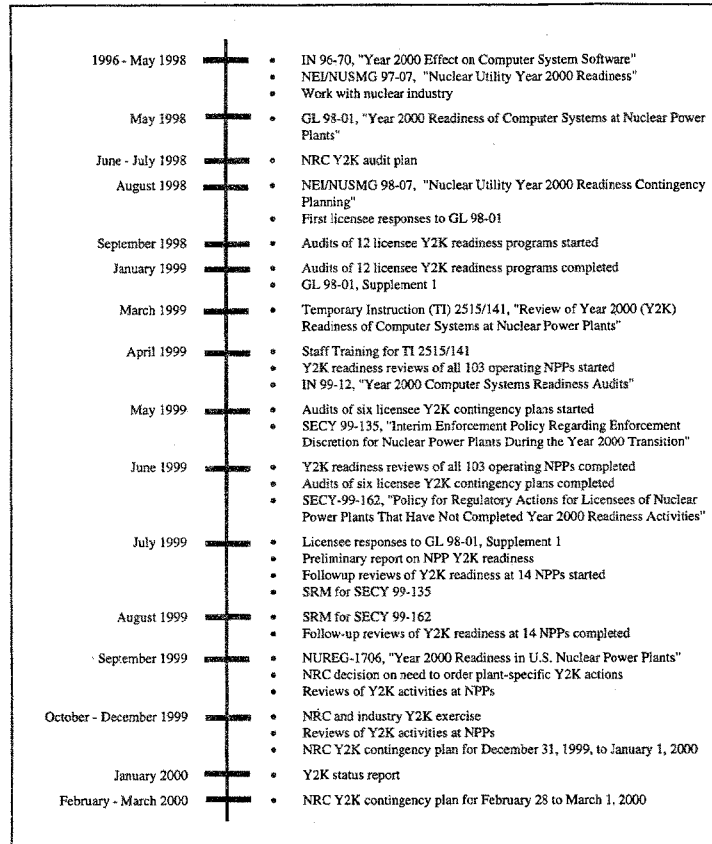
The Y2K problem has presented the NRC with a unique challenge, because NRC regulatory oversight and authority does not extend to the U.S. offsite electrical grid system. Nonetheless, we recognize the national importance of a broader focus that helps to ensure that potential concerns with electrical grid reliability are identified and resolved. 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 reliable grid operation in the face of the Y2K problem as well.

**NRC Actions With Reactor Licensees**

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

Since then (as depicted in the time line that follows), the NRC has been working with nuclear industry organizations and licensees to address issues related to transition into the next century. In 1997, the Nuclear Energy Institute (NEI) agreed to take the lead in developing

## TIMELINE OF SIGNIFICANT NRC Y2K REGULATORY ACTIVITIES



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). This document provides a step-by-step method to identify, test, and repair potential Y2K computer problems and contains detailed procedures and checklists for resolving Y2K issues, based on the best utility practices available. The NRC subsequently accepted this guidance as an appropriate program for nuclear power plant Y2K readiness.

In Generic Letter 98-01, issued in May 1998, the NRC formally accepted the NEI/NUSMG 97-07 guidance as an appropriate program for nuclear power plant Y2K readiness. GL 98-01 requested written responses from each operating U.S. nuclear power plant licensee, to confirm that the Y2K problem was being addressed effectively. All licensees initially responded in August 1998, stating that they had adopted plant-specific programs intended to make the plants "Y2K Ready" by July 1, 1999. The licensees' Y2K programs include both the onsite backup power and the alternate ac power systems that are covered by the terms and conditions of the license and NRC regulations. GL 98-01 also required written confirmation of Y2K readiness no later than July 1, 1999, or, for licensees not Y2K ready by that date, a status report and schedule for the remaining work needed to ensure timely Y2K readiness.

On January 14, 1999, the NRC issued Supplement 1 to GL 98-01, providing an alternative to the response required by GL 98-01. The alternate response, also due by July 1, 1999, was to voluntarily include a broader spectrum of information on the overall Y2K readiness of the plant, including those systems necessary for continued plant operation that are not covered by the terms and conditions of the license and NRC regulations. By July 1, 1999, all licensees of operating nuclear plants had responded to the request in GL 98-01, Supplement 1. A summary of the reports was posted on the NRC external web site at <http://www.nrc.gov/NRC/Y2K/plantstatus.html>, and this status is routinely updated.

---

<sup>1</sup> A computer system or application is defined as "Y2K Ready" when it has been found suitable for continued use into the Year 2000, even if it has not been made fully Y2K Compliant ("Y2K Ready" systems will continue to function correctly). "Y2K Compliant" means that the computer systems or applications will accurately process date/time (including but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, the years 1999 and 2000, and leap-year calculations.

At this time, we are not aware of any Y2K problems in nuclear power plant systems that directly impact performance of safety systems. The majority of commercial nuclear power plants have protection systems that are analog rather than digital or software-based, and thus are not impacted by the Y2K problem. Errors such as incorrect dates in print-outs, logs or displays have been identified and corrected by licensees in some safety-related devices, but these errors have not affected the functions performed by the devices or systems. Most Y2K issues are in non-safety systems such as security systems and plant monitoring systems which support day-to-day plant operation but have no functions necessary for reactor safety. These systems are being addressed in the licensee Y2K readiness programs, in a manner consistent with the industry guidance and GL 98-01 schedule.

As you know, in ensuring public health and safety across the full range of our regulatory programs, we rely on both our own independent oversight and the recognized ability of our licensees to complete critical self-assessments and to initiate appropriate corrective actions. In the Y2K readiness arena, in addition to the comprehensive industry efforts, we have recognized the importance of providing an appropriate level of NRC oversight of nuclear power plant Y2K preparations.

One such NRC initiative was to audit, on a sample basis, the plant-specific Y2K programs at 12 nuclear power plant sites. The audit sample included a variety of plants of different ages, types, and locations, to provide an effective evaluation of Y2K readiness program implementation. These audits were completed in January 1999. Based on the results, we concluded that licensees were taking effective actions to achieve Y2K readiness by the GL 98-01 target date. We did not identify any issues that would preclude licensees from achieving Y2K readiness. These findings were consistent with those reported by the Department of Energy in the August 1999 report prepared by the North American Electric Reliability Council on the status of Y2K readiness of the electric power grid.

NRC audit results were reported on the NRC web site and discussed at industry workshops. In April 1999, we communicated a summary of audit observations and lessons learned through NRC Information Notice 99-12. The audit results indicated several common factors among effective programs. We found that following the industry guidance documents resulted in an overall functional and effective Y2K readiness program. In addition, we found that active management oversight is important and that central control of Y2K activities, independent peer reviews, and aggressive quality assurance involvement promoted consistency across program activities and products. Further, it was helpful for licensees to share information via owners' groups and utility alliances.

In NRC Generic Letter 98-01, we had also noted that despite the best of efforts to achieve Y2K readiness, unanticipated problems (particularly external events) could disrupt continued plant operation, and contingency plans were needed to deal with these 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). This document provided guidance for establishing a contingency planning process that included management controls, preparation of individual contingency plans, and development of an integrated contingency plan that allows the licensee to manage risks associated with Y2K-induced events internal and external to the plant. This guidance, which was found acceptable by the staff, has been incorporated into Y2K readiness programs by all U.S. nuclear power plant licensees. Plant-specific Y2K contingency plans were also developed.

The January 1999 audit results indicated that licensees began to develop contingency plans late in the Y2K preparation process. Consequently, we concluded that six additional reviews were needed, focused differently and involving licensees other than the previous 12, to determine the effectiveness of licensee contingency planning. These reviews, which were completed in June 1999, focused on the licensees' approach to addressing both internal and external Y2K risks to safe plant operations based on the guidance in NEI/NUSMG 98-07. The results of these additional audits indicated that licensees had developed effective contingency planning for reducing the risks associated with Y2K-induced events. The results of these audits were also placed on the NRC's Y2K web site.

To gain additional confidence that nuclear power plant licensees were effectively implementing Y2K readiness programs, NRC regional staff reviewed plant-specific Y2K program implementation activities, including contingency planning, at all 103 NRC-licensed commercial nuclear power plant facilities. These inspection activities were completed between April and June 1999 and provided an independent assessment of licensee Y2K readiness programs. The results of these inspections were used as a benchmark to compare with licensee responses to Generic Letter 98-01 Supplement 1, and to provide an informed approach for determining any further regulatory responses. In early September NRC published NUREG-1706, "Year 2000 Readiness in U.S. Nuclear Power Plants," providing detailed information on plant readiness, remaining work to be done, and staff activities. Copies have been provided to the Committee and placed on the NRC Y2K Web site.

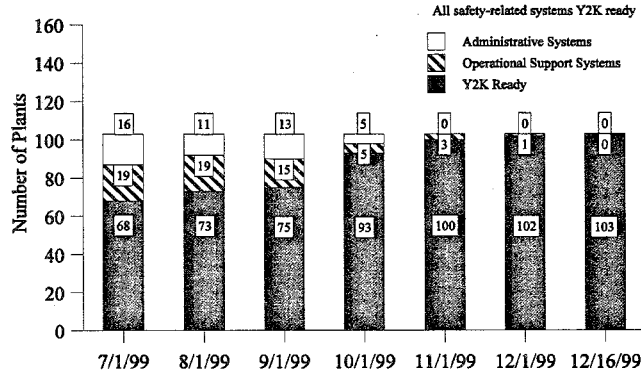


**Current Status of Nuclear Power Industry Year 2000 Readiness**

Regarding our highest priority—the uninterrupted performance of plant safety systems—all 103 nuclear power plants report that their efforts are complete, and that no remaining Y2K-related problems exist that could directly affect the performance of safety systems or the capability for safe shutdown. As of September 30, 91 plants had completed the next order of priority, reporting that all of their computer systems that support plant operation are “Y2K ready and that contingency plans were in place.” The remaining 12 plants reported that, to be fully Y2K ready, they still had additional work to complete on a few non-safety computer systems or devices, i.e., systems that could affect power operations or plant monitoring or are administrative. Typically, the remaining Y2K work is waiting on a scheduled plant outage in the fall, or is delayed while awaiting the delivery of a replacement component. In each case, the licensees with Y2K work remaining provided satisfactory schedules for completing that work.

During September, 18 additional nuclear power plants completed their Y2K readiness activities. Late last month, the staff sent letters to the 12 licensees of the plants that were not expected to be Y2K ready on non-safety systems by September 30 to confirm their completion schedules and tasks for the remaining work. These plants include Comanche Peak Units 1 & 2, Cook Units 1 & 2, Hope Creek, Farley Unit 2, Peach Bottom Unit 3, Salem Units 1 & 2, South Texas Units 1 & 2, and Three Mile Island Unit 1. Subsequently, South Texas Units 1 & 2 reported that they had completed their work ahead of schedule and that these two nuclear power plants were Y2K ready. Therefore, only 10 plants have Y2K work remaining on non-safety systems and 93 plants have reported that they are fully Y2K ready.

Nuclear Power Plant Y2K Readiness



The plants that have Y2K work remaining are continuing to progress toward Y2K readiness. As depicted in the chart above, we expect this trend to continue. Based on the information available today, by November 1, 1999, only three plants are projected to have Y2K work remaining. Those three are Comanche Peak (Unit 1), Farley (Unit 2), and Salem (Unit 1). The Y2K work remaining for all these plants is on non-safety plant support systems and an outage is required to complete the Y2K activities. The outages have been scheduled, and each of these licensees has experience on sister units in successfully completing the most significant Y2K remediation activities.

The NRC will continue to monitor progress at those plants with remaining work and will independently verify completion of the scheduled items, including reviews of licensee Y2K contingency plans. At this time, we believe that all licensees will be able to operate their plants safely during the transition from 1999 to 2000 and beyond, and we do not anticipate the need for the NRC to direct any plant-specific action. Given the readiness of the nuclear power plants, their operation through the transition to the Year 2000 should be beneficial in terms of maintaining reliable electrical power which is important to public health and safety.

**Nuclear Power Plant Emergency Power**

Based on current information from the North American Electric Reliability Council (NERC), it appears highly unlikely that availability of offsite power from the electrical grid will be significantly affected by Y2K-induced problems. According to NERC's latest report of August 3, 1999, more than 99 percent of the nation's electricity supply is classified Y2K-ready or Y2K-ready with limited exceptions, and 96 percent of all local distribution systems are certified ready for the Year 2000. In its reports issued on January 11 and April 30, 1999, NERC states, "Transmission outages are expected to be minimal and outages that may occur are anticipated to be mitigated by reduced energy transfers established as part of the contingency planning process." Both reports indicate that the transition through critical Y2K rollover dates should have a minimal impact on electric systems operations in North America and that widespread, long-term loss of the grid as a result of Y2K-induced events is not a credible scenario.

Nevertheless, the possibility of electric grid instabilities and blackouts during Y2K critical dates has been addressed by both the NRC and licensees. The scope of licensees' Y2K programs, including contingency planning, covers the onsite power and other emergency power systems at the plant, including emergency diesel generators (EDGs). NRC audits and reviews of licensee Y2K program activities to date have verified licensee consideration of these systems, and no associated Y2K issues relating to onsite or emergency power systems have been identified. Moreover, licensees are taking anticipatory measures for the Y2K transition, including completing surveillances and assuring EDG fuel supplies are "topped off." Existing regulatory and technical specification requirements provide a high confidence in EDG operability, availability, and reliability. Additionally, EDG reliability in emergency situations has been high, as demonstrated during weather-related power upsets. For example, following the 1992 landfall of Hurricane Andrew at the Turkey Point nuclear power plant, EDGs operated reliably for approximately six days providing electrical power to plant systems. Therefore, we do not consider it necessary to impose additional EDG requirements on licensees during Y2K critical dates.

**Spent Fuel Pools At Operating Nuclear Power Plants**

Spent fuel pool (SFP) cooling and makeup systems are mostly based upon analog controls and, therefore, are not subject to Y2K problems. Nevertheless, as previously explained, licensees implemented a structured program to be Y2K ready before the Year 2000 transition. This is a staff approved industry program that involves the identification of all software-based systems, equipment

and components, assessment of their vulnerability to the Y2K problem, and remediation if found vulnerable. The SFP systems and components are included in the program. The program also includes contingency plans for both external and internal events during the Y2K critical dates. For example, loss of off-site power and other types of grid issues are included as part of the contingency plan. SFP cooling water pumps can be powered from emergency power supplies if normal power is lost. Generally, the contingency plan makes use of existing plant procedures for loss of power to the SFP cooling and makeup systems that are based on NRC regulations.

Analysis has shown that a sufficient period of time is available for a licensee to take mitigative actions upon loss of spent fuel pool cooling pumps' electrical power. Therefore, the staff has confidence that spent nuclear fuel stored at operating nuclear power plants will remain safe during the Y2K transition.

#### **Spent Fuel Pools At Decommissioning Facilities**

Currently, there are 19 permanently shutdown nuclear power plants, 14 of which have spent fuel remaining on site. As time passes, fission products in the spent fuel decay and the heat in the spent fuel generated by this decay reduces significantly. Thus, the SFP heat load is reduced and the time available for operators to take actions to mitigate off-normal conditions increases. The maintenance of the integrity of spent nuclear fuel in the water-filled spent fuel pools is the major nuclear safety objective of these plants. This objective is assured through programs and systems such as systems to monitor fuel pool water temperature, level, chemistry and radiation in the area of the pool, and a safeguards program. Existing procedures and operator training allow the licensee to deal with normal and off-normal situations. Computers may be used to control, monitor and log the various parameters of the required programs and systems. However, the permanent plant staff would have ample time available and is capable of manual control of these functions, if needed.

In view of the reduced spent fuel pool decay heat loads at permanently shutdown plants and the long periods of time available to take mitigative actions, no formal Y2K guidance was issued to decommissioning plants. However, the NRC staff did contact all decommissioning reactor licensees by telephone in early 1999, and they all stated that they had taken actions to address the Y2K issue.

**NRC Actions With Materials Licensees and Fuel Cycle Facilities**

To alert licensees and certificate holders to the Y2K issue, NRC has issued four Information Notices (INs) to all materials licensees and fuel cycle facilities. An additional IN, which forwarded a copy of an FDA letter to medical device manufacturers, was sent to medical licensees only. The INs described potential Y2K issues, encouraged development of a Y2K readiness program (e.g., inventory, testing, remediation), alerted licensees and certificate holders to systems that were known to be or may be affected by Y2K problems, provided updates of NRC's Y2K activities, provided sources of Y2K information, and encouraged development of Y2K contingency plans. NRC has not identified any generic Y2K issue for NRC regulated material used by materials licensees.

NRC inspected the ten major fuel cycle facilities between September 1997 and October 1998 to assess the status of the facilities' Y2K programs and other safety matters. These inspections indicated that the facilities were adequately addressing Y2K issues.

To confirm that the ten major fuel cycle facilities were effectively addressing the Y2K issue, the NRC issued Generic Letter (GL) 98-03, "NMSS Licensees' and Certificate Holders' Year 2000 Readiness Programs." As with GL 98-01 for nuclear power plants, GL 98-03 required that the ten major fuel cycle facilities submit written responses regarding their facility-specific Y2K readiness program for safety and safeguards. All ten facilities provided the required response, and six facilities were Y2K ready by October 1, 1999. The remaining facilities provided a status report and schedule for remaining work to become Y2K ready well before December 31, 1999. There have been no identified risk-significant Y2K concerns for fuel cycle facilities. All of the major fuel cycle licensees, with the exception of the Gaseous Diffusion Plants (GDPs), have informed NRC that they plan to be in safe shutdown during the transition to the Year 2000. NRC has two resident inspectors assigned full time at each GDP. One inspector will be onsite at each GDP during the Y2K transition. NRC conducted follow-up Y2K inspections, including review of contingency plans, at the Portsmouth GDP in August 1999 and the Paducah GDP in September 1999. These inspections determined that the Y2K programs at both GDPs had taken the necessary actions to resolve the Y2K issue and had adequately addressed management planning, implementation, quality assurance, regulatory considerations, and documentation.

NRC will continue to make Y2K inquiries during inspections and will continue to monitor list servers, manufacturer web sites, news media, Congressional reports, and the President's Y2K Council reports for Y2K issues that may affect materials licensees and fuel cycle facilities. If Y2K issues that may affect materials licensees and fuel cycle facilities are discovered, the information will be forwarded to licensees and fuel cycle facilities and placed on the NRC Y2K web site. Also, NRC will confirm that the remaining fuel cycle facilities have completed Y2K readiness actions prior to the transition.

**NRC Internal Year 2000 Readiness Preparations**

As of February 5, 1999, all of NRC's systems have been examined and, as needed, fixed or replaced with regard to the Y2K problem. This work was accomplished more than a month ahead of OMB's established milestone and well under budget.

We have completed all work necessary to ensure that 100 percent of our telecommunications infrastructure is compliant or not affected by Y2K issues. We have contacted our telecommunications service providers, and all have responded that they are Y2K compliant.

The NRC's Y2K Contingency Plan describes steps the staff will take in the unlikely event that a Y2K problem would result in a safety concern at a nuclear power plant or gaseous diffusion plant. Beginning at noon on New Year's Eve, a team of specialists will staff the NRC Headquarters Operations Center to monitor, evaluate, and communicate any Y2K problems at foreign reactors that have potential safety implications for domestic reactor licensees. At 10:00 p.m. the Headquarters Operations Center will be staffed by a multi-disciplinary Y2K response team, headed by a senior NRC manager.

In addition to Headquarters staff, the Y2K response team will include inspectors stationed at each nuclear power plant and gaseous diffusion plant site and a team of specialists at the Incident Response Centers in each region. The NRC regional office in Arlington, Texas, will be prepared to assume the functions of Headquarters if an unanticipated Y2K problem results in the unavailability of the Headquarters Operations Center. In addition, the inspectors on site as well as the regional incident response centers and the Headquarters Operations Center will be equipped with satellite phones for use in the unlikely event that there is a major problem with the telephone network.

Yet another aspect of the NRC's Contingency Plan involves the sharing of information. The NRC is developing a Y2K Early Warning System to facilitate the sharing of information. We are working with our international partners to invite countries with major nuclear power programs to participate in this system. So far, about 25 countries, including Japan, South Korea, Taiwan, several Western European countries, Canada, and Mexico have committed to using this system.

The NRC has coordinated and communicated our Y2K Contingency Plan with our Federal partners, including the Federal Emergency Management Agency (FEMA), the Department of Energy, the Environmental Protection Agency, the National Communication System, the Federal Communications Commission, and the President's Council on the Year 2000 Conversion.

The Commission has recognized that continued safe operation of nuclear power plants during the transition to the Year 2000 may be important to help maintain reliable electrical power supplies. As such, as a companion to the NRC Y2K contingency plan, the Commission has expanded its enforcement discretion policy to allow for rapid decision-making under circumstances where an emergent, unanticipated Y2K problem might result in licensee non-compliance, but would not affect continued safe plant operation. The NRC has a policy of exercising its enforcement discretion with regard to temporary non-compliance of license conditions when it can be demonstrated that it is in the interest of safety. The Y2K transition enforcement policy builds on the existing enforcement discretion policy and continues to ensure public health and safety while appropriately considering some of the unique aspects associated with the Y2K transition.

#### **Y2K Exercises**

In July, NRC conducted a Y2K Tabletop exercise involving NRC, Baltimore Gas and Electric, the State of Maryland and the counties surrounding the Calvert Cliffs nuclear power plant. The exercise tested the NRC Y2K contingency plan procedures against a number of scenarios, including loss of power and loss of telecommunications. The exercise confirmed that each participant had put a considerable amount of thought into preparing for potential problems during the Y2K transition. Although no major Y2K contingency plan inconsistencies were identified, there were a number of valuable observations and lessons from this tabletop. We placed a synopsis of this exercise on our Y2K web site, so that the information can be shared with other stakeholders.

On October 15, 1999, NRC conducted a full scale exercise to validate our readiness to execute the provisions of the NRC's Y2K Contingency Plan for the Nuclear Industry. During the first phase of the exercise, which started at 6:00 a.m., an NRC team monitored information reported by regulators in nations which would experience the Y2K transition in advance of the U.S. This information was provided through the Internet-based Y2K Early Warning System developed by NRC. Through this system, nuclear power plant licensees, who have read only access, were able to monitor the status of foreign nuclear power plant designs similar to their own. The second phase of the exercise, focusing on potential domestic concerns, assembled an NRC Y2K response team that included staff in the Headquarters Operations Center, the Regional Incident Response Centers, and participating nuclear power plant sites. Licensee participants from eleven reactor sites and three fuel cycle facilities presented challenges ranging from simple requests for enforcement discretion to plant upsets resulting in an NRC emergency response activation. In some cases, licensee participants conducted internal Y2K exercises in parallel with this exercise. The exercise, simulated a Headquarters failure, necessitating a transfer of all Headquarters functions to NRC's Regional Office in Arlington, Texas. At that point, the back-up Operations Center in Texas assumed the lead role for NRC response and exercised their ability to assume the vital headquarters response roles. The exercise successfully demonstrated the NRC's ability to effectively deal with a wide range of unlikely, but possible, Y2K challenges. Although the exercise was highly successful, several valuable lessons were learned which will allow the NRC to further improve its high state of readiness.

Throughout the exercise, a mock White House Information Coordination Center (ICC) was operated the NRC Auditorium. The personnel who will represent the NRC at the ICC during the actual Y2K transition period had the opportunity to test the procedures for communicating and sharing data between the NRC Operations Center and the mock ICC. In addition, a Joint Public Information Center was simulated, where Graduate-level journalism students from American University, were present to play the role of the media.

#### **Federal Coordination**

On the Federal level, the coordination and cooperation between Federal agencies on the Y2K issue are a foundation upon which the Federal government is building for future cooperative efforts. Much of the effort being spent on the Y2K problem will help Federal agencies better respond to emerging unconventional threats to the United States, such as terrorist acts. For example, the National



Communication System, in partnership with the telecommunications industry, has established a telecommunications network used for communicating national security and emergency preparedness information that is independent of the public telephone network. Although the Y2K problem was the impetus for enhancing this network, it will become permanent following the Y2K transition. The President's Council on the Y2K Conversion also has established a command center that will collect and disseminate information during the Y2K transition. After the Y2K transition, this center will be turned over to the Critical Infrastructure Assurance Office to support our national response to emergent threats. NRC has purchased satellite phones for all of our nuclear power plant resident inspector locations as part of our Y2K contingency plan, and many utilities are also investing in upgraded communication systems. Our new satellite phones have already been put to use in our response to the recent hurricanes. These are just a few examples of how the Y2K effort will pay off long after the Year 2000 transition.

#### **International Activities**

We are involved in promoting awareness of the Y2K issues internationally. For consideration at the 42nd International Atomic Energy Agency (IAEA) General Conference in September 1998, the NRC took the lead in drafting a resolution on Y2K as it applies to the safety of nuclear power plants, fuel cycle facilities, and other enterprises using radioactive materials. The resolution was adopted by the IAEA Member States and urged, among other things, that: (1) member States submit information to the IAEA on activities underway to inventory and remediate Y2K problems at their nuclear facilities; and (2) the IAEA act as a central coordination point in disseminating information about Member State Y2K activities.

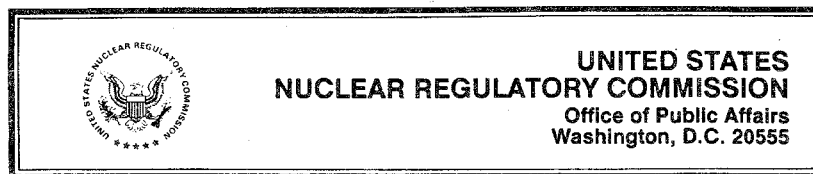
Since the General Conference, the NRC has worked with the IAEA to formulate a Y2K program that would address nuclear safety aspects of the Y2K problem. The NRC has also been working with its foreign bilateral nuclear safety cooperation partners on raising awareness of the Y2K problem and offering assistance within its means. The most notable development in this area has been the creation of the Y2K Early Warning System, discussed earlier, which will allow all participating countries to rapidly share Y2K related information on nuclear facility and grid performance.

**Summary**

The Commission has been active in addressing the Y2K problem with our licensees and continues to work, both nationally and internationally, to promote awareness and provide assistance in addressing the Y2K problem. We recognize that despite efforts of the industry and the NRC, unexpected events could occur; consequently contingency plans have been established.

With that said, it is of paramount importance to note that the NRC and the U.S. nuclear power industry are addressing the Y2K computer problem in a comprehensive, thorough and deliberate manner. Licensees for all 103 nuclear power plants have reported that the safety systems are Y2K ready. We expect all nuclear power licensees will complete their remaining Y2K readiness activities before the Y2K transition. The NRC has also conducted independent reviews of Y2K programs at all operating U.S. nuclear power plants. The results of these reviews all indicate that licensees have taken the proper steps to identify and remediate systems that could be affected by the Y2K bug. We will closely monitor the progress of plants that still have some systems left to remediate, but we fully expect that all commercial nuclear power plants will operate safely, as planned and without interruption, through the Y2K transition.

I look forward to working with the Committee, and I welcome your comments and questions.



Frank J. Miraglia

Professional Qualifications

Deputy Executive Director for Reactor Programs which oversees the implementation of agency programs associated with nuclear reactor regulation and regional operations.

Served as Deputy Director, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, Washington, D.C from April 1990 until December 1998. This office consisted of a staff of over 700 and is responsible for the reactor regulation program for all commercial, test and non-power reactors in the U.S.

Joined the Regulatory Staff of the U.S. Atomic Energy Commission in November 1967. Attended the Polytechnic Institute of Brooklyn, Brooklyn, New York, receiving a B.S. degree in Chemical Engineering in 1959. All requirements for a M.S. degree in Chemical Engineering (Nuclear Engineering minor), except for thesis, were completed at the same Institute in 1961. I am a member of the American Nuclear Society, the American Institute of Chemical Engineers and the American Chemical Society.

Past Professional Positions

09/99-Present	Deputy Executive Director for Reactor Programs, NRC
12/98-9/99	Deputy Executive Director for Regulatory Programs, NRC
04/90-12/98	Deputy Director, Office of Nuclear Reactor Regulation, ONRR
05/88-4/90	Associate Director for Technical Assessment, ONRR
04/87-05/88	Associate Director for Projects, ONRR
11/85-04/87	Director, PWR-B Division, ONRR. Responsible for safe operation of all CE and B&W reactors, also non-power reactors and standard plant reviews.
06/84-11/85	Deputy Director, Division of Licensing, ONRR
09/82-06/84	Assistant Director for Safety Assessment, Division of Licensing, ONRR
09/80-09/82	Chief, Licensing Branch, Division of Licensing, ONRR
02/80-09/80	Chief, Resources and Scheduling Branch, PSB, ONRR

06/79-02/80	Task Group Leader, Rogovin Task Force
07/78-06/79	Technical Assistant to Director, ONRR
06/76-07/78	Technical Assistant to Director, DSE, ONRR
09/72-07/76	Senior Environmental Project Manager, USNRC/AEC. Conduct environmental reviews and prepare the Commission's Environmental Statements related to the construction and operation of nuclear power reactors. Responsible for planning, scheduling and coordinating all technical effort in reviews for projects assigned. Projects included Arkansas Nuclear One, Comanche Peak Steam Electric Station, Hope Creek, Midland, Salem and South Texas Project.
09/69-09/72	Staff Assistant for Inspection, USAEC, RO. Technical direction and coordination in implementing DNMS safeguards inspection policies and procedures.
11/67-09/69	Chemical Engineer, USAEC, DNMS. Evaluation of materials licensing applications relative to the requirements for nuclear materials safeguards.
03/65-11/67	Group Leader, Martin Marietta Nuclear Division, Development Department. Responsible for administration and supervision of process development group. Lead engineer for Chemistry on Isochem program. Served as program manager and project engineer last two months of Isochem project.
12/63-03/65	Chemical Engineer, Martin Marietta Nuclear Division, Materials and Chemical Department. Responsible for scale-up of Sr-90 space fuel laboratory process to pilot plant process. Consultant for water chemistry problems on MH-1A, PM-3A and PM-1 reactors.
11/61-11/53	Plant Chemist and Health Physicist SM-1, U.S. Army, Ft. Belvoir. Responsible for chemical analyses of plant water systems. Also responsible for health physics functions.
09/60-09/61	Research Fellow (ChE), Polytechnic Institute of Brooklyn
01/60-09/60	Teaching Fellow (ChE), Polytechnic Institute of Brooklyn
06/59-01/60	Chemical Engineer, USAERDL, Ft. Belvoir, Virginia

Mr. HORN. Our last panelist is Ralph Beedle, the senior vice president and chief nuclear officer for the Nuclear Energy Institute.

Tell us a little bit about the Nuclear Energy Institute. I assume it is the trade association.

**STATEMENT OF RALPH BEEDLE, SENIOR VICE PRESIDENT  
AND CHIEF NUCLEAR OFFICER, NUCLEAR ENERGY INSTITUTE**

Mr. BEEDLE. Chairman Horn. Thank you for the opportunity to testify today.

The Nuclear Energy Institute is a member organization consisting of over 275 companies. Every nuclear operating utility is a member of the Institute. We establish policy and set practices for the nuclear industry as a whole.

I applaud the efforts of the joint committees to monitor the status of year 2000 readiness across the spectrum of American industry. In the past 2 years, the Nuclear Energy Institute has developed and implemented a comprehensive year 2000 readiness program. As a result of the tremendous effort of the thousands of professionals in the industry at our 103 reactors, I am proud to report that the U.S. nuclear power plants have demonstrated that all safety systems are year 2000 ready.

Since I last spoke to you in May 1998, over 200,000 systems and equipment have been reviewed for year 2000 readiness, and as of this morning, the 101, as previously mentioned, are Y2K ready. The two remaining facilities are in the process of making modifications during maintenance periods that are currently in progress.

The industry's nuclear power plants are well prepared for year 2000 and beyond.

The comprehensive year 2000 program developed by NEI in 1997 looks at all equipment that is important to plant operations, not just a few critical systems. The program is embodied in two documents, "Nuclear Utility Year 2000 Readiness" and "Year 2000 Readiness Contingency Planning." We supplemented these with training sessions for our project managers, conducted workshops to exchange year 2000 related information, and established an on-line bulletin board to speed the sharing of the most effective Y2K solutions.

Throughout the process, NEI has carefully monitored and reported the status of nuclear industry preparation to the Nuclear Regulatory Commission, as well as the North American Electric Reliability Council.

Safety is the nuclear energy industry's top priority, and with this in mind the first systems to undergo evaluation were those related to plant safety.

The industry has worked closely with the Nuclear Regulatory Commission in an open process that facilitates meaningful oversight of the industry's program. After careful assessment and evaluation, industry experts are confident that the nuclear utilities will continue to produce safe and reliable electricity without being affected by year 2000 computer problems.

NEI and our member utilities have worked closely with the North American Electric Reliability Council. As large-scale electric generating units, nuclear power plants are an important element in the overall stability of our Nation's electric transmission grid.

Data reporting, testing, and exercise participation are all part of the FERC program to ensure that generation, transmission, and distribution of electricity will continue to be reliable.

Recognizing the apprehension that many people have concerning this issue, the nuclear industry has prepared a Y2K contingency plan. Additional personnel, backup communication systems, and response strategies have been developed for each reactor facility. This advanced preparation will reduce the likelihood that even a minor problem will cause a disruption in power generation.

Be assured, however, that any problem that could compromise safety would result in placing the plant in a safe shutdown condition.

Before I conclude, let me address the subcommittee's request for information regarding the nuclear industry and the international year 2000 readiness.

The U.S. Department of State serves as the lead entity in providing assistance to other nations on Y2K issues in conjunction with the International Atomic Energy Agency. The readiness program developed by NEI that I mentioned earlier is used as a basis for the IAEA international efforts. I'm certain that the State Department and the IAEA would be glad to provide you with additional details on their activities.

In conclusion, the nuclear utilities have reviewed, tested, and resolved equipment problems and are ready for year 2000. Consumers can approach the transition of year 2000 with confidence that the Nation's 103 nuclear plants will provide 20 percent of the electricity in a reliable and safe manner.

Thank you, sir.

Mr. HORN. Thank you very much. That is a helpful document you have submitted and I appreciate your summary.

[The prepared statement of Mr. Beedle follows:]

**Testimony Submitted for the Record**

**Ralph Beedle**

**Senior Vice President and Chief Nuclear Officer**

**Nuclear Energy Institute**

**October 22, 1999**

**U.S. House of Representatives**

**Science Subcommittee on Technology**

**&**

**Government Reform Subcommittee on Government Management,  
Information and Technology**

Testimony of Ralph Beedle  
October 22, 1999

Chairwoman Morella, Chairman Horn, Ranking Members Barcia and Turner and members of the subcommittees, my name is Ralph Beedle. I am Chief Nuclear Officer and Senior Vice President of the Nuclear Energy Institute. The Institute is a policy organization that represents 275 companies, including every electric utility operating a nuclear power plant in this country, nuclear systems suppliers, design and engineering firms, radiopharmaceutical companies, labor unions and law firms.

Madam chairwoman and mister chairman, I applaud the efforts of your joint committees to monitor the status of Year 2000 readiness across the spectrum of American industry. In the past two years, the nuclear energy industry has developed and implemented a comprehensive and uniform Year 2000 readiness program. As a result of the tremendous efforts of industry professionals at 103 reactors across the country, I am proud to report that all U.S. nuclear power plants have demonstrated that all safety systems are Year 2000 ready. In fact, a total of just four non-safety-related issues remain to be completed before January 1, and those are being addressed during current maintenance and refueling outages. Since I last spoke with you on May 14, 1998, America's nuclear power plants have become well prepared for the Year 2000.

The comprehensive and uniform Y2K program NEI developed in 1997 is broad based. It looks at all systems that are important to plant operations, not just a few critical systems. The program was embodied in two documents: *Nuclear Utility Year 2000 Readiness* and *Year 2000 Readiness Contingency Planning*. We supplemented these with training sessions for Y2K project managers, conducted workshops to exchange Y2K-related information and established an on-line bulletin board to speed the sharing of the most effective Y2K solutions. Throughout the process, NEI has carefully monitored and reported the status of nuclear industry preparation to the Nuclear Regulatory Commission and the North American Electric Reliability Council.

Safety is the nuclear energy industry's top priority. We recognize our obligation to assure adequate protection of public health and safety. With this in mind, the first systems to undergo evaluation were those related to plant safety. The industry has worked closely with the Nuclear Regulatory Commission, in an open process that facilitates meaningful oversight of the industry program. After careful assessment and evaluation, industry experts are convinced that nuclear utilities will continue to produce safe, reliable, clean and affordable electricity for our homes, neighborhoods, businesses and industries without being impacted by Y2K issues.

The Institute also has worked closely with the North American Electric Reliability Council in its effort to ensure reliable generation, transmission and distribution of electricity to customers. The electric utility industry has a high degree of confidence in the Y2K efforts at our nuclear power plants. As baseload units,



Testimony of Ralph Beedle  
October 22, 1999

operating nuclear plants are an important element in the overall stability of our nation's transmission grid.

There are no Y2K problems concerning safety at the nation's 103 nuclear reactors. In fact, 99 of the nation's 103 nuclear reactors have completed Y2K remediation. The 4 remaining facilities are currently shutdown for maintenance periods and are in the process of addressing the four outstanding continuity of power Y2K issues before resuming the generation of electricity. None of the outstanding Y2K issues are safety-related.

Recognizing the concerns presented by the potential for Y2K problems outside the control of our plant operators, and the importance of reliable electric power, we in the nuclear industry deemed it prudent to prepare detailed contingency plans. Therefore contingency plans for each nuclear facility are in place and ready should circumstances require them to be implemented during the transition to the New Year. Additional personnel will be on site, backup communications systems are available, and response strategies have been developed. This advance preparation will reduce the likelihood that a minor glitch will result in the plant being taken off the grid. However, rest assured that any problem that could affect safety would result in a plant shutdown following normal procedures.

Before I conclude madam chairman and mister chairman, allow me to address the subcommittee's request for information regarding the nuclear industry and international Y2K issues. The U. S. Department of State serves as the lead entity in providing assistance to other nations on Y2K issues, in conjunction with the International Atomic Energy Agency (IAEA). The NEI-developed plans are being used as the basis for the IAEA's efforts internationally. I am certain that the State Department and IAEA will be glad to provide the subcommittee with more detailed information about their efforts on the international front.

In conclusion, there are no Year 2000 safety problems at America's 103 nuclear reactors. The 20 percent of our nation's electricity generated by nuclear power—enough electricity for 65 million homes—will not be jeopardized by Y2K. America can rely on electricity from nuclear energy—the greatest source of emission-free electricity—on New Year's Day 2000 and on into the new century. We approach the new era knowing that all safety-related issues have been resolved and that these baseload electric facilities will continue to substantially contribute to the stability of the nation's electricity power grid.

**Nuclear Utility Industry Year 2000 Readiness Status**  
**Updated October 18, 1999**  
(Year 2000 Readiness Disclosure<sup>1</sup>)

Each of the 103 commercial nuclear power reactors has reported the status of their Year 2000 readiness program, based on industry guidelines in *Nuclear Utility Year 2000 Readiness*. These programs apply to software, hardware and firmware in which failure due to a Y2K issue could interfere with performance of a safety function or impact continued safe operation of the nuclear facility.

To date, 99 reactors have completed all remediation and are Y2K ready. There are only four open items at the four remaining reactors. Remediation is in progress at two reactors currently shutdown for refueling outages. One site with two reactors is remediating a site support system that does not impact reactor operations.

The industry has tested approximately 200,000 items that could be susceptible to Y2K issues over the past two years. Of these, approximately five percent—or 10,000 items—needed remediation. The industry has completed over 99 percent of the overall readiness program.

Each facility also prepared contingency plans for key Y2K rollover dates using guidance in *Nuclear Utility Year 2000 Readiness Contingency Planning*. These plans will reduce the impact of internal or external Y2K induced failures. Both industry guidelines are publicly available at the Nuclear Energy Institute web site (<http://www.nei.org>).

The Nuclear Regulatory Commission (NRC), the federal government's nuclear safety regulator, has been directly involved in the industry's Y2K readiness activity for the past two years, including on-site program reviews. NRC audits and on-site reviews have confirmed that nuclear power plants will continue to generate electricity safely and reliably as we enter the year 2000. The agency also concurs that all safety systems will function if required to safely shut down a plant. Independent NRC and industry audits demonstrate that Y2K readiness programs have been properly executed.

The nuclear industry's Y2K effort has been closely coordinated with the North American Electric Reliability Council (NERC), the organization managing the overall Y2K readiness effort of the electric industry. The current industry status leads to high confidence that nuclear generation plants will continue to reliably deliver 20 percent of the nation's electricity needs well into the next century.

---

<sup>1</sup> This year 2000 readiness disclosure is made under the "Year 2000 Information and Readiness Disclosure Act" (Public Law 105-271)

### Nuclear Generation plants that are Y2K Ready

The following 99 plants report they have completed all remediation and are Y2K ready.

Company--Plants
Alliant Energy—Duane Arnold
Ameren UE—Callaway
Arizona Public Service Company—Palo Verde 1, 2 & 3
Baltimore Gas & Electric—Calvert Cliffs 1 & 2
Carolina Power & Light Company—Brunswick 1 & 2
Carolina Power & Light Company—Harris 1
Carolina Power & Light Company—Robinson 2
Commonwealth Edison—Braidwood 1 & 2
Commonwealth Edison—Byron 1 & 2
Commonwealth Edison—Dresden 2 & 3
Commonwealth Edison—LaSalle 1 & 2
Commonwealth Edison—Quad Cities 1 & 2
Consolidated Edison—Indian Point 2
Consumers Energy—Palisades
Detroit Edison—Fermi 2
Duke Energy Corporation—Catawba 1 and 2
Duke Energy Corporation—McGuire 1 and 2
Duke Energy Corporation—Oconee 1, 2, and 3
Duquesne Light Company—Beaver Valley 1 & 2
Entergy Operations—Arkansas Nuclear One 1 and 2
Entergy Operations—Grand Gulf 1
Entergy Operations—Pilgrim
Entergy Operations—River Bend
Entergy Operations—Waterford 3
First Energy Corporation—Davis-Besse
First Energy Corporation—Perry 1
Florida Power & Light—St. Lucie 1 & 2
Florida Power & Light—Turkey Point 3 & 4
Florida Power Corporation—Crystal River 3
GPU Nuclear Corporation—Oyster Creek
GPU Nuclear Corporation—Three Mile Island 1
Illinois Power—Clinton
Nebraska Public Power District—Cooper
New York Power Authority—James A. Fitzpatrick
New York Power Authority—Indian Point 3
Niagara Mohawk—Nine Mile Point 1 & 2

Northeast Utilities—Millstone 2 & 3
Northeast Utilities—Seabrook 1
Northern States Power Company—Monticello
Northern States Power Company—Prairie Island 1 & 2
Omaha Public Power District—Fort Calhoun
Pacific Gas & Electric Company—Diablo Canyon 1 & 2
PECO Energy Company—Limerick 1 & 2
PECO Energy Company—Peach Bottom 2
Pennsylvania Power & Light—Susquehanna 1 & 2
Public Service Electric & Gas—Hope Creek
Public Service Electric & Gas—Salem 1 & 2
Rochester Gas and Electric—Ginna
South Carolina Electric & Gas—V. C. Summer
Southern California Edison—San Onofre 2 & 3
Southern Nuclear Operating Company—Farley 1
Southern Nuclear Operating Company—Hatch 1 & 2
Southern Nuclear Operating Company—Vogtle 1 & 2
STP Nuclear Operating Company—South TX Project 1 & 2
Tennessee Valley Authority—Browns Ferry 2 & 3
Tennessee Valley Authority—Sequoyah 1 & 2
Tennessee Valley Authority—Watts Bar 1
TXU Electric—Comanche Peak 1 & 2
Vermont Yankee—Vermont Yankee
Virginia Power—North Anna 1 & 2
Virginia Power—Surry 1 & 2
Washington Public Power (Energy Northwest)—WNP-2
Wisconsin Electric Power—Point Beach 1 & 2
Wisconsin Public Service—Kewaunee
Wolf Creek Nuclear—Wolf Creek

**Nuclear Generation Plants and Sites with Y2K Remediation  
Outstanding**

**Safety systems:**

Company—Plant Item—Impact	Completion Date
NONE	

**Plant Operating and Plant Support Systems:**

<b>Company—Plant</b>	<b>Completion</b>
<b>Item—Impact</b>	<b>Date</b>
<b>PECO Energy Company—Peach Bottom 3</b>	
Unit 3 Digital Feedwater System—Work will be performed during September outage. <b>(Outage started 9/29/99)</b>	10/31/99 (fall outage)
Unit 3 Turbine Vibration Monitor—Used for protection of feed pump and turbine system. Work will be performed during September outage. <b>(Outage started 9/29/99)</b>	10/31/99 (fall outage)
<b>Southern Nuclear Operating Company—Farley 2</b>	
Unit 2 Turbine Digital Electro-Hydraulic (DEH) system—Needed for plant operations and will be upgraded during the fall outage. This upgrade has been successfully completed on Unit 1. <b>(Outage started 10/15/99)</b>	12/16/99 (fall outage)

**Site Support Systems:**

The following facility has a site support system, within the scope of the industry program, that will be Y2K ready when the indicated remediation is completed. This support system does not impact continued plant operation.

<b>Company—Plant</b>	<b>Schedule</b>
<b>Item—Impact.</b>	<b>Date</b>
<b>American Electric Power—Cook 1 &amp; 2</b>	
Site Meteorological Information and Dispersion Assessment System (MIDAS)—Used for gathering weather information in support of the emergency plan. Alternate sources of weather data are available. Installation completed on 10/14/99. Validation testing is in progress	10/30/99



## Year 2000 Readiness: Nuclear Power Plants Prepare for the Millennium Challenge

### Key Facts

■ The 66 facilities that are home to the United States' 103 nuclear energy reactors are on the verge of achieving complete Year 2000 readiness.

■ As of Oct. 18, 99 reactors had reported that they are Y2K ready, with all remediation work completed. The remaining four reactors had a total of four computer items to remediate. These items have no outstanding Y2K issues that affect safety.

■ Federal agencies and industry authorities—such as the U.S. Nuclear Regulatory Commission (NRC) and the North American Electric Reliability Council (NERC)—confirm that the nuclear energy industry is well on its way to assuring that nuclear plant safety systems, if called upon, will function as designed when the Year 2000 arrives.

■ Industry tests have shown that systems needed to safely shut down nuclear power plants—even the small percentage of systems that involve computers—will not be compromised by Y2K issues and will respond to plant conditions with high levels of reliability, if needed after Jan. 1, 2000.

■ The industry expects that, based on its Year 2000 readiness efforts, nuclear power plants will continue to generate electricity as safely on Jan. 1, 2000, as they do today.

### Status of Industry Y2K Remediation

All nuclear power plants have completed the detailed assessments needed to pinpoint computer systems that might be affected by Y2K issues. As of Oct. 18, 99 reactors reported to NRC that they are Y2K ready, with all remediation work completed—encompassing safety, operating and site support systems. The remaining four reactors had a total of four items to remediate. These items have no outstanding Y2K issues that affect safety.

On Aug. 4, NRC Chairman Greta Joy Dicus told the United States Senate, "We conclude that the Year 2000 problem will not adversely affect the continued safe operation of U.S. nuclear power plants." She added, "No remaining Y2K problems exist that could directly affect the performance of safety systems or the capability for safe shutdown." Typically, the remaining Y2K work to be completed after July 1 is because of a scheduled plant outage in the fall or the necessity to wait for delivery of a replacement component for a plant. Maintenance shutdowns at nuclear power plants often are scheduled for the fall, so that the plants' ability to provide electricity at the most economical rates during hot summer months is not impeded.

During the past two years, the nuclear industry has tested more than 200,000 items (encompassing safety and operating systems) potentially susceptible to Y2K



SUITE 400  
1776 I STREET, NW  
WASHINGTON, DC  
20006-3708  
202.739.8000  
www.nei.org



## Nuclear Power Plants Prepared for the Millennium Challenge

Page 2 of 2 – October 1999

issues. Approximately 5 percent of these—or 10,000 items—required remediation.

In its latest Y2K status report released Aug. 3, NERC said that, “The current industry status leads to high confidence that nuclear generation plants will continue to reliably deliver their share of the nation’s electricity needs well into the next century.” NERC is the coordinating group for regional organizations that address electric reliability issues.

The NRC’s oversight of the industry’s Y2K readiness has included on-site audits of measures taken by 12 nuclear power plants. [These audits were conducted over a five-month period.] Summarizing the audit findings, the agency announced April 28 that, “No problems were found at the plants that will interfere with the ability of their computers to control key safety systems.” The agency said, more broadly, “NRC has no indication that Y2K computer-related problems exist with safety-related systems in nuclear power plants.”

### Industry’s Approach to the Y2K Challenge

The Year 2000 challenge is caused by computer systems that recognize a year by its last two digits (for example, “1987” is “87” in computer language) and could, if not corrected, cause malfunctions by reading the Year 2000 as 1900.

In 1997, the nuclear industry began moving quickly to assess the Y2K challenge and work with key federal agencies to help plant operators prepare for continued safe operations at the start of the millennium. The Nuclear Energy Institute and the Nuclear Utilities Software Management

Group released the *Nuclear Utility Year 2000 Readiness* plan in October 1997.

All nuclear power plants are following this comprehensive program, which provides detailed procedures and checklists for resolving Y2K issues, based on the best utility practices. The NRC has stated that this guidance document “has yielded effective Y2K readiness programs.” NEI has supplemented *Year 2000 Readiness* with workshops and an on-line bulletin board to help plant managers share information and best practices. NRC audits of Y2K programs at selected nuclear power plants have affirmed the effectiveness of the industry’s effort.

As they correct or replace systems affected by Y2K issues, plant operators continue to review and refine contingency plans for potential challenges to plant operations from situations not under their control. In July 1998, NEI released its *Year 2000 Readiness Contingency Planning* guidance document to help plant operators prepare for potential external impacts such as: events in regional power supply systems; fluctuations in water levels in rivers used for cooling; availability of supplies needed for plant operations; interruptions in water services or communications; Y2K events at plant suppliers; and performance of some offsite emergency preparedness equipment.

*This policy brief is also available on NEI’s site on the World Wide Web—  
<http://www.nei.org>—where it is updated periodically.*

Mr. HORN. We have a number of members here from both the Science Technology Subcommittee, as well as Government Reform's Government Management, Information, and Technology Subcommittee. We will now go into questioning. Everybody on the panel, including myself, will be limited to 5 minutes until everybody else gets through. We have about 10 Members present, so it will take an hour for the questioning.

But let me start out, based on the letter we wrote in December 1998 to Chairman Jackson when we asked her about the audit on the year 2000 readiness of all domestic nuclear power plants and facilities.

We were told that, "Well, we really don't have to worry that much. American reactors are different than French reactors," and so forth. And in February 1999, the NRC did respond finally to our letter and said 42 or 41 percent of the 103 nuclear power plant units were included in the NRC sample audits of 12 utilities.

What I'd like to know is: how did you develop that sample? Was that based on different reactors within the universe, or what?

Mr. MIRAGLIA. Yes, sir. I will be happy to respond to that.

In terms of your letter—we did respond in February—there were 12 licensees that were examined in terms of the audit, and they covered 42 units. The units were picked on a number of criteria—the age of the plant, multiple units, single unit, different regions of the country, boiling water reactors, pressurized water reactors. And the 12 utilities did represent 42 plants, which was a unique representative mix of the 103 facilities.

In addition, we did six audits of the contingency plans at six licensees other than the 12, and that covered another 18 units. These were detailed audits where we used as the basis of the review the guidelines Mr. Beedle reviewed with you. Those guidelines were endorsed by the NRC as being appropriate guidelines to follow for Y2K remediation and assessment, as well as contingency planning.

Based upon those reviews, sir, we did develop an inspection protocol and came up with an inspection protocol that was completed by our inspectors at each of the 103 facilities, based upon the insights of those audits.

Through subsequent conversations and discussions, we did exactly what you originally had asked us in terms of where we stand today.

Mr. HORN. Well, can you say that the 103 are Y2K compliant?

Mr. MIRAGLIA. In terms of the safety systems, they were reported as Y2K ready on July 1st, and we have confirmed that by independent inspections and followup inspections. As I have indicated in my testimony, right now, as officially reported by us, there are four that we consider to have some additional work in non-safety systems. Three of those are expected to be completed by the end of the month, and that one unit, Farley 2, would be Y2K ready by December.

Mr. HORN. In terms of the use of computers in relation to the reactors, what do we know and what did the inspectors find out? Did they try a pilot where they advanced the date to January 1, 2000? And, if so, what happened?



Mr. MIRAGLIA. In terms of the inspection guidelines that were endorsed, there were a number of aspects of that plan in terms of how to assess the impact of potential computer problems and how to remediate and how to test. The testing could be roll-back, as you suggest, or roll-forward, as well as working with vendors to modify the programming within the systems.

An important point that should be made is that there are not many digital control systems within the nuclear power plants' safety systems, so the scope of those kinds of activities is reduced.

Mr. HORN. What do you know about the nuclear plants abroad? Is there a relationship between your commission in terms of loaning expertise on this? And what is your feeling as to what is happening there?

Mr. MIRAGLIA. We have worked through the International Atomic Energy Agency, as well as the Nuclear Energy Agency, which is part of OECD, the European economic community, and have provided what we have done in this country, in terms of the guidance. And, as Mr. Beedle has indicated, that guidance has been utilized by a number of foreign countries to review and remediate their facilities.

As Mr. Rhodes has indicated, there have been concerns expressed relative to the Russian facilities. We don't have direct involvement and other than providing information and sharing what we have done here and what our regulatory processes are.

Mr. HORN. My understanding on the Russian facilities is that one is very close to Alaska, in terms of at least the islands and reaching out to the Bering Strait. Is that a problem at all? Do we know anything from the Russians on that?

Mr. MIRAGLIA. I couldn't address that question.

Mr. HORN. OK. Let me ask—because I have got about 40 seconds left—GAO, did you look at the sample? Did you have any concern about the sample they took and the way they did it?

Mr. WILLEMSEN. The concerns that we would have had, Mr. Chairman, were really parallel to the ones that you pointed out in your letter. Subsequent to the letter, as NRC has pointed out, there were additional evaluations done. As we mention in our testimony, a 452-question check list was administered to all plants.

In addition, we are aware that many of the plants did have independent verification and validation efforts performed; however, we are not clear on the exact nature of those IV&V efforts. One of the suggestions that we have for NRC is to be clear and precise on what was done and how consistent it was across plants so that, if there is additional IV&V needed at plants, there is still a couple months to do that.

Mr. HORN. My time is up, so I'm going to yield 5 minutes to Mr. Kanjorski, acting for the minority.

Mr. KANJORSKI. Thank you very much, Mr. Chairman.

Just in regard to the Peach Bottom plant in Pennsylvania, by the end of November you anticipate they will be in compliance, or the end of October?

Mr. MIRAGLIA. The end of October, sir.

Mr. KANJORSKI. Is there any reason why they are running late compared to the other 100?

Mr. MIRAGLIA. In terms of some of the remediation that has to be done, it requires an outage. Nuclear power plant outages are traditionally spring and fall. They completed the outage, the spring outage, on one unit and made the remediations. They are just in their fall outage, and the remediation is underway and expected to be completed by the end of the month, sir.

Mr. KANJORSKI. The entities that have the spent fuel, are there any that are at total capacity? And, if you can tell me, what type of manual backup is there if the computer system fails to keep the spent fuel secure.

Mr. MIRAGLIA. As I indicated in my oral and in my written testimony, most of the systems at these facilities are analog and do not have much digital and computer controls. The 14 decommissioned facilities that one is talking about, the fuel has been in the pool for in excess of 2 years, and therefore the decay heat is significantly reduced. This would allow operators a significant amount of time, on the order of hours, to restore and to make up water and to replenish water, and that could be easily done manually.

In addition, they do have emergency supplies that they can line up, as well.

Mr. KANJORSKI. It seems to me that, when you look at the number of plants in the world, the United States has about a third of the nuclear plants, and we could rest assured they are in pretty good shape. The other two-thirds, do you all have opinions as to what status they are? And is there a possibility that they could go to a critical point and, if so, cause a disaster such as we recently almost had in Japan, or something that you really have a reaction?

Mr. MIRAGLIA. That would be purely conjecture on my part, but my view would be that the concern, as Mr. Rhodes indicated, is directed at perhaps some of the facilities in the former Soviet Union, and that the concern there is perhaps not just directed at the plants as much as perhaps the reliability of the grids in those countries.

Mr. KANJORSKI. Backup systems for power?

Mr. MIRAGLIA. Maintaining power to the plant to assure safe operation, and I think there's little known. And I think, because of what is known in terms of real facts makes it difficult for one to make conjectures in that regard.

Mr. KANJORSKI. If there were failures in some of these other countries, particularly in the former Soviet Union, do we have a national policy or international policy of forming a response team to get in there before something would become critical, or are we just waiting under normal processes, if a disaster occurred, to then put together a response?

Mr. MIRAGLIA. I believe there is activity underway in terms of perhaps Department of Energy providing more assistance, but that is all I could say. I think the government is trying to provide assistance to these facilities.

Mr. KANJORSKI. But that is assistance now in helping them get to compliance. I'm talking about if something happens after January 1st and we say a week period of time or 2-week period of time. Do we have something that we can lend the best expertise and a response team very quickly to get into those areas?

Mr. MIRAGLIA. A very good example of that, sir, would be the events that did occur in Russia in 1986, and that the Federal Government does have a response plan and we would be prepared to interact, and that would involve a large number of agencies, of which NRC is just a part of what that response would be.

Mr. KANJORSKI. I notice on the list here plants, Korea. Is that South Korea, or North Korea, too?

Mr. MIRAGLIA. Most of the plants are in South Korea in terms of power plants.

Mr. KANJORSKI. But there are some power plants in North Korea?

Mr. MIRAGLIA. You are stretching my knowledge now. I believe there are some smaller reactors within North Korea.

Mr. KANJORSKI. The whole panel, if you can, more on the international problems, the other 66 percent, what do you think the degree of reliability is at this point? Is it that there are no problems out there that could be serious for other countries or for the world, as a whole, for something critical?

Mr. RHODES. In terms of the former Soviet Union, leveraging off of what the NRC has said, again, the concern—for example, let's take South Korea. Well, South Korea's reactors are CANDU reactors. They are Canadian light-water reactors, so the design is understood. When I was in Ottawa, Canada, in February at the International Nuclear Power Preparedness Conference, the Canadian Atomic Energy Control Board was there. They did meet with the South Koreans and they are helping them.

We had the developers from Czechoslovakia, who built most of the Russian reactors, who were there. They have a few reactors themselves, and there was a good exchange.

The concern that we had at that time, which stands today, is that the Russian nuclear power plant industry is still in what we would all describe as the "awareness phase."

When you are talking about a graphite-moderated light water reactor of the Chernobyl type—it is called an RBMK—the concern again is not so much with the reactor itself as it is with the instability of the grid, the instability of diesel backup, and the fact that you are talking about a country that has a struggling economy.

There are always anecdotal stories about people selling the diesel fuel as currency. I mean, you are moving into a barter environment. That is the concern. It is a concern that Lawrence Gershwin of the intelligence community voiced several times now over the last year, in that it is not with the reactor itself so much as it is with the stability of the grid.

The United States is providing actual technical support, but we can't solve every problem for all the reactors in the former Soviet Union because we don't have the resources to do that unless we draw resources away from solving our own problem.

That is the concern that I and other people who are tracking international nuclear power have. It is not so much our domestic it is not ourselves or Canada or Great Britain or even France as much as it is the former Soviet Union. And it is not so much the reactor as it is the stability of the grid.

Mr. HORN. The time is up. We will now start on Ph.D. row to my left here. Mr. Ehlers is a physicist. We will go to Mr. Bartlett.

With two degrees, you are Dr. Dr. Bartlett, I guess. Go ahead, Roscoe.

Mr. BARTLETT. Thank you very much.

Are the nuclear reactors isolated from the grid, so if the grid fails there is not a problem with the functioning of the reactors?

Mr. MIRAGLIA. In terms of the design of our reactors, sir, we are concerned about the grid in two ways. First is the impact of the grid on the plant, itself. Second is the loss of the plant being a large power supply and what effect that may have on the grid.

The plant can be isolated from the grid and operate on emergency diesel in isolation from the grid, but in that condition the plant is in a shut-down mode and maintaining itself in a safe shut-down condition.

Mr. BARTLETT. I have a lot more confidence in the integrity of the nuclear power plants in Y2K than I do in the continuity of the grid.

Are plants prepared, if the grid goes down, to immediately isolate themselves so that there is no fall-back problem?

Mr. MIRAGLIA. In terms of even prior to the grid—the concern about Y2K, the loss of offsite power is a design basis event that the plants are evaluated and can cope with in terms of its design, and so the answer to that question would be yes, sir.

Mr. BARTLETT. Let me ask a policy question. I suspect that our nuclear reactors are going to behave flawlessly in Y2K. I do not have that same degree of confidence for the grid and the other power plants. Will this give us an opportunity to help educate the American people as to the safety of the nuclear power generation so that we might be able to expand that contribution to our electricity production in the future?

Mr. MIRAGLIA. That would be conjecture on my part, sir, but, since you have asked for a personal view, I would give it. I think, as indicated here, 20 percent of our electrical supply is nuclear. The expectation is that the grids will remain whole and that the nuclear power plants would safely go through that transition.

As to whether that would be renewed interest in nuclear power I think that would remain to be seen.

Mr. BARTLETT. I would like us to be prepared to exploit what I think is going to be a meaningful opportunity here.

We have 2 percent of the known reserves of oil. We use 25 percent of the world's oil. That is a prescription for disaster and an obvious indication that we ought to be looking for alternative ways of producing our energy, and nuclear is certainly one of those.

The big impediment to using more nuclear power has been one of education and the perception by the public that somehow this is not safe, although I think it has been the safest type of power generation that we have had.

I hope that the Administration and others are looking for the opportunity of educating the American people so that they will be more comfortable with nuclear power. They are not now accepting of nuclear power. If we don't do something, the 20 percent electricity we are now producing by nuclear power will shrink to zero. All the while, we are using up even more of the small amount of oil that we have remaining.

As I said, although we have only 2 percent of the known reserves, we use 25 percent of the world's energy.

Certainly, of all the countries in the world, we ought to be looking more aggressively at nuclear power, and we are actually turning away from it. As far as I know, no new plants are going to be licensed.

I just hope that we will exploit the opportunity I'm quite sure we are going to have in Y2K for educating the American people as to the safety, the reliability of nuclear power plants so that we can hopefully move forward on that front.

I have no further questions, Mr. Chairman.

Mr. HORN. Thank you very much.

We will now ask Mr. Baird from Washington, 5 minutes on questioning.

Mr. BAIRD. Thank you, Mr. Chairman.

I have just two fairly brief questions.

First of all, we focused a lot on power generation. What about the waste storage programs around the country? What reviews have been put in place for that?

Mr. MIRAGLIA. Most of the spent fuel, sir, is at the operating reactors, and it is either stored in spent fuel pools, and those systems were examined in the context of 103 operating reactors.

As indicated, there are 14 facilities that are being decommissioned and no longer generating power, but they are maintaining the fuel in water pools. There are five facilities that have fuel either shipped offsite or in dry cask storage, which is a passive type system.

Those systems and those facilities are being—maintaining cooling is the primary objective. The plant procedures are such that the operators are trained in taking appropriate response to those events. As I have indicated, most of the fuel in the pool is 2 years old or closer to 3 years old, and so the heat load is fairly low and there is significant time for the plants to deal with any contingency that might arise with respect to Y2K.

As I indicated, most of the systems are analog and not Y2K prone, in many cases.

Mr. BAIRD. In one of the testimonies it discussed a Y2K exercise, in which NRC conducted a table top exercise with Baltimore Gas and Electric. It sounds, from reading this, like it went pretty well and that people are well prepared.

Was it your impression that people were well prepared because they knew they would be part of this exercise, or if we were to, say, randomly drop in tomorrow at some community that is near a nuclear reactor and say, "What would happen? Would they be as well prepared?"

Mr. MIRAGLIA. I think, in context, the regulatory structure that exists and has existed prior to the Y2K issue always had emergency preparedness as a key centerpiece in defense and depth concept; therefore, there are emergency plans. We work with FEMA, our sister Federal agency. FEMA coordinates the offsite response to State and locals are prepared to respond to events at the nuclear facilities.

We work with the utilities to assure that their emergency response plans are coordinated with the State and local officials.

So that infrastructure existed. The existing table top brought the local facilities and local counties in and around Calvert Cliffs together, along with the utility, as well as State, FEMA, and us, and walked through scenarios to say, "If this happens, how are we going to augment communications? How are we going to communicate?" That was the kind of exercise that was conducted in terms of the table top, which was July, and that went very well.

There were lessons learned, in that communications need to be compatible so one needs to talk to one another and say, "What are your plans," and that activity was ongoing.

In addition, we did a drill on October 15th where we exercised our contingency plan and dealt with 11 nuclear power plants and three fuel facilities. Some of those facilities were exercising their contingency plans with the State and locals at that time, as well.

Mr. BAIRD. From listening to that, though, I'm hearing about 12 plants where some sort of exercise has been done. To what extent has this been recreated across the broad spectrum?

The nightmare scenario, of course, and not to be alarmist, of course, is an accident at a plant and simultaneously the grid goes down, communication is disrupted, transportation is disrupted, other problems. I mean, I'm not an alarmist with that, but it is worth saying. To what extent have other communities around nuclear plants within this country taken a very serious look at, if that scenario were to play out with the disruption of communication, power, transportation, et cetera, how would they cope with it? To what extent have they done that?

Mr. MIRAGLIA. In terms of the guidelines, the guidelines address those types of issues. Many of the utilities participated in the September 9, 1999, drill that was conducted with NERC in terms of exercising their plans, as well. So there were those kinds of exercises, as well, across the country, not only at the nuclear power plants, but most generating stations.

In terms of our own contingency plans, we are going to have a resident or inspector stationed at the facility during the rollover in the transition. They will be familiar with the contingency plans at the licensees' facilities. They will be equipped. We have provided to each site, each inspector that is going to be at the facility, with satellite communications, so there is guaranteed communications between the facilities and our operations offices here in headquarters, as well as our regions.

Mr. BAIRD. One last question. My understanding is that the French have distributed iodine to their residents as just a precautionary note, not in relation to Y2K. They did this some time back. Is there any thought about doing that?

Mr. MIRAGLIA. In terms of the use of potassium iodine for occupational workers, that is a part of most emergency response plans. The issue is a more widespread distribution of KI, and that policy matter is under review.

Mr. BAIRD. It seems like it might be a fairly prudent prophylactic just in case, you know. To have it around anyway might be useful, but certainly in the off chance there would be a Y2K problem.

Thank you, Mr. Chairman.

Mr. HORN. Thank you very much.

We now yield 5 minutes to the vice chairman of the Subcommittee on Government Management, Information, and Technology, the gentlewoman from Illinois, Mrs. Biggert.

Mrs. BIGGERT. Thank you, Mr. Chairman.

Mr. Miraglia, in the international activities, you mentioned the Y2K early warning system, and I understand that that will allow the U.S. nuclear power operators to monitor the status of the foreign nuclear power plants similar to their own, and that would give us about 12 to 15 hours that this will be ahead so that our plants will know if something is happening. But is there a similar system that would allow the U.S. nuclear plants, kind of looking across the United States, where there will be some in the west coast that will be following on later? Is there a plan in each of the plants in the different time zones to be able to know immediately if there is a problem?

Mr. MIRAGLIA. Yes. The "YEWS" system, the Y2K early warning system, is an Internet-based system. We have worked through NEA in trying to get foreign governments to subscribe to that system. At this time, there are about 25 countries that will be providing information. That information will be provided on a read-only basis to all of the nuclear power plants. We have indicated how they could subscribe and have access.

That information would also be shared with the Information Coordinating Committee of the President's Y2K Council to share that information throughout the community.

It is approximately a 17-hour head start if you go all the way to Australia and New Zealand and come across.

Mrs. BIGGERT. Then each one will have a contingency plan that will be based on—let's say, the communication, as Mr. Baird mentioned, would shut down. Is there a contingency plan that they would still be able to know?

Mr. MIRAGLIA. In terms of the "YEWS" system, that is a source of information to say what is happening elsewhere and can we glean some knowledge so we would be better prepared.

The contingency plans for the individual facilities are in place, and it would perhaps better prepare them to manifest for some potential impact. It should be within the context of the existing plans already, ma'am.

Mrs. BIGGERT. And you said that all of the 103 domestic plants are Y2K compliant. How was the verification of that compliance done?

Mr. MIRAGLIA. We said Y2K ready. There is a slight difference between compliance and ready.

In terms of the 103, we looked at the guidance documents that we endorsed, and in the context of those guidance documents and the audits that we did, we did focus inspections on the elements of that guidance.

GAO has indicated that it was a 450 question checklist, but in order to complete those lists you went and looked at individual, specific attributes of the guidance.

For example, five to six software systems and modifications were examined. Were they independently verified? Was there a peer review or was their quality assurance done on those aspects? And so those questions led to specific focused activities by the inspectors

to look at the various elements and were they complying with the guidance that we developed and endorsed. That would give us the confidence to say that appropriate assessments had been made, appropriate remediation had been done, appropriate testing and contingency planning had been completed.

Mrs. BIGGERT. Then was there a certification that they were compliant?

Mr. MIRAGLIA. In terms of our inspection activities, we would indicate in our inspection reports that were docketed for each of the facilities that we have completed those inspections and have concluded that they implemented the guidance and the guidance documents that would give us confidence in saying there is reasonable assurance of Y2K readiness of those facilities.

Mrs. BIGGERT. So are there remaining risks to our domestic nuclear facilities?

Mr. MIRAGLIA. In terms of absolute guarantees, they are very difficult. There are many computer systems, many embedded chips. The systems that we used and the guidance that we provided we believe provided a framework to appropriately assess, remediate, test, and have contingency planning, and we believe that we have a basis for reasonable assurance.

Mrs. BIGGERT. Thank you.

Thank you, Mr. Chairman.

Mr. HORN. Thank you very much.

We now move to—well, I see there is a pass down there, so we will begin the round again.

Mr. Beedle, when I was at the beginning of the first question, I think you had something you wanted to add to it. This is your chance.

Mr. BEEDLE. You had asked a question, Mr. Chairman, concerning audits of the plants, and I wanted to point out that each one of these utilities has had at least three audits of one variety or another, consisting of self audits by their own QA organizations, which are rather extensive, audits of one utility against another one, and then third party audits, where we bring in contractors. That gives us a great deal of confidence that the effort on the part of the utilities has been detailed and thorough in their examination of the Y2K issues.

Mr. HORN. When the Federal Government and the executive branch looked at the September 9, 1999, bit, there didn't seem to be much of a problem. Was there any problem in any of the nuclear reactors on that?

Mr. MIRAGLIA. Nothing was reported that was related to any Y2K event at any nuclear facilities, sir.

Mr. HORN. There are about 300 foreign nuclear power facilities, and often the so-called "facilities" and their safety standards don't meet the U.S. standard. Getting back to where are we in some of the international bit, what is your feeling on that? Have you been called upon for technical expertise by the International Atomic Energy Commission?

Mr. MIRAGLIA. Yes. We have provided, in terms of participating in workshops, we have participated in workshops on the guidance that was developed here. That was shared.



As NEI has indicated in their testimony here today, sir, that guidance has been used by a number of foreign countries to examine the Y2K issues.

We have participated in discussing Y2K contingency planning. I'm scheduled to participate in an IAEA workshop next week in Vienna to discuss what we have done relative to the contingency planning here in the United States, so there has been that type of activity.

In addition, we have worked through the Nuclear Energy Agency in developing the Y2K early warning system, and that has been another vehicle for us to indicate interest in activities that we have been engaged in.

Mr. HORN. Mr. Rhodes, we have read articles, we have heard people say that nuclear weapons have no Y2K problem; that is, that the weapons, themselves, have no dates or clocks, and therefore there really wouldn't, in relation to time. Is that really true?

Mr. RHODES. Yes, it is. We performed an audit of the nuclear weapons stockpile. I led the team. GAO went out from one of our sister divisions that handles the stockpile stewardship issues, and we did a complete design review of the nuclear weapons, themselves, what's called the "physics package," the actual weapon, and in the process walked through every electronic component, every design. I even did code walk-throughs.

In terms of time and a nuclear weapon, you are talking about a stop watch. Even those weapons that have chips in them, the chips don't have time. They get time from an external oscillating crystal, and that is just giving them a time interval. It is just a vibration, and they get an electrical impulse out of that vibration.

So all they are doing is counting up time. And, while they are counting up time, certain events are taking place.

So, I give you my professional opinion, and we have issued a letter stating that we have found that the U.S. domestic—well, the entire nuclear stockpile for the United States is not a Y2K issue.

They operate on what is called "fiducial time."

Mr. HORN. Well, without objection, we will put the letter and any summary you have of the review in the record at this point.

Mr. RHODES. I will make certain it gets to you.

Mr. HORN. I assume it isn't classified?

Mr. RHODES. No. There were many classified discussions, but it is an unclassified, public document.

Mr. HORN. Last month, Congress set up the National Nuclear Security Administration, which is being formed to run the Nation's nuclear weapons laboratories. In your opinion, GAO's, how should this organization work with the Department of Energy to manage our nuclear weapons, assets, and security measures? Has GAO done any work in that area?

Mr. RHODES. We haven't done any formal work on it, but we have worked on discussions about security at the Department of Energy, and one of the points, key points, I would want to make about the oversight that is being brought to the Department of Energy is—and being someone who has come out of the weapons complex, it is very hard for the complex itself to assess its own risk, and what it considers to be valuable may be different than what

the Department of Energy considers valuable may be different than what nationally is of value.

If the external structure that is being applied to the Department of Energy can assess the value of the assets regarding the nuclear weapons, that would be of great value. That would be of great importance to the agency. And that would be one of the key—I think one of the key tasks at hand is to make certain that everyone understands the export value of super computer equipment, the domestic development of certain materials, et cetera, and how they should be handled and safeguarded.

Mr. HORN. Well, continuing the second round, I will yield to Mr. Kanjorski, the ranking member.

Mr. KANJORSKI. Thank you, Mr. Chairman.

Mr. HORN. The gentleman from Pennsylvania.

Mr. KANJORSKI. Since all four of you gentlemen are experts, and since obviously the American people may be seeing this testimony, I would sort of like each one of you to render your expert opinion based on reasonable certainty of your various disciplines as to what your professional opinion is as to the safety of the nuclear industry—and stockpile system is included, just so that you get a shotgun starting off, Mr. Willemsen.

Mr. WILLEMSSEN. Well, as mentioned earlier by the NRC, there is no way we can give an absolute guarantee, but I think, through the efforts of NRC and the licensees, they have significantly reduced the remaining risk that is there.

We have some additional steps that we think the NRC can take to further reduce that risk to even a more microscopic level along the lines of what we have talked about today, for example, additional information on independent verification and validation. We'd also like to see some additional evidence of detailed day one planning at each of the nuclear plants—that is, the series of steps that they plan to take at the end of December and early January in the unlikely event that there are problems.

Mr. RHODES. Let me expand on one point that Mr. Willemsen touched on.

If you take an existing nuclear reactor and you look at a pump and you are basing your risk assessment and the emergency procedures based on the mean time between failure and the mean time to repair of an individual pump, you are taking a very large sample of equipment and you are trying to figure this probabilistic curve, and you say this individual pump failing has a probability of some value, some very small point. That is a probability based on standard manufacturing requirements.

The point that I would make in amplifying Mr. Willemsen's point about day one planning is that you go to any nuclear power plant and there are literally rooms filled with operating procedures. The people are well trained. You cannot become a senior reactor operator without tremendous training, tremendous background, recertification.

However, if that operator is operating according to normal emergency procedures where the probability of something going wrong may change because of an instability in communications or a perceived instability in the grid, then the point that Mr. Willemsen is making about that detailed day one planning, it is day one plan-

ning in light of the probability of a Y2K failure. It is not day one planning in light of the mean time between failure of a normal pump or the mean time between failure of a diesel generator or the mean time between failure of the grid.

Now you have a very focused event, you have a very focused bit of data that you are supposed to capture, and that is the basis for our recommendation about formal day one planning.

But I do concur that there is an extraordinarily low risk associated with nuclear power failure right now.

Mr. MIRAGLIA. In terms of the completeness of what we have done, if you look at the existing regulatory structure and what we have done to address the Y2K problem—and by the “we,” I mean the efforts of the industry and the agency, itself—I think we have reasonable assurance of continued safe operation of the facilities through the transition.

With respect to the points and suggestions made by GAO, I think, in terms of the independent verification and validation efforts, I believe, if one looks at the guidelines, the audits that we have completed, and the inspections, I think we have, in looking at that entire framework, addressed some of those suggestions.

With respect to the contingency plan, as Mr. Rhodes picked out, the uniqueness about the Y2K issue is that it is an event whose date is set. We know it is going to happen.

In terms of the contingency planning guidance that we have provided and endorsed via the industry guidelines, it does address the topics and the issues that are outlined in GAO’s letter of October 13th to the Federal agencies with respect to staffing, with respect to consumables, with respect to having additional contractor help, and security and those kinds of aspects are built into the guidelines for the contingency planning.

I think, in terms of what we have in place and what has been developed, it addresses those issues such that it complements and supplements the normal processes and procedures.

As Mr. Rhodes has said, the remediation and assessment addresses our attempt to try to keep the frequencies of failure to what is normally perceived by addressing the Y2K issue, and also designating specific contingency planning to assure that there is additional help and support during the transition.

So, with respect to the suggestions, we believe that we have encompassed most of those.

In your question, sir, you also asked for an opinion relative to the weapons stockpile, and I just want to say that I am not expert in that area and I would not offer an opinion.

Mr. BEEDLE. With regard to the operation of these plants, we daily train, daily operate and maintain these plants. Yes, equipment fails on occasion. The operators are prepared to deal with that.

We don’t see that the Y2K is going the present any different situation for the operator than they would on a normal operating day, but we recognize the vulnerability of the Y2K, and, as a result of that, we have tested, as I indicated, some 200,000 pieces of equipment and systems in these plants. We have had to remediate about 10,000 throughout the industry.

So we are talking about roughly 100 pieces of equipment or systems in each one of these plants that has been remediated, and they range from things of valve controllers, where we have embedded systems, to data collection and monitoring systems on these plants.

There are relatively few systems in these plants that are actually controlled by computers. They are all controlled by individuals, human beings that are at the control switches. For the most part, these systems monitor and provide indication of plant performance, rather than actual control of the equipment.

We have tested and verified that these systems will be ready for Y2K. We don't see that the vulnerability and risk to the plant is significantly different than the normal routine operational capabilities that we have with these plants today.

I, like Mr. Miraglia, really don't have any opinion with regard to the weapons programs.

Mr. KANJORSKI. Thank you, Mr. Chairman.

Mr. HORN. Thank you very much.

I now yield to the chairman of the House Science Technology Subcommittee of House Science, the gentlewoman from Maryland, who is co-chairman of the select task force of her committee and my committee.

Mrs. MORELLA. Thank you very much, Mr. Chairman.

Mr. HORN. You take as much time as you would like.

Mrs. MORELLA. Thank you.

I apologize to this expert panel for not being here earlier, but I was involved with a great technology and education event in Montgomery County, MD, which is where NRC is located, Mr. Miraglia, as you know, in that beautiful White Flint Building.

I do appreciate the testimony that has been given. I also appreciate the fact that I understand, Mr. Miraglia, that you commented on the fact that, of 103 operating nuclear plants, all but seven, I think, are Y2K compatible.

Mr. MIRAGLIA. That was updated during the testimony. There are four remaining.

Mrs. MORELLA. Only four remaining?

Mr. MIRAGLIA. Yes, ma'am.

Mrs. MORELLA. Maybe by the end of our hearing it will be down to one.

But I do appreciate the fact that this has been done. I'm certainly very laudatory about those efforts.

I guess the line of questioning that I would have would deal with how does your contingency plan at NRC differ from other contingency plans you might have. How does it differ from your usual emergency situation? I mean, do you have more safety people? How do you link up with coordinating with command control? Tell me what the difference is.

Am I explaining that clearly enough?

Mr. MIRAGLIA. I believe I understand your question, Madam Chairman.

Mrs. MORELLA. What new elements do you need and do you have?

Mr. MIRAGLIA. As I indicated earlier, there is an existing regulatory infrastructure for emergency response for off-normal circumstances.

Mrs. MORELLA. Right.

Mr. MIRAGLIA. As a result of Y2K, we have developed guidelines for the industry to develop additional contingency planning. That would supplement those kinds of activities.

In addition, our agency has augmented our own contingency plans and developed a Y2K contingency plan and provided that for comment, and we have coordinated with our other Federal agencies to indicate how we are going to operate during the transition period.

We will have inspectors at each of the 103 reactors during the transition. We are developing procedures and processes for them to look for, things to look for.

We have equipped each of those inspectors with satellite communications to maintain communications with our response center, which is located in White Flint. In addition, we have response centers at all four regional offices.

We will have additional staff at our response center in Washington. We would have a staff of 40 folks during the transition. We will have a smaller team manning the response center, about six on New Year's Eve, to start looking at the reports from across the international community and to monitor the transition within the facilities.

Each of our regional offices will have a team—regional administrators, senior managers, as well as a support team in each of our regional offices.

We have also planned, in the unlikely event if we lose communications with the headquarters response center, that that could be turned over to our region four office, which is in Arlington, TX. It is in a different time zone, it is on a different grid.

And we have exercised that contingency plan this past October and it was a very successful drill, notwithstanding we have learned some things to improve our ability during the transition.

So we are going to have additional staff and folks at the facilities, as well as our response centers.

Mrs. MORELLA. Is it important to let the community around these 103 operating nuclear plants know of the fact that you are prepared, and just to kind of assuage any concerns they may have? In other words, do you have any kind of a public relations outreach plan?

Mr. MIRAGLIA. In terms of the agency itself, through the Y2K President's Council we have participated, there have been the community outreach issues. Our sister agency, FEMA, has had regional meetings in and around certain of the nuclear power plants that the NRC has participated in. As discussed earlier here today, Madam Chairwoman, we did a table top exercise with the Baltimore Gas and Electric utility with their local representatives and implementers of the emergency plan, as well as the State.

We have encouraged the industry, through NEI, to inform the local community in what its state of readiness is, not only at the nuclear power plant but to also assure themselves that the tele-

communications and electrical supply and the reliability of that in the vicinity is known to them as well as to the local community.

Mrs. MORELLA. And, finally—because my time is expiring—what plans do you have for alternative energy if there are difficulties, breakdowns with the nuclear power? Isn't it 20 percent of our energy emanates—electrical energy emanates from nuclear power?

Mr. MIRAGLIA. In terms of the issue of reliability and the independent nature of our regulatory, statutory framework, our goal is to maintain the plants in a safe condition. Notwithstanding that, the Y2K issue does present a unique challenge to us. It is also important to maintain the facilities such that it doesn't adversely impact the grid.

The plants are designed to tolerate a loss of offsite power. There are emergency diesels onsite. Those are under normal maintenance and surveillance programs, they are tested. As part of the contingency planning, there will be no surveillance tests during the transition period. Fuel tanks would be topped off and things of that nature would occur.

So, in terms of maintaining a power supply available at the facility to maintain itself in safe shutdown, it will be done.

Without the grid, the plant cannot generate power to the grid, so the objective is to keep the plants in safe shutdown.

Mrs. MORELLA. Mr. Chairman, would you indulge me just one final question for the group?

Mr. HORN. Certainly. You may have all the time you wish.

Mrs. MORELLA. Thank you.

Let me ask our GAO people, Mr. Willemsen and Mr. Rhodes, do you feel pretty good that they are following your suggested actions? Would you have any final comments to make? I mean, should we feel comfortable that everything is proceeding as it should with the countdown of so few days?

Mr. RHODES. The point that I would make, as I mentioned earlier about the—you design emergency procedures in a nuclear power plant based on probability, and there are some very, very fine probabilistic analysts that work at all of the nuclear power plants.

But the probability today of the grid going down or the probability today of communications failing is different than when we hit the roll-over.

Our concern and our suggestion is based on, one, the independent validation and verification that, as Mr. Miraglia has pointed out, there has been either a peer review, a quality assurance analysis, or an independent validation and verification done at all the plants.

The point we would make is that NRC should take steps to make certain that a peer review, a quality assurance, and an IV&V are all equivalent.

Second point is that that gives you the basis for understanding what the probability of failure is going to be. If the probability of failure is actually going to be unique at that time, you need to extract from these huge, huge volumes of operating procedures and emergency procedures the exact set of steps that you think you are going to probably need to take for day one.

Now, that would affect, as you pointed out, staffing, consumables, et cetera. That would be the single point that we would make is

that, until we know that the peer review, the quality assurance, and the independent validation and verification are equivalent and complete, and that, as a result of those analyses, someone didn't decide that they needed to have independent testing of a device, or something like that, then saying that this room full of emergency procedures is going to cover all contingencies is probably true, but making certain that you are ready for the most probable failures is where our suggestion comes in.

Mrs. MORELLA. Did you agree, Mr. Willemsen?

Mr. WILLEMSSEN. Yes. I totally concur with Mr. Rhodes' comments.

Mrs. MORELLA. And, Mr. Miraglia, you do too?

Mr. MIRAGLIA. In terms of what I indicated, Madam Chairwoman, previously, is that in the content and scope and the concepts being offered, we agree. And I think our view is the steps and the framework that we have in place has addressed the issues raised by GAO.

Notwithstanding that, we appreciate the views that are expressed and we will look at those suggestions to determine if additional things need to be considered.

I think, in terms of the IV&V and the day one planning, when one looks at where we are and what we have done, I think we have essentially complied with the suggestions.

I think, in terms of what GAO may be indicating during their review, they were perhaps able to ascertain exactly what we had completed.

Mrs. MORELLA. Would you like to add anything, Mr. Beedle?

Mr. BEEDLE. Yes, I would, Chairwoman.

In developing this contingency plan that we provided to the utilities for implementation at each of the facilities, we have consideration for increased staffing, increased allocation of consumables in the event that you had some transportation problems. We wanted to make sure that you had adequate supplies and stocks.

We think that we have addressed each of the issues that the GAO has pointed out, and, in fact, we have had the GAO review this document and provided valuable input in the construction of this plan.

So everything that Mr. Rhodes is talking about is certainly valid, and, as Mr. Miraglia indicates, the NRC and I would add that the utilities, the licensees, are prepared to deal with those.

A failure at the plant is a failure that results in action by people, and we have people trained and prepared to deal with these issues.

Mrs. MORELLA. Thank you.

And thank you, Mr. Chairman. Thank you to the panelists.

Mr. HORN. Without objection, that document will be put in the record at this point.

[The information referred to follows:]

**Note:** An electronic copy of NEI/NUSMG 97-07 and NEI/NUSMG 98-07 may be obtained from the NEI public web site at [http://www.nei.org/library/y2k\\_arch.html](http://www.nei.org/library/y2k_arch.html)

The manuals are stored in pdf format.



**NEI/NUSMG 97-07**



**NUCLEAR UTILITY  
YEAR 2000 READINESS**

**OCTOBER 1997**

**NEI/NUSMG 97-07**

**NUCLEAR ENERGY INSTITUTE  
NUCLEAR UTILITIES SOFTWARE MANAGEMENT GROUP**

**NUCLEAR UTILITY  
YEAR 2000 READINESS**

**OCTOBER 1997**

**ACKNOWLEDGMENTS**

This document, *Nuclear Utility Year 2000 Readiness*, NEI/NUSMG 97-07 was developed with the assistance of an issue task force of industry managers dealing with current software issues. Timely development of this document was facilitated by use of the combined resources and expertise of the Nuclear Energy Institute and Nuclear Utilities Software Management Group. NEI wishes to acknowledge the extensive review and comments by the industry representatives who shaped the final form of this document.

**NOTICE**

Neither the Nuclear Energy Institute, nor any of its employees, members, supporting organizations, contractors or consultants make any warranty, expressed or implied, or assume any legal responsibility for the accuracy or completeness of, or assume any liability for damages resulting from any use of, any information, apparatus, method, or process disclosed in this report. Further, neither NEI nor any of its employees, members, supporting organizations, contractors or consultants make any warranty, expressed or implied, that such use does not infringe on privately owned rights.

## TABLE OF CONTENTS

Acknowledgments .....	i
1 INTRODUCTION .....	1
2 PURPOSE AND SCOPE .....	2
2.1 Purpose .....	2
2.2 Scope .....	2
3 DEFINITIONS .....	2
4 MANAGEMENT PLANNING .....	3
4.1 Management Awareness .....	3
4.2 Sponsorship .....	3
4.3 Project Leadership .....	4
4.4 Project Objectives .....	4
4.5 Project Management Team .....	4
4.6 The Management Plan .....	5
4.7 Project Reports .....	5
4.8 Interfaces .....	5
4.9 Resources .....	6
4.10 Oversight .....	6
4.11 Quality Assurance .....	6
5 IMPLEMENTATION PLAN .....	6
5.1 Awareness .....	7
5.2 Initial Assessment .....	7
5.3 Detail Assessment .....	9
5.4 Remediation .....	11
5.5 Y2K-Testing and Validation .....	12
5.6 Notification .....	12
6 QUALITY ASSURANCE .....	12
6.1 Project Management Quality Assurance .....	13
6.2 Implementation Quality Assurance .....	13
7 REGULATORY CONSIDERATIONS .....	14
8 DOCUMENTATION .....	14
8.1 Documentation Requirements .....	15
8.2 Project Management Documentation .....	15
8.3 Vendor Documentation .....	15
8.4 Inventory Lists .....	16
8.5 Checklists for Initial and Detailed Assessments .....	16
8.6 Record Retention .....	16

## APPENDIXES

A.	Communications Plan.....	A-1
B.	Inventory Instructions.....	B-1
	Device Survey Form.....	B-3
	Application Survey.....	B-4
C.	Compliance Specification.....	C-1
	Y2K Compliance Warranty.....	C-3
	Technical Criteria for Y2K Compliance.....	C-7
D.	Vendor Readiness Questionnaire.....	D-1
E.	Detailed Assessment Procedures & Checklists.....	E-1
	Assessment Plan.....	E-3
	Detailed Assessment Package.....	E-15
F.	Test Specifications.....	F-1
	Embedded Systems Testing.....	F-3
	A Millennium Survival Guide for IT Personnel.....	F-11
	Assessing Computer Software for Millennium Compliance.....	F-43
G.	Readiness Tracking Process.....	G-1
H.	Compliance Checklist.....	H-1
	Year 2000 Compliance Checklist.....	H-3
	Year 2000 Certification Checklist, Non-IS Supported.....	H-15



**NUCLEAR UTILITY YEAR 2000 READINESS****1. INTRODUCTION**

Nuclear utilities, like many other industries and government agencies, cannot satisfy their operating commitments without software. As nuclear utilities approach the turn of the century, they face a significant and complex task in resolving the Year 2000 (Y2K) problem in their software.

The problem occurs in some software because two-digit date fields were used to represent the year. In some software the logic fails when the "00" of year 2000 is inserted in the two-digit field. Others do not correctly identify the year 2000 as a leap year. The Y2K problem can affect software in mainframes, desktop computers, local area networks (LAN) or digital control systems.

No utility can escape the deadline and none are immune to the costs and responsibilities associated with this problem. Defining the exact severity and extent of Year 2000 problems is complicated by many factors:

- A large and diverse software inventory (typically 300 applications per nuclear unit),
- Numerous embedded systems that are difficult to inventory and test,
- The potential for operability issues or unreviewed safety questions (USQ) in safety system software,
- Costs - \$1 to \$3 million estimated at many units,
- The need to obtain information from vendors, and
- Limited time to identify and correct the problem, and significant staff requirements.

Nuclear facility licensees must ensure facilities are operated safely and in compliance with all license provisions. The Nuclear Regulatory Commission expressed their concern over this issue in Information Notice 96-70, "Year 2000 Effect on Computer Systems Software."

This document is the result of actions taken by the Nuclear Utility Software Management Group (NUSMG) in conjunction with the Nuclear Energy Institute (NEI) to provide the nuclear industry with an approach to resolve the Y2K problem.

This document suggests a strategy for a nuclear utility Year 2000 Project. This strategy recognizes management, implementation, quality assurance, and documentation as the fundamental elements of a successful Project. The NEI/NUSMG Task Force recognizes that any solution to the Year 2000 problem is an iterative process and many steps overlap as methods improve the testing and management will evolve through the feedback process.

## 2. PURPOSE AND SCOPE

### 2.1 Purpose

The purpose of "Nuclear Utility Year 2000 Readiness" is to recommend methods for nuclear utilities to attain Y2K readiness to ensure that their facilities remain safe and continue to operate within the requirements of their license. These methods and suggestions are designed to expedite completion and control costs.

### 2.2 Scope

"Nuclear Utility Year 2000 Readiness" applies to software, or software based system or interface, whose failure due to the Y2K problem would prevent the performance of the safety function of a structure, system, or component. This document also applies to any software, or software based system or interface, whose failure due to the Y2K problem would degrade, impair, or prevent operability of the nuclear facility. It is intended to supplement and use existing procedures used for software quality control, configuration management and problem reporting.

## 3. DEFINITIONS

3.1 **Year 2000 (Y2K)** — A term used to describe a set of date-related problems that may be experienced by a software system or application. These problems include: not representing the year properly, recognizing that the year 2000 is a leap year, and improper date calculations.

3.2 **Y2K Compliant** — Computer systems or applications that accurately process date/time data (including but not limited to, calculating, comparing, and sequencing) from, into and between the twentieth and twenty-first centuries, the years 1999 and 2000, and leap-year calculations.



- 3.3 **Y2K Ready** — 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.
- 3.4 **Validation** — A process that evaluates the functional characteristics of the software, and certifies the achievement of acceptable comparisons with Objective Evidence.
- 3.5 **Objective Evidence** — Any statement of fact, information, or record, either quantitative or qualitative, pertaining to the quality of an item or service based on observations, measurements, or tests that can be verified.
- 3.6 **Remediation** — Remediation is the process of retiring, replacing, or modifying software or devices that are to be retained in service, but have been determined to be affected by the Y2K problem.

#### 4. MANAGEMENT PLANNING

The management plan suggests an approach to establish, organize, manage, integrate, and complete a nuclear utility's Y2K project. The recommended components for the management plan are shown in the following systems.

##### 4.1 **Management Awareness**

The scope and nature of the problems that may occur in software systems at the turn of the century are not generally appreciated or understood at many levels of utility management. Correcting this condition is essential for a Y2K project to obtain the necessary levels of support, cooperation, and funding.

Communicating an awareness of the Y2K issues ensures that senior management, and their management team, understand the vulnerability of their utility. Senior management's attention to this problem indicates their commitment to maintaining the margin of safety and the operability of their facilities.

##### 4.2 **Sponsorship**

The Y2K project requires significant commitments of personnel, facilities, and funds. The project also requires support between, and by, many organizations within the utility. Available estimates indicate that even a single-unit utility project requires resource variances that are typically authorized by senior management. Senior management sponsorship is recommended.

#### 4.3 Project Leadership

The Y2K project requires a significant commitment of people knowledgeable of the commitments, strategic intent, culture, vulnerabilities, and capabilities of the utility. The project must be sufficiently staffed during the planning stage and continuing through completion. Since many tasks are required and many software systems evaluated, the resources must be allocated and managed effectively. The project requires strong, effective leadership.

The authority given to the project manager is largely a function of the number of units, the extent of the interfaces with suppliers, the complexity of the problems encountered, and the culture of the utility. The reporting level of the project manager should be established to ensure appropriate corrective measures are completed.

The project management may be a matrixed function that includes project managers from major organizations within the utility. However, this does not diminish the ultimate authority and responsibility of the individual that manages the overall project.

#### 4.4 Project Objectives

The project manager should fully understand the project sponsor's expectations concerning the major objectives of the project. This includes allocation of resources and schedule. The project manager should document the understanding of the project and obtain written agreement from the sponsor.

#### 4.5 Project Management Team

The project manager selects a project team that may include other managers, technical specialists and support staff seconded from functional organizations. This team may benefit from the participation of professionals that specialize in project management, cost and scheduling, outage management, and other disciplines.

The project team requires access to the skills of a multi-disciplined cross-section of the organization. This includes the process owners (system engineers, technicians, subject matter experts, etc.), information technology professionals, and support organizations such as engineering, licensing, quality assurance, procurement, and financial management. The use of consultants and contractors may be desired, or even necessary for completion of the project.

#### 4.6 The Management Plan

The project team may use this document to develop the approach that the utility will use to address the Y2K problem. The management plan documents the major milestones of the project and the schedule for completion. The management plan includes a description for addressing each item in Section 4 of this document.

The management plan identifies those responsible for creating the implementation plan (see Section 5), its content, and the procedures and controls to be used to manage the implementation the Y2K project. The management plan should indicate the strategies used to address or establish:

- Ownership of software changes,
- Vendor relationships and responsibilities,
- Communication and feedback from affected parties, and
- Contingency plans for unanticipated events at the point of the turn of the century.

The project sponsor and management of participating organizations approve the management plan and subsequent revisions.

#### 4.7 Project Reports

The project manager documents the progress of the project in status reports to the project sponsor and appropriate members of management. These reports should include details of key performance indicators such as numbers of systems addressed, expenditures, the current disposition of resources in the field, and schedule status.

#### 4.8 Interfaces

The project manager should ensure that interfaces to other organizations (electric utilities, telecommunications utilities, suppliers, emergency services, government offices, etc.) are considered for their importance to the objectives of the project. Interfaces that are identified should be addressed by ensuring that the responsible organization institutes an appropriate Y2K effort.

**4.9 Resources**

Significant resources will be required to complete the Y2K project. The project sponsor is accountable for allocating the resources agreed to in the project plan and meeting additional requests as the project matures.

**4.10 Oversight**

This project requires the project sponsor to remain actively engaged in the oversight of the project through completion. The project sponsor may also engage the services of outside organizations to supplement the oversight of the project.

**4.11 Quality Assurance**

Quality assurance measures are applied throughout the Y2K effort to include both the management and the implementation activities. These measures are structured to ensure that the performance of essential activities is supported by objective evidence. These measures are to ensure:

- Personnel participating in this project are qualified for assigned tasks,
- Activities that could affect safety or operability are accomplished using appropriate procedures, and
- Non-conforming conditions discovered during the conduct of the Y2K project that are determined not to be Y2K issues are identified and dispositioned in accordance with appropriate procedures.

Further details regarding quality assurance measures are presented in Section 6, Quality Assurance.

**5. IMPLEMENTATION PLAN**

Each project team defines the process and methods used to carry out the requirements of the management plan by developing implementation plans. The implementation plans for the project is approved by appropriate levels of management. The suggested phases of implementation include awareness, an initial assessment, a detailed assessment and notification.

## 5.1 Awareness

The purpose of the initial communications is to raise general awareness of the issue and to communicate its importance to the organization. The communication or indoctrination must be aligned to the audience. The audience includes the following:

- Management,
- Subject matter experts,
- System engineers,
- Software or system sponsors,
- General employees, and
- Support organizations such as procurement and engineering programs.

At a minimum, communications should include a description of the Y2K problem, the process or plans to address and remediate the problem, the significance or priority of the problem, the resources required and the schedule. An example of a communications plan is included as Appendix A.

## 5.2 Initial Assessment

The initial assessment consists of identifying software in use by the utility. This requires input and support from all participating organizations. Initial assessment consists of several steps.

### 5.2.1 Inventory

An inventory of all potentially affected items is required. The data collected is used to make initial decisions on categorization, classification, and prioritization. The data is also used to determine budget and resource estimates for the detailed assessment phase. The information collected may include the following:

- Software or device name,
- Version or model number,
- Description and use,
- Priority based upon importance to safety, operability, regulatory commitments, business considerations, etc.,
- Vendor or manufacturer, and
- Owner or support group.

Embedded systems are particularly difficult to inventory. The software components are often not recognized or apparent. Particular care should be taken to ensure that embedded systems are included in

the inventory. When systems are being examined to determine whether embedded components are within, the individuals tasked for this activity should be highly skilled in their design or use. Some suggested indicators that may be used to determine the presence of embedded software include:

- Searching procedures and documentation for the occurrence of phrases that would indicate the existence of an internal clock or processor,
- Surveying vendors for information on their equipment,
- Performing system walk-downs, and
- Reviewing schematics, programming listings, and reference manuals.

The guidance for collection of the inventory should include the types of items to list, the use of existing inventories, and information required for future actions and decisions. This is to ensure that all software within the scope of the project is evaluated for the Y2K problem and documented. Examples of inventory instructions are in Appendix B.

#### 5.2.2 Categorization

After the inventory is collected, a categorization of the inventoried items is performed. Categorization is the process that groups software, allowing management to efficiently assign resources to the classification and prioritization activities. Examples of categories are:

- Mainframe applications,
- System software (operating systems, databases, utilities, etc.),
- Client/server applications,
- Telecommunication equipment,
- Embedded devices,
- Process systems,
- PC's and servers,
- Test equipment, and
- Software interfaces.

### 5.2.3 Classification

After the inventory is categorized, each item within each category is classified. The process employed should reflect the importance of the item to the objectives of the project. Examples of classifications are:

- Safety-related,
- Important-to-safety,
- Required by regulations,
- Required by license commitments,
- Important to operation,
- Personnel safety,
- Continuity of business, and
- Non-essential.

### 5.2.4 Prioritization

Prioritization is the process of reviewing all items within the inventory after classification and assigning an order to the performance of the detailed assessment. Criteria used to set the priorities are established by the utility in their management plan. Examples include:

- Number of systems of a given type,
- The availability of individuals with required talents or experience, and
- Competing schedules such as equipment replacement and outages.

### 5.2.5 Analysis of Initial Assessment

The final step of the initial assessment is to determine the scope, schedule and estimated resources required for the detailed assessment based on the initial prioritization and categorization. This is a critical business consideration that requires significant resources to perform. Analysis of the data may require substantial management and technical resources and will certainly be an iterative process.

**Note:** Some items may not require detailed assessment and may be dispositioned as used-as-is.

## 5.3 Detailed Assessment

The purpose of the detailed assessment is to obtain sufficient information about each inventoried item to determine its expected performance beyond December 31, 1999. Written instructions, checklists or test procedures

should be developed to describe the detailed assessment process and provide for documentation and quality assurance of the work performed. Assessment results are used to make decisions regarding actions required to ensure the continued operation of the software. Several activities occur during the detailed assessment phase.

#### 5.3.1 Vendor Evaluation

It is essential to determine whether the software in question is vendor supplied so that responsibility for subsequent activities can be established. For software determined to be vendor supplied, but for which no vendor support is available or forthcoming, the software must be evaluated by the utility using their Y2K processes (see 5.3.2).

For vendor supplied software that the vendor supports, the utility needs to determine the appropriate commercial instrument (contract, license agreement, interface plan, etc.) to use, or institute, for subsequent activities. These activities may include remediation by the vendor, cooperative efforts with the vendor, or the issuance of a request for Y2K information and certification.

The development of a generic Y2K compliance specification for communicating the definition of compliance to vendors, the type of information requested, and the desired extent of documentation is beneficial. The vendor compliance specification may also be used for current purchases to ensure that only Y2K compliant software is purchased. Refer to Appendix C for an example of a compliance specification and Appendix D for an example of a vendor readiness questionnaire.

For vendor responses that indicate an application or device is Y2K ready or compliant, a decision on whether or not to perform validation testing is required. This decision may be based on the criticality of the item, prior experience with the vendor, the extent of documentation provided, or utility knowledge of the item.

#### 5.3.2 Utility Owned or Supported Software Evaluation

An assessment of the utility owned and supported applications and devices is performed using procedures or checklists. Appendix E contains examples of detailed assessment procedures and checklists. There are many methods for determining the Y2K operability of applications and devices including knowledge-based decisions, scanning (used for mainframe and some large client server applications) and testing.



Testing (see 5.5) may be used for Y2K assessments and requires the development of test specifications or procedures. Testing results often reveal the best strategy for remediation. Appendix F contains examples of test specifications.

### 5.3.3 Interface Evaluation

It is essential to coordinate interfaces between the software applications modified by the Y2K project and those maintained by other internal or external organizations. For example, the utility should ensure that all telecommunication equipment required under the scope of this project is Y2K compliant or ready.

The coordination and timing of such efforts presents many challenges and may require a high level of project management attention. Interfaces with external organizations should be identified early in the process and require regular management attention.

### 5.3.4 Remediation Planning

After an application or device has been determined to be susceptible to the Y2K problem, a business decision must be made. At issue is whether the software can be used as-is, or whether it must be retired, replaced or modified (RRM). This evaluation must be documented and should include the options evaluated, their cost, schedule, benefits, and risks. The results of the RRM decisions provide the input to the scope, schedule, and cost estimates for the remediation phase.

## 5.4 Remediation

The purpose of remediation is to retire, replace or modify software identified in the detailed assessment. The remediation phase requires the project to develop a process for tracking progress and evaluating the risks for items remediated. The process should track replacement projects, purchases, conversions, deletions, retirements, and vendor efforts (see Appendix G for examples of a readiness tracking process).

During remediation the utility should ensure proper software quality assurance controls and procedures are utilized. For unit equipment remediation, the work will need to employ existing station modification procedures.

### 5.5 Y2K-Testing And Validation

The purpose of Y2K-testing in support of evaluation efforts is to determine whether the Y2K problem is present. This testing is performed during detailed assessments.

The purpose of Y2K-testing subsequent to remediation is to determine whether those efforts have eliminated the Y2K problem and no unintended functions are introduced.

Y2K-testing may be performed at several levels:

- Unit testing focuses on functional and compliance testing of a single application or software module,
- Integration testing tests the integration of related software modules and applications, and
- System testing tests the hardware and software components of a system.

The purpose of validation is to determine that the software is capable of performing its intended function. Validation is performed subsequent to remediation and Y2K-testing.

Upon satisfactory validation, the project manager obtains from those performing the validation certification and documentation consistent with the requirements of the project. The certification should clearly indicate Y2K ready or compliant.

### 5.6 Notification

Affected parties, including users, and vendors, shall be notified of changes to the software or hardware. This includes changes to documentation that may also result from this project.

## 6. QUALITY ASSURANCE

Quality assurance measures are applied to processes and systems to provide a level of assurance that they will adequately perform their intended function. In the context of Y2K, processes refer to those activities that are managed by the project manager and performed to ensure the accomplishment of project objectives. Systems refer to software, digital processors, and associated files, documentation, and equipment pertinent to the Y2K Project.

The project manager should consider the quality assurance programs that exist within the utility and determine applicability to the Y2K project. This includes the nuclear programs, business programs used for non-nuclear applications, and commercial programs that apply to products that are supplied to others. The quality assurance measures may be graded in their application so the extent of the quality assurance activities is consistent with the importance of the item or process to safety and operability.

A nuclear quality program governs some systems addressed under this project. They are subject to the provisions in CFR 50 Appendix B, certain regulatory guides, and commitments in the licensee's Safety Analysis Report. The project manager ensures that the nuclear quality assurance program adequately implements applicable requirements to software systems.

#### 6.1 Project Management Quality Assurance

Quality assurance measures applied to the Y2K project should be performed in accordance with approved procedures. The measures should ensure that an appropriate level of oversight of the Y2K project is performed. This oversight may take the form of planned periodic audits, inspections at documented hold points, or reviews of approved documents. Oversight should be provided by individuals or groups not directly involved in the management of performance of Y2K project activities.

#### 6.2 Implementation Quality Assurance

Quality assurance measures should be applied to the implementation phase of the Y2K effort. In addition to those measures identified in Section 5, Implementation Plan, additional measures should be applied as follows:

The project manager should ensure:

- The system is classified and categorized according to nuclear safety,
- Pertinent system procurement information is obtained,
- Systems are placed, or retained, under a system of configuration management, and
- All systems completed are validated and their design and licensing basis are documented using approved procedures.

The measures should ensure that required remediation changes to the software, hardware, and affected documents are made and that affected groups and individuals are notified of the change.

**7. REGULATORY CONSIDERATIONS**

Appropriate reviews and/or evaluations are performed and documented. Those that apply are dependent upon the classification of the system. Examples include, but are not limited to:

- 10 CFR 50.59:
  - Safety Screenings
  - Safety Evaluations
  - Determination of Unreviewed Safety Questions
- NRC Safety Evaluation Reports
- Reportability Evaluations per:
  - 10 CFR 50.72
  - 10 CFR 50.73
  - 10 CFR 21
- Operability Determinations
- Reviews to determine the need for changes to:
  - Safety Analysis Reports
  - Technical Specifications
  - Technical Requirements Documents
  - Design Basis Documentation Procedures
  - Licensing commitments
- Radiological/non-radiological reviews
- Emergency data response system reviews
- Purchasing review
- Legal department reviews

**8. DOCUMENTATION**

Documentation of Y2K program activities and results serves several important purposes:

- Provide management's expectations and guidance on the conduct of the project,
- Collect the data needed to monitor and manage the progress of the project,
- Allow independent parties to review of the project during and after completion,
- Record the basis of the ready or compliance certification,

- Record the justification for leaving an application "as-is" but neither compliant or ready, and
- Record utility management and technical decisions in the event of litigation.

This section provides basic requirements and examples for organizing data collection and developing records for the project. Utilities should use existing Software Quality Assurance (SQA) and configuration management procedures as primary records of change control.

#### 8.1 Documentation Requirements

Utilities should prepare documents that demonstrate the completeness of their Y2K program efforts and record the disposition of each item in their inventory. Records should be formatted to support information retrieval. They should support the audit and oversight activities of the project.

#### 8.2 Project Management Documentation

Project management procedures and the documents generated through their use should be retained. They document the utility efforts to resolve the Y2K problem and the results of the many activities performed. The procedures and documents will also serve as legal records of the utility efforts to resolve a problem that has generally recognized legal liabilities.

Examples of records used to document management of the Y2K project are:

- Program procedures or plans used to define the requirements of the project,
- Inventory lists,
- Project tracking data,
- All records signed by management, and
- Status reports and financial reports.

#### 8.3 Vendor Documentation

Since most utilities use vendor software extensively, the management of vendor documentation poses a significant task. The records resulting from this task will be challenging to manage, understand, integrate with internal efforts, and disposition. The project should consider dedicating specific management resources to this topic. Vendor documentation includes:

- Letters to vendors,
- Vendor responses,

- Utility disposition or additional testing of the item, and
- Other correspondence files.

#### 8.4 Inventory Lists

An accurate inventory list is an essential document and forms the basis for generating other records. It also stands as the record of a complete and thorough assessment process. Inventory records that should be developed were identified in the implementation plan section.

#### 8.5 Checklists for Initial and Detailed Assessments

Checklists should be used for each application indicating progress through each step in the Y2K project. The checklist should be reviewed and completed by both the business subject matter experts and the technical team members who are responsible to support the item. The checklist should lead the responsible persons through the entire process in a manner that helps them properly evaluate the items and record their responses and comments to specific questions. An example of a Y2K checklist is provided in Appendix H, Certificates of Completion.

A Certificate of Completion should be prepared and signed by appropriate personnel for each application to indicate its final disposition. It represents management's approval both from a technical and business perspective. management's approval also indicates acceptance of risk when an application is not certified as compliant or ready.

It is prudent to have both the technical owner and the business owner document their concurrence with the final resolution and disposition of the application.

#### 8.6 Record Retention

Project records should be maintained in accordance with the utility's Software Quality Assurance (SQA) procedures, configuration management programs, recommendations of the legal department, and the project plans.

**NUCLEAR UTILITY YEAR 2000 READINESS**

**Appendix A**

**COMMUNICATIONS PLAN**





## **Introduction**

---

This document describes the communications plan for the Year 2000 Program. This plan addresses the range of communications needs required to raise awareness and inform COMPANY employees about the Year 200 Program.

The strategy ensures that stakeholders are kept informed about the program's goal, objectives, risks and progress according to plan.

It is important that all participants in the program are provided with materials to prepare them for their roles and responsibilities.

---

## **Audience**

The target audience for this document is COMPANY employees who use information technology and work in conjunction with the Year 200 Program Office.

This plan also can be used for external communications with third-party vendors, government regulatory agencies and the media.

## Communications Planning Requirements

Information in the matrix below outlines the Year 2000 communications needs.

- The target audiences -- internal and external.
- The objectives in communicating to the target audiences.
- The communication vehicles to use in communicating to the target audiences.
- The recommended messages for each target audience.

INTERNAL Target Audience	Communications Objectives	Communications Vehicles	Recommended Messages
<p>General COMPANY population. Includes all INTERNAL target audiences.</p>	<p>General awareness including:</p> <ul style="list-style-type: none"> <li>• Provide project background</li> <li>• Explain benefits to COMPANY</li> <li>• Describe risks to COMPANY</li> <li>• Provide overview of how the program is proceeding including a timeline and status.</li> </ul>	<ul style="list-style-type: none"> <li>• COMPANY Week</li> <li>• Technology Connection</li> <li>• Emphasis</li> <li>• Update Video</li> <li>• SCN Broadcast</li> <li>• Y2k Hotline</li> <li>• Y2k E-mail box</li> <li>• Y2k Web Page</li> </ul>	<p>COMPANY management understands the severity of the problem and has a team in place who is working to solve it in a timely and cost effective manner.</p> <p>Y2k impacts all employees who use information technology.</p>
<p>Client Contacts</p>	<p>Clarity about project progress including:</p> <ul style="list-style-type: none"> <li>• Status</li> <li>• Timeline</li> <li>• Impact</li> <li>• Explain work required.</li> <li>• Identify who will do that.</li> <li>• Identify how work will be accomplished.</li> </ul>	<ul style="list-style-type: none"> <li>• Inventory Spreadsheets</li> <li>• Detailed project schedules And work plans</li> <li>• Compliance sign off sheets</li> <li>• Presentations</li> <li>• Y2k Hotline</li> <li>• Y2k Web Page</li> <li>• Periodic briefings for department meetings</li> <li>• Steering Committee Briefings/Reports</li> </ul>	<p>Business Units are the owners of the technology and need to participate in the process.</p> <p>Client contacts are our single point of contact for all communications about the project.</p> <p>Client contacts need to dedicate time to the program on a periodic basis.</p> <p>Client contacts are essential to the success of the project.</p> <p>Client contacts will decide priority, and whether to repair, replace or retire applications.</p> <p>Client contacts will be required to sign off on Y2k compliance.</p>

INTERNAL Target Audience	Communications Objectives	Communications Vehicles	Recommended Messages
C&TS Support Staff	<ul style="list-style-type: none"> <li>· Clarity and project progress and delivery of technical information.</li> <li>· Status</li> <li>· Timeline</li> <li>· Impact to work</li> <li>· Describe when work will be required?</li> <li>· Identify who will do what.</li> <li>· Identify how work will be accomplished.</li> </ul>	<ul style="list-style-type: none"> <li>· Technical Documentation</li> <li>· Inventory Spreadsheets</li> <li>· Detailed project schedules and work plans</li> <li>· Compliance sign off sheets</li> <li>· Y2k Hotline</li> <li>· Y2k E-mail box</li> <li>· Y2k Web Page</li> <li>· TSC Help File</li> <li>· Briefings for department meetings</li> <li>· Presentations</li> </ul>	<p>C&amp;TS support staff are essential team members. Their knowledge of the technology is essential to the success of the project.</p> <p>C&amp;TS support staff will need to dedicate time to the project on a periodic basis.</p> <p>Y2k Program Team will work with C&amp;TS to solve technical issues.</p> <p>Y2k "fixes" will impact C&amp;TS work.</p> <p>If "outsourcing" is necessary, C&amp;TS will conform to Y2k standards and schedule.</p> <p>When necessary, C&amp;TS support will be required to sign off on Y2k modifications.</p>
Senior Management including the IT Policy Committee and UPC	<ul style="list-style-type: none"> <li>· Identify the objectives and Magnitude of the program.</li> <li>· Identify the business issues.</li> <li>· Explain the business/legal Risks.</li> <li>· Outline strategic decisions that need to be made on an ongoing basis.</li> </ul>	<ul style="list-style-type: none"> <li>· Program Office Documentation</li> <li>· Regular status reports</li> <li>· Summary level schedules and work plan</li> <li>· Program Job Estimate</li> <li>· Issues list</li> <li>· Risk Assessment</li> </ul>	<p>Business units are responsible for funding and strategic decisions about the Y2k program.</p> <p>Senior management's commitment and involvement is essential to the success of the program.</p> <p>The program runs a high risk of failure if senior management is not committed.</p> <p>Senior management runs the risk of legal liability if due diligence is not exercised.</p> <p>Low priority and unidentified applications will not be Y2k compliant by 1/1/2000.</p> <p>Significant competitive advantage can be obtained by a successful Y2k program implementation.</p> <p>Senior managers and/or a designee will be required to sign off on Y2k modifications.</p>

INTERNAL Target Audience	Communications Objectives	Communications Vehicles	Recommended Messages
Law	<ul style="list-style-type: none"> <li>· Describe the legal issues related to Y2k.</li> <li>· Identify the third-party software contractual issues related to Y2k.</li> <li>· Define Y2k compliance for COMPANY.</li> </ul>	<ul style="list-style-type: none"> <li>· Trade press articles</li> <li>· Briefings from law firms with Y2k practices</li> <li>· Legal analysis drafted by COMPANY's law department</li> <li>· Y2k third-party contract Warranty language</li> <li>· Y2k third-party compliance Sign off document</li> </ul>	<p>The Corporation and its officers run the risk of legal liability if due diligence is not exercised.</p> <p>Third-party vendors must deliver a Y2k compliant product.</p> <p>Legal action will be taken if third-party vendor products are not made Y2k compliant in a timely fashion.</p>
Third-Party Software Vendors	<ul style="list-style-type: none"> <li>· Identify the third-party software contractual issues related to Y2K.</li> <li>· Define Y2k compliance for COMPANY.</li> </ul>	<ul style="list-style-type: none"> <li>· Y2k third-party contract warranty language</li> <li>· Y2k third-party compliance sign off document</li> </ul>	<p>Third-party vendors must deliver a Y2k product.</p> <p>Legal action will be taken if third-party vendor products are not made Y2k compliant in a timely fashion.</p>
Government Agencies- CPUC, FERC	<ul style="list-style-type: none"> <li>· Taking a proactive approach, describe how COMPANY is working towards Y2k compliance.</li> <li>· Respond effectively to any required regulations.</li> </ul>	<ul style="list-style-type: none"> <li>· COMPANY Week</li> <li>· Summary level schedules and work plan</li> <li>· Responses to regulatory requests</li> </ul>	<p>COMPANY management understands the severity of the problem and has a team in place who is working to solve it in a timely and cost effective manner.</p>
Media	<ul style="list-style-type: none"> <li>· Describe how COMPANY is working towards Y2k compliance.</li> <li>· Cost to rate payers.</li> </ul>	<ul style="list-style-type: none"> <li>· News Articles</li> <li>· Press Releases</li> </ul>	<p>COMPANY management understands the severity of the problem and has a team in place who are working to solve it in a timely and cost effective manner.</p>

## Communications Responsibility Matrix

The Communications responsibility matrix outlines who does what in the communications process. The communications process requires the participation of all members of the Year 2000 team.

Communications Process	Program Manager	Communications Manager	Program Office	Steering Committee
1. Establishes Recommended Messages	▪	·	·	·
2. Identifies/Confirms Target Audiences	·	▪	·	·
3. Selects Communications Vehicle(s)	·	▪	·	·
4. Designs Communications Message	·	▪	·	·
5. Develops Communications Message	·	▪	·	·
6. Reviews Communications Message	▪	·	·	·
7. Approves Communications Message	·	·	·	▪
8. Secures Communications Approval(s)	▪	·	·	·
9. Delivers Communications Product	·	▪	·	·
10. Incorporates Lessons Learned into Future Communications Products.	·	▪	·	·

▪ Leads · Contributes

## Program Office Staff

Name Position	Phone Extension	ID	Cube Number

## Communications Vehicles

The following chart shows the various vehicles used for Year 2000 communications within the company. Contacts are also listed.

Written	Contacts	Phone
E-mails	Program Manager/Communications Mgr.	
E-mail box Y2kemail@AsiCms@CTS	Communications Mgr.	
Fact Sheet (Q&A, Scripts, etc.)	Program Manager/Communications Mgr.	
Help Browser	C&TS	
Intranet/Web Page	Corp. Comm. Info. Tech.	
Mailers - Letters/Memos (internal)	Program Manager/Communications Mgr.	
Media Contact Information	Corp. Comm.	
News Papers (external)	Corp. Comm.	
Technology Connections	C&TS	
COMPANY Week	Corp. Comm.	
Emphasis	Corp. Comm.	
Posters in Lobby	Corp. Comm.	
Press Release (external)	Corp. Comm.	
Printers (internal)	Corp. Comm.	
Trade Journals (external)	Corp. Comm.	

Verbal	Contact	Phone
Booths at Special Functions	Program Manager/Communications Mgr.	
Employee Year 2000 Hotline	Program Manager/Communications Mgr.	
Manager Presentations	Program Manager/Communications Mgr.	
Radio Spots (external)	Corp. Comm.	

Visual	Contact	Phone
Broadcasts - SCN One-way	Corp. Comm.	
Television Spots (external)	Corp. Comm.	
Update Video	Corp. Comm.	
Video Projects	Corp. Comm.	

NEI/NUSMG 97-07  
October 1997

The following chart shows the various vehicles used by the Year 2000 Program Office to disseminate Program status information. Contacts are also listed.

Written	Contacts	Phone
Status Reports to Utility Policy Committee - Quarterly Basis	Program Manager	
Status Reports to the Strategic Information Technology Policy Committee	Program Manager	
Monthly Project Status Reports to the PMO	Program Manager	
Help Browser	C&TS	
Intranet/Web Page	Corp. Comm. Info. Tech.	





**NUCLEAR UTILITY YEAR 2000 READINESS**

**Appendix B**

**INVENTORY INSTRUCTIONS**



Device Survey

NEI/NUSMG 97-07  
October 1997

Y2K - Device Survey  
Completed by:

Site:  
Date:

This survey is intended to identify any device/equipment that may have YEAR 2000 implications.

Information needed to complete this form:

- 1) Device/Equipment # - Device name or equipment number.
- 2) Device location - where is the device located.
- 3) Primary System/User Group - who owns/maintains the device.
- 4) Number Used - Total number of devices on-site.
- 5) Functional Description - Brief business description of the devices function.
- 6) Business Criticality:
  - 5 - The date implications impact personnel safety, safety systems, or lost generation.
  - 4 - The date implications impact systems important to safety or regulatory commitments .
  - 3 - The date implications could cause substantial financial impact.
  - 2 - The date implications could cause some financial impact, but work arounds exist.
  - 1 - The date implications can cause minor financial impact, but are not a priority.

**Please choose one of the above.**

7) External Agent/Vendor - Name of Company/Contact  
(External Agent - Information exchanged outside of Company)

8) Vendor Address

- 9) Y2K Impact:
  - 5- Dates are used to determine calculation outputs.
  - 3- Dates are only used in printed output; no calc impact.
  - 1- No impact

**Please choose one of the above.**

10) Planned Retirement: Is device planned for replacement if so when will replacement be complete. If replacement is not planned enter NO.

11) Comments

Application Survey

NEI/NUSMG 97-07  
October 1997

Y2K - Application Survey  
Completed by:

Site:  
Date:

This survey is intended to identify any application software that may have YEAR 2000 implications.

Information needed to complete this form:

- 1) Application - The name the application is commonly called.
- 2) Functional Description - Brief business description of the application function.
- 3) Business Sponsor: Who is the primary business sponsor for this application. ex: BEST, group, individual.
- 4) User(s) Group: What groups use this application.
- 5) Supported by: LIT(L), Individual(I), Vendor (V)
- 6) Business Criticality:
  - 5 - The date implications impact personnel safety, safety systems, or lost generation.
  - 4 - The date implications impact systems important to safety or regulatory commitments.
  - 3 - The date implications could cause substantial financial impact.
  - 2 - The date implications could cause some financial impact, but work arounds exist.
  - 1 - The date implications can cause minor financial impact, but are not a priority.

**Please choose one of the above.**

7) Targeted for Replacement/YR: Is device planned for replacement, if so when will replacement be complete. If replacement is not planned enter NO.

- 8) Y2K Impact, if known: 5- Dates are used to determine calculation outputs.
  - 3- Dates are only used in printed output; no calc impact.
  - 1- No impact

**Please choose one of the above.**

9) External Agent/Vendor - Name of Company/Contact  
(External Agent - Information exchanged outside of Company)

10) Vendor Address

12) Development Tools: Tools used to develop application. (ex. Tool/Database/Operating System: VB/Sybase, EXCEL, WIN95, DOS, etc)

13) Comments:

**NUCLEAR UTILITY YEAR 2000 READINESS**

**Appendix C**

**COMPLIANCE SPECIFICATION**



**YEAR 2000 COMPLIANCE WARRANTY**

This Agreement is made this \_\_\_\_\_ day of \_\_\_\_\_, 1997 by and between

\_\_\_\_\_ ("Seller"),

a \_\_\_\_\_ corporation and \_\_\_\_\_ ("Buyer")  
(State)

a \_\_\_\_\_ corporation.  
(State)

**WITNESSETH:**

WHEREAS, Seller and Buyer have entered into an AGREEMENT dated \_\_\_\_\_ for the \_\_\_\_\_ of \_\_\_\_\_.

WHEREAS, when computational resources (hardware, software and firmware), begin mixing dates from 19xx and 20xx, various and uncertain results can be produced and

WHEREAS, Buyer is aware that various and uncertain results in computational resources can be produced; therefore, it has created the **TECHNICAL CRITERIA FOR YEAR 2000 COMPLIANCE**, a copy of which has been furnished to Seller; and

WHEREAS, Buyer and Seller desire to modify the above referenced AGREEMENT to make it comply with the **TECHNICAL CRITERIA FOR YEAR 2000 COMPLIANCE**.

NOW, THEREFORE, the parties agree to amend the above referenced AGREEMENT as follows:

Y2K Compliance Warranty

NEI/NUSMG 97-07  
October 1997

## A. YEAR 2000 COMPLIANCE

1. Seller represents and warrants that the Product sold, licensed, or provided by Seller to Buyer for Buyer's use is and will continue to be "Year 2000 Compliant", as defined in Buyer's **TECHNICAL CRITERIA FOR YEAR 2000 COMPLIANCE**.

## B. TESTING

1. Seller warrants that the Product has been tested by Seller and has determined that the Product is Year 2000 Compliant.
2. Seller shall deliver the test plans and results of such test upon written request from Buyer.
3. Seller shall deliver documentation listing for each remediation, the location within the Product and the technique used to remediate, upon written request from Buyer.
4. Seller agrees to participate in additional tests of the Product at no charge to Buyer, to determine Year 2000 Compliance.
5. Seller shall notify Buyer immediately of the results of any tests or any claim or other information that indicates the Product is not Year 2000 Compliant.

## C. LIABILITY

Notwithstanding any provision in the above referenced agreement to the contrary, Seller agrees to indemnify and hold Buyer and its shareholders, officers, directors, employees, agents, successors, and assigns harmless from and against any all claims, suits, actions, liabilities, losses, costs, reasonable attorney's fees, expenses, judgments, or damages, whether ordinary, special, or consequential, resulting from any third-party claim made or suit brought against Buyer or such persons, to the extent such claim or suit results from Seller's breach of the warranties contained herein.



## D. OBLIGATION

1. To the extent that it is determined by Buyer in its reasonable discretion that the Product is not Year 2000 Compliant, Seller agrees to immediately formulate and implement a written plan of action within ninety (90) days to modify the Product to make it Year 2000 Compliant.
2. A copy of such plan of action shall be delivered to Buyer within ten (10) business days after completion of same.

## E. PROVISIONS

1. This warranty shall begin as of the date of this Agreement, shall be perpetual, and shall survive any other expiration of warranty period or the termination of this Agreement. This warranty shall not be modified except by written agreement signed by both parties.
2. Any provisions of the License or other Agreements which limit or eliminate the liability of either party shall have no application with respect to the Year 2000 Compliance Warranty set forth herein.
3. In the event that Buyer is entitled to modify the Product pursuant to any Licensed or other Agreement, Buyer agrees that it shall not modify the Product in any manner which would affect the performance of the Product in such a manner as to cause it to fail to meet the Year 2000 Compliance Technical Criteria (as defined in Section A).
4. There shall be no Liability on the part of Seller for any failure of the Product to conform to the Year 2000 Compliance Technical Criteria (as defined in Section A) to the extent that any such failure is attributable to a modification of the Product by Buyer.
5. In the event of any conflict or apparent conflict between the terms and conditions of the License or other Agreements and the terms and conditions of this Year 2000 Compliance Warranty, the terms and conditions of the Compliance Warranty shall take precedence. Except to the extent otherwise set forth herein, the terms and conditions of the License or other Agreement shall remain in full force and effect.

Y2K Compliance Warranty

NEI/NUSMG 97-07  
October 1997

6. This Compliance Warranty, together with the License or other Agreement, constitutes the entire agreement between the parties with respect to the subject matter hereof.

F. Except as modified herein the Agreement dated \_\_\_\_\_ shall remain in full force and effect.

IN WITNESS WHEREOF, THE PARTIES HAVE EXECUTED THIS AGREEMENT AS OF THE DATE FIRST ABOVE WRITTEN.

BUYER:

SELLER:

By: \_\_\_\_\_

By: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

**TECHNICAL CRITERIA FOR YEAR 2000 COMPLIANCE****I. INTRODUCTION****BACKGROUND**

The Year 2000 situation arises from the use of only two digits for the year, ignoring the two digits which denote the century. When computational resources, both hardware and software, begin mixing dates from 19xx and 20xx, various and uncertain results can be produced. At one extreme, the computation may fail immediately at the point of an error, thus alerting users of the problem. At the other extreme, a particular computation may use dates and times in such a way as to not experience any problem whatsoever. The most dangerous results fall in the middle ground. In that case a date usage problem occurs, but the process continues using the incorrect data, without being noticed.

Addressing the Year 2000 problem is an urgent matter. However, addressing the problem without some up-front analysis could impact the overall goal of achieving timely and cost-effective Year 2000 compliance. The organization should begin its Year 2000 compliance program by clearly defining criteria for compliance and establishing baseline standards for going forward.

The purpose of this document is to provide a standard enterprise-level definition of "Year 2000 compliance" and how compliance will be implemented. It is intended to be used by all Company entities as a framework for achieving enterprise-wide compliance. The enterprise-level definition of compliance will identify the technical elements of the Year 2000 challenge for criteria for Year 2000 compliance, and a standard interpretation of the criteria.

Official notification and communication of the compliance definition and standards will be made with the publication of this document to the entire enterprise. This document will undergo revisions as we move forward with the Year 2000 program. Any changes or revisions to this document will be reviewed and approved by the Year 2000 program management team, and formally communicated to the organization as part of the Year 2000 communication strategy.

**DEFINITIONS**

For the purposes of this document, the following definitions apply:

1. Computational Resources

All applications of programming, primarily software but also including firmware or embedded programming in hardware. All criteria apply to computational resources in combination.

a. Software

Includes operating systems, end-user application programming, third party vendor software, networking software, real-time and batch programming software, telecommunications programming, process control and monitoring software, etc.

b. Firmware and Microcode

Includes PLCs, EPROMs or any other programmable hardware changeable by persons other than the OEM.

c. Hardware

Primarily BIOS chipsets, but also includes embedded programming in automobiles, elevators, clocks, HVAC systems, telecommunications, etc. Also applies to the entire combination of electronic equipment used for calculational processes.

2. DBMS

Data Base Management System, such as DB2, Oracle, Sybase, ADABAS, etc.

3. Julian (Ordinal)

Refers to a method of displaying date in which the 2-digit year and the sequential day within that year are shown as "YY.DDD". For example, September 20, 1996 is the 264th day of that year, so the Julian representation of that date would be "96.264".

## II. TECHNICAL ELEMENTS

The technical elements of the Year 2000 remediation involve the computational processes of accepting, creating, manipulating, and outputting calendar-related information. The primary study effort has been on whether computational resources can properly process the change of century to the year 2000. This is of course a high-risk concern, and should be of primary importance to remediation efforts. However, several other date-related problems exist in association with the Year 2000 date rollover. These are summarized in Table 1.

Table 1. Technical Elements of the Year 2000 Challenge

Element	Description	Example Event	Probable Timing
Century Ambiguity	<p>This is the most common element. Computer represents dates with a 1- or 2-digit year. When computer does not recognize that dates are not all in the 19xx range, the results are unpredictable.</p> <p>a. Data edits reject years in early 20xx as invalid</p> <p>b. User interface does not allow 4-digit year to clarify century.</p> <p>c. Sorting leaves dates in 20xx and 19xx in jumbled order.</p> <p>d. Durations such as invoice aging are calculated incorrectly.</p> <p>e. The century is truncated or changed between entering and retrieving a date.</p> <p>f. Comparing a date in 19xx with a date in 20xx assumes both are in 19xx.</p>	<p>Examples of century ambiguity can appear in the following events:</p> <p>a. Bank ATM rejects an otherwise valid bank or credit card with an expiration date of "00".</p> <p>b. Lotus 1-2-3 accepts only 2-digit years which it assumes to be in 19xxly.</p> <p>c. Itemized monthly bill lists transaction for Jan 1, 2000 through Jan 15, 2000 followed by Dec. 19, 1999 through Dec. 31, 1999.</p> <p>d. Invoice age calculated as a ridiculously large number or as negative number, erroneously triggering overdue notices and staggering interest penalties.</p> <p>e. Software stores dates in the 20xx range using DBMS but only passes 2-digit years to the product. DBMS defaults to 19xx and stores.</p> <p>f. Payroll-deduction calculations for years in 20xx incorrectly mistake the year as 19xx and fail to apply recent changes in tax laws.</p>	<p>Examples of events can occur with timing as early as:</p> <p>a. First use of cards issued in 1995.</p> <p>b. First need to enter values later than 1999. Has already occurred.</p> <p>c. First monthly data processing in 2000.</p> <p>d. January, 2000</p> <p>e. Could happen in 1996 for systems with 5-year time horizon.</p> <p>f. First quarter of 2000.</p>

Table 1. Technical Elements of the Year 2000 Challenge (continued)

Element	Description	Example Event	Probable Timing
Extended Semantics	In general, specific values for a date field are reserved for special interpretation. The most common example is interpreting "99" in a 2-digit year files as an indefinite end date, i.e. "does not expire". Another is embedding a date value in a <i>non-date</i> data element.	Some software may erroneously process a transaction with a valid end date in 1999 - such as not terminating an expired software license or failing to age back-up tapes for recycling as scratch tapes.	Will occur on various days after Dec. 31, 1998.
Calendar Errors	Errors typically include failing to treat 2000 as a leap year and converting incorrectly between date representations. Day-of-week may also be incorrect, since the year 2000 begins on a Saturday, while 1900 begins on a Monday.	Logic sensitive to day-of-week will be two days off at the beginning of the year, and an additional day off after February 28, 2000. Calculating day of week for all dates following this will be incorrect.	Day of week error will occur Jan 1, 2000. Leap year error will occur the first time input data contains Feb. 29, 2000.
Date Overflow	Many computer products represent dates internally as a base date/time plus an offset in days, seconds, or microseconds since that base date/time. Integers holding the offset value can overflow past the maximum corresponding date - an event which may lead to undefined behaviors.	Value for date can revert to a date near the base date/time, to a negative value, or crash the computer because of an illegal operation.	Happened in the 1980s on certain Tandem hosts. Could happen again at any time to any product depending on how product stores dates.
Inconsistent Semantics	At interface between systems, each side assumes semantics of data passed; systems must make same century assumptions about 2-digit years.	Software on one side assumes all dates in 19xx. Software on other side assumes years 51-99 are 19xx, and 00-50 are 20xx.	Could happen in 1996 for software that stores date values 5 or more years into the future.

**III. CRITERIA FOR YEAR 2000 COMPLIANCE**

This document requires that computational resources satisfy the General integrity and Date integrity criteria, and either the Explicit or Implicit century criteria. It is preferred and recommended that both the Explicit and Implicit criteria be met if possible, although meeting one or the other of these criteria is acceptable. Resources (hardware, software, or "firmware") that meet these conditions will be considered "Year 2000 Compliant". These criteria are listed in Table 2.

**Table 2. Four Criteria for "Year 2000 Compliance"**

Criterion	Description
General integrity	No value for <i>current date</i> will cause interruptions in desired operation.
Date integrity	All manipulations of calendar-related data (dates, durations, days of week, etc.) will produce desired results for all valid date values within the operational domain.
Explicit century	Date elements in interfaces and data storage permit specifying century to eliminate ambiguity.
Implicit century	For any date element represented without century, the correct century is unambiguous for all manipulations involving that element.

Each criterion as described in this table is intended to be a general requirement. The following sections describe the criteria in more detail.

**A. General Integrity**

As a system date advances normally on a computer resource, each date roll-over must not lead the computer resource (including, but not limited to, the host processor and any software executing there) to erroneous processing. This must also be true if the system date is regressed to a prior date. All date roll-overs must be transparent to the user.

The best-recognized, high-risk date change is roll-over to 2000, although all other roll-overs such as Feb. 29 also apply. The term "desired operation" in Table 2 is intentionally broad and must be interpreted for specific technologies and applications.

**B. Date Integrity**

This criterion primarily covers the correctness of manipulations of date data as described in Table 3. These manipulations need to be reliable only over the range of dates that a computer resource is expected to handle.

For example, sales-order processing may handle dates from 5 years in the past to one year in the future. In contrast, an employee database may store dates of birth from early in the 20th century to planned retirement dates well into the 21st century.

**Table 3. Variety of Manipulation of Date Data**

Category	Examples of Manipulation
Arithmetic	<ul style="list-style-type: none"> <li>• Calculate the duration between two dates</li> <li>• Calculate date based on starting date and duration</li> <li>• Calculate day of week, day within year, and week within year</li> <li>• Hashing calculation using year as divisor</li> </ul>
Branching	<ul style="list-style-type: none"> <li>• Compare two dates</li> </ul>
Format	<ul style="list-style-type: none"> <li>• Convert between date representation (YMD, Julian, etc.)</li> <li>• Reference same data address with different variables</li> </ul>
Data Storage	<ul style="list-style-type: none"> <li>• Storing and retrieving</li> <li>• Sorting and merging</li> <li>• Searching</li> <li>• Indexing on disk file or database table</li> <li>• Moving data within primary memory</li> </ul>
Extended Semantics	<ul style="list-style-type: none"> <li>• "99" as special value for year</li> <li>• "99.365" as special value for Julian year</li> <li>• "00" as special value for year</li> </ul>

#### C. Explicit Century

This criterion essentially requires the *capability* to store explicit values for century.

For example, third-party products that can use a 4-digit year in all date data elements stored and passed across each interface (including the user interface) would satisfy this criterion. A base-and-offset representation of dates that covers all centuries of interest would also satisfy this criterion. Whether this capability *should* be used to eliminate century ambiguity is part of the last criterion.

#### D. Implicit Century

This last criterion requires that, if the century is not explicitly provided, its value can be correctly inferred with 100% accuracy from the value of date provided.

For example, the range of values for an "invoice date" would very rarely span more than 10 years. Because the century can always be guessed correctly from an invoice date with a 2-digit year, this date data element would satisfy this criterion.



Note that this criterion permits cost-risk trade-offs that minimize changes to existing date formats.

#### IV. INTERPRETATION OF THE CRITERIA

##### A. STANDARD INTERPRETATION

Although these four criteria fully define Year 2000 Compliance, compliance represents a balance between cost and risk rather than an absolute yardstick. Such a balance will vary with each organization, according to its business needs and technological base. Consequently, organizations will possibly require a greater level of detail to absolutely interpret how these criteria apply to that organization.

Table 4 contains the standard interpretation of these criteria. Any deviation from this interpretation in a Company organization must be documented and approved by both the organization and by the provider of the computational resource.

Note the importance of clearly identifying the specific date ranges for compliance, reasonable latitude in date format, and situations under which implicit century values will be tolerated. Also note that certain exceptions are included to support important options for cost/risk trade-off.

Table 4. Interpretation of Year 2000 Compliance Criteria

Criterion	Description of Criterion	Interpretation of Criterion
General Integrity	No value for current date will cause interruptions in desired operation.	<ul style="list-style-type: none"> <li>All computational resources will function correctly, without human intervention, and transparent to the user, for all values of system date between 1900-01-01 and 2050-12-31</li> <li>Of special interest are the following dates and the ability to roll over forwards and backwards to the correct next date: 1998-12-31, 1999-09-09, 1999-12-31, 2000-01-01, 2000-02-28, 2000-02-29, 2000-03-01, 2000-12-31, 2001-01-01, 2027-12-31.</li> </ul>
Date Integrity	All manipulations of calendar-related data (dates, durations, days of week, etc.) will produce desired results for all valid date values within the operational domain.	<ul style="list-style-type: none"> <li>Computing resources must correctly handle all representation and manipulation of dates with values between 1900-01-01 and 2050-12-31. Especially important is that all years divisible by 4 in this 150-year range are leap years except 1900.</li> <li>All computational resources developed for the Company must initialize all date elements with either all zeros (0000-00-00) or null values. Null values are defined for each application by the development facilities, such as the language compiler. A null-value feature is strongly recommended in third-party product selection.</li> <li>All developed software must not contain literals or constants for dates unless required to capture specific business rules such as calculations of payroll deductions.</li> <li>All developed software must not use special date values as logical flags, such as "99" as year to mean "no end date" or "00" to mean "does not apply".</li> </ul> <p><b>Exceptions:</b></p> <ul style="list-style-type: none"> <li>Valid date ranges in existing developed or existing third-party software may start with the oldest date value in the application's archived data rather than 1900-01-01 when there is no business need to support earlier dates.</li> </ul>

Table 4. Interpretation of Year 2000 Compliance Criteria (continued)

Criterion	Description of Criterion	Interpretation of Criterion
Explicit Century	Date elements in interfaces and data storage permit specifying century to eliminate date ambiguity.	<ul style="list-style-type: none"> <li>All developed and third-party software must permit the use of date formats which explicitly specify century in all date data stored or transmitted. The format of these date elements must be YYYYMMDD or YYYYJJJ as specified by ANSI X3.30-1985(R1991) unless superseded by another application-specific standard or convention.</li> <li>In storing or transmitting date data, some applications must conform to domain-specific standards, contractual agreements, or APIs to necessary third-party products whose date formats must supersede ANSI X3.30 as appropriate in the application. Examples in Table 5.</li> <li>Third-party products must permit formatting data with explicit century in the user interface.</li> <li>All developed applications using third-party products must always explicitly supply century and never rely on those products' default value for century.</li> </ul> <p><b>Exceptions:</b></p> <ul style="list-style-type: none"> <li>For date data formatted for a user interface, it is acceptable to use punctuation (slash, hyphen, period, comma) within a formatted date, to spell out or abbreviate the name of the month, or to reorder year-month-day to serve customs among the end users.</li> <li>DBMSs which cannot store date in conformance with SQL standards but do store century explicitly (such as DD-MMM-YYYY) are acceptable.</li> <li>Default values for century are permitted only when supplied by data-entry aids and the end-user can verify the defaulted value before committing the data.</li> </ul>
Implicit Century	For any date element represented without century, the correct century is unambiguous for all manipulations involving that element.	<ul style="list-style-type: none"> <li>Century must be explicit in all date data stored or transmitted unless the correct century can be inferred with 100% accuracy based on the value for date. Explicit century is preferred where practical.</li> <li>Developed and third-party software may imply century in the user interface in the format YYYYMMDD or YYJJJ (as specified by ANSI X3.30).</li> <li>In storing or transmitting date data, some applications must conform to domain-specific standards whose requirements for dates may supersede ANSI X3.30 as appropriate within the application. Examples of these standards are listed in Table 5.</li> </ul> <p><b>Exceptions:</b></p> <ul style="list-style-type: none"> <li>For date data formatted for a user interface, it is acceptable to use punctuation such as slash within a formatted date, to spell out or abbreviate the name of the month, or to reorder year-month-day to serve customs among the end users.</li> </ul>

Table 5. Additional Year 2000 Compliance Criteria Interpretations

Criterion	Description of Criterion	Interpretation of Criterion
Leap Year Calculation	For any year that is either evenly divisible by 400 or evenly divisible by 4 and not evenly by 100, there are potential exposures.	<ul style="list-style-type: none"> <li>Day-in-year calculations must address 366 days not 365.</li> <li>Day-of-the-week calculations must address the fact that 28 February 2000 is a Monday and 1 March 1 is a Wednesday, not a Tuesday which is February 29, 2000.</li> <li>Week-of-the-year calculations. The 11<sup>th</sup> week of the year 2000 is 5 through 11 March, not 6 through 12 March.</li> </ul>
Special Values	Fixed dates cannot be used as a global indicator.	<ul style="list-style-type: none"> <li>Certain years cannot be used as an "end of input" flag, e.g. 99 and 00.</li> <li>Certain dates cannot be used to indicate "no-expiration", e.g. 12/31/99.</li> </ul>
Century Calculations	All manipulations of century data will produce desired results for all valid date values within the operational domain.	<ul style="list-style-type: none"> <li>Rollover to 1/1/2000 - The calculation of 12/31/1999 23:59:59 plus 1 second must produce 1/1/2000 00:00:00.</li> <li>Pre-2000 Calculations - The calculation of 12/31/1999 plus 1 day must produce 1/1/2000.</li> <li>Post-2000 Calculations - The calculation of 1/1/2000 less 1 day must produce 12/31/1999.</li> </ul>

## B. STANDARD DATE FORMAT

Standardizing the format for date data is an important part of Year 2000 compliance. However, although several standards for date data format are available, the criteria in this document take precedence over other date standards. These other date standards may be used, as long as the criteria in this document are met.

Furthermore, two considerations must be made when evaluating computing resources for compliance.

## 1. Limitations in Standards

None of the 3 standards for date representation (ANSI, ISO, FIPS) mandates a 4-digit year for ALL calendar data. For example, conformance to ANSI X3.30 does not eliminate century ambiguity from all date variables and interfaces. Instead, conformance simply reduces the variety of formats occurring in the computing resource.

## 2. Accommodating Conflicts

While trying to conform to ANSI X3.30, some applications may need to satisfy other standards or conventions for date representation. Table 5 lists examples of standards with date representations that may supersede ANSI X3.30 in specific applications. In addition, the criteria and performance expectations set forth in this document take precedence over all other standards or conventions.

**Table 6. Examples of Standards which may Supersede ANSI X3.30**

Domain	Standard
Interoperability with international concerns	ISO 8601 (1988)
SQL	ANSI X3.135-1992, ISO-IEC 9075:1992, or FIPS 127-2
Electronic commerce (EDI)	ASC X12 EDI draft std for trial use, ISO 9735, UN/EDIFACT



**NUCLEAR UTILITY YEAR 2000 READINESS**

**Appendix D**

**VENDOR READINESS QUESTIONNAIRE**





Vendor Readiness Questionnaire

NEI/NUSMG 97-07  
October 1997

Year 2000 Ready? Software and Hardware Vendors All Other Suppliers		answer Sections A, B, C, & D answer Sections A, B, & C
<b>Section A: Company General Information</b>		
1. Vendor name, Address		
2. Vendor Internet Page(s) dedicated to Year 2000	http://	
3. Y2K Vendor Contact, Address		
4. Y2K Vendor Contact's E-mail Address		
5. Y2K Vendor Contact's FAX (XXX) XXX-XXXX		
6. Y2K Vendor Contact's Phone Number (XXX) XXX-XXXX		
<b>Section B: Year 2000 Ready?</b>		
1. Product Name	<input type="checkbox"/> Software <input type="checkbox"/> Business Application <input type="checkbox"/> System Software <input type="checkbox"/> Office Productivity Software <input type="checkbox"/> Product has software or microprocessor component <input type="checkbox"/> Hardware <input type="checkbox"/> Computer Hardware <input type="checkbox"/> Equipment / Device <input type="checkbox"/> PC / Workstation <input type="checkbox"/> Other <input type="checkbox"/> Product does not have software or microprocessor component	
2. Product Type / Category		
3. If Software, Current Release Number		
4. If Hardware, Model Number		
5. To the best of your knowledge, is this product Year 2000 ready? (A product is Year 2000 ready when it can be proven that date changes between 19xx to 20xx can be performed without error.)	<input type="checkbox"/> Yes Please review & sign Warranty Letter attached. <input type="checkbox"/> No	

Vendor Readiness Questionnaire

NEI/NUSMG 97-07  
October 1997

<p>6. If Yes, what is the basis for your answer?</p>	<p><input type="checkbox"/> No Date/Time Dependencies in Product</p> <p><input type="checkbox"/> Code Analysis Performed</p> <p><input type="checkbox"/> 4-digit year is used (ccyy)</p> <p><input type="checkbox"/> Date encoding is used (Convert yy from decimal to hexadecimal, etc.)</p> <p><input type="checkbox"/> Windowing technique is used (yy less than 50 means cc equals 20)</p> <p><input type="checkbox"/> Century indicator is used (1 digit where 0=cc of 19 and 1=cc of 20)</p> <p><input type="checkbox"/> Product has been tested and is proven to be ready</p> <p><input type="checkbox"/> Other: _____</p>
<p>7. If No, do you have a solution to make the product Year 2000 ready?</p>	<p><input type="checkbox"/> Yes</p> <p>Scheduled release number: _____</p> <p>Scheduled release date of ready product (mm/ccyy) _____</p> <p>Indicate what method will be used? _____</p> <p><input type="checkbox"/> 4-digit year (ccyy)</p> <p><input type="checkbox"/> Date encoding (Convert yy from decimal to hexadecimal, etc.)</p> <p><input type="checkbox"/> Windowing technique (yy less than 50 means cc equals 20)</p> <p><input type="checkbox"/> Century indicator is used (1 digit where 0=cc of 19 and 1=cc of 20)</p> <p><input type="checkbox"/> Other: _____</p> <p><input type="checkbox"/> No</p> <p><input type="checkbox"/> No plan exists at this time</p> <p><input type="checkbox"/> Patch available/being developed for limited readiness</p> <p>Scheduled release number: _____</p> <p>Scheduled release date of patch product (mm/ccyy) _____</p> <p><input type="checkbox"/> Work is in process to make product Year 2000 ready</p> <p>Scheduled release number: _____</p> <p>Scheduled release date of ready product (mm/ccyy) _____</p> <p><input type="checkbox"/> Replace existing product. No further support of this product is planned beyond 2000:</p> <p>Recommended replacement: _____</p>

Section C: Strategy/Solution Identification for Year 2000 Readiness (Hardware & Software vendors)	
1. Will there be an additional charge to the client for upgrading?	<input type="checkbox"/> Yes      Cost = _____ <input type="checkbox"/> No      Upgrade is part of maintenance/contract agreement <input type="checkbox"/> Undecided
2. Will you warrant product against failure?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
3. Will you provide a maintenance agreement?	
4. Will you provide a copy of the test plan used to ensure readiness?	<input type="checkbox"/> Yes <input type="checkbox"/> Attached <input type="checkbox"/> No
5. Will you provide a copy of the test data used to ensure readiness?	<input type="checkbox"/> Yes <input type="checkbox"/> Attached <input type="checkbox"/> No
6. Will you provide written confirmation of readiness?	<input type="checkbox"/> Yes <input type="checkbox"/> Attached <input type="checkbox"/> No
7. Will installation of the Y2K-compliant release require upgrades to the operating environment (i.e. Operating System, DBMS, etc.)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know If Yes, please describe:
8. Will installation of the Y2K-compliant release require modification to existing application data?	<input type="checkbox"/> Yes <input type="checkbox"/> Conversion utility will be supplied <input type="checkbox"/> No <input type="checkbox"/> Don't Know
9. Will the changes implemented in the Y2K-compliant release have any additional performance impact on data?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know If Yes, please describe:
10. What functionality is impacted by date processing/where do dates play a role in processing?	

Vendor Readiness Questionnaire

NEI/NUSMG 97-07  
October 1997

Section D: Readiness Details/Checklist for Determining Year 2000 Readiness (Software & Hardware Vendors)	
1. Expected Fail Date: When will the product be impacted by a year 2000 date field (mm/dd/ccyy)?	<input type="checkbox"/> _____ <input type="checkbox"/> N/A
2. Does the product represent the year using 4 digits: On Screens On Reports Within Programs Within Databases	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know
3. Does this product perform date calculations?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know If Yes, please describe:
4. Does this product perform logical ordering / sequencing of dates?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know If Yes, please describe:
5. Does this product have date fields or date-related variables in the programming code?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know
6. Does the product's files/databases contain 1- or 2-byte indicators to indicate the century? (e.g. 1 for 19, 2 for 20)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know Please describe:
7. Are there identifier fields that use dates embedded within the field? (e.g. Policy Number X3700121096)	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know Please describe:
8. Are there hard-coded dates (e.g., literals 99, 01, 19) within the product? For example, product uses 19 as century and/or 99 as an end-of-file indicator.	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know Please describe:
9. Does the product use the computer operating system date within calculations or comparisons?	<input type="checkbox"/> Yes <input type="checkbox"/> From Server? <input type="checkbox"/> From Workstation? <input type="checkbox"/> No <input type="checkbox"/> Don't Know
10. Does the product use common date routines?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know
11. Are future dates used (e.g. 1998, etc.)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know

Vendor Readiness Questionnaire

NEI/NUSMG 97-07  
October 1997

<p>12. Does the product currently process dates beyond the Year 2000 in this product? (e.g. 2000, 2005, etc.)</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know</p> <p>If Yes, please provide an idea of how long Year 2000 dates have been used in this product</p> <p><input type="checkbox"/> Less than 1 year  <input type="checkbox"/> 1-3 years  <input type="checkbox"/> Greater than 3 years</p>
<p>13. How far into the Year 2000 do the dates extend? (e.g. 2010, 2034, etc.)</p>	
<p>14. Do date fields require expansion from 2 digits to 4 digits:</p> <p>On Screens? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know  On Reports? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know  Within Programs? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know  Within Databases? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know</p>	
<p>15. Are there any regulatory requirements that stipulate expansion of date fields from 2 digits to 4 digits? (e.g., adherence to govt. standard for expiration of pharmaceutical products.)</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know</p> <p>If Yes, please describe:</p>
<p>16. Does this product interface with other vendors' products?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>17. If Yes, what are they and have the interfaces been tested?</p>	<p>Product:  Tested: <input type="checkbox"/> Yes <input type="checkbox"/> No  Product:  Tested: <input type="checkbox"/> Yes <input type="checkbox"/> No  Product:  Tested: <input type="checkbox"/> Yes <input type="checkbox"/> No  Product:  Tested: <input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>18. Does your product recognize Year 2000 as leap year?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>19. Are there any hardware attachments to the application? i.e. An inventory system may require use of a Bar Code Wand.</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>If Yes, please describe:</p>

## Vendor Readiness Questionnaire

NEI/NUSMG 97-07  
October 1997

Section E: Vendor Readiness Details/Checklist for Determining Year 2000 Readiness (All Other Suppliers)	
1. Is the manufacturing of your product dependent on any other critical suppliers or third party vendors?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know
2. If Yes, have you had any discussions with those suppliers regarding their Year 2000 readiness?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know
3. If Yes, will your suppliers be Year 2000 ready?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know
4. Do you have any manufacturing equipment with Year 2000 issues?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know
5. If Yes, will your manufacturing equipment be Year 2000 ready?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't Know
6. Have you assessed the impact of Year 2000 on your business systems?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't know
7. Are your business systems Year 2000 ready?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't know
8. If No, do you have a plan for making your business systems Year 2000 ready?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Don't know
9. If Yes, what is your targeted Year 2000 readiness date?	

Please return completed questionnaire(s) within 14 days to:

**NUCLEAR UTILITY YEAR 2000 READINESS**

**Appendix E**

**DETAILED ASSESSMENT PROCEDURES  
AND  
CHECKLISTS**





**Assessment Plan**

## I. Purpose

The purpose of assessment is to complete the assessment begun by IBM and to determine the magnitude of the impact from the year 2000 and the risk from the year 2000 on a company wide basis. It is expected that at the completion of this plan a company wide inventory of systems and non-IT assets with an assessment of year 2000 impact and risk will be produced.

## II. Methodology

Assessment was initiated by IBM using a survey. Response to this survey was inadequate to complete the assessment. Further information will be gathered by the corporate year 2000 project team by continuing the collection of surveys from the Business units and through meetings with each Business unit's year 2000 project point. This information will then be used to complete the assessment plan.

The business units will use the following assessment plan to inventory and analyze impact and risk of their assets. The business units will make the preliminary assessment. The corporate project team will review the business units findings and audits will review the overall findings. In cases where the business unit assessment does not agree with the corporate assessment a consensus process will be followed to achieve a consensus assessment. If audits does not concur with the consensus assessment then the corporate project team will coordinate resolution of the concern with audits.

## III. Assessment Plan

## A. Prepare an Inventory

1. Prepare an inventory of all Information Technology assets. This includes networks, operating environments, databases, application programs, CASE tools, off the shelf products, etc.. These are assets usually maintained by IS personnel.
2. Prepare an inventory of all Non-IT assets. These are systems or devices that are usually device driven chips, EPROMS, or other PLCs and which may be maintained by users. Examples include data acquisition systems, badge control systems, environmental control systems, engineering applications, plant control systems, workstations, end user maintained spreadsheets and databases,

trending applications, plant monitoring systems, LANs and LAN equipment, PBXs and other telephony equipment, PCs, test equipment, and metering systems.

3. Prepare an inventory of all external interface systems that transfer electronic data. These include any EDIs, and interfaces with other companies, regulatory agencies, public domain networks such as the Internet, interfaces with other utilities of Qualified Facilities, interfaces with other distribution systems.

**B. Assess the Size of the Asset In Terms of Amount of Code**

The purpose of this part of the assessment is to get a feel for the size of assets in terms of Lines of Code or functionality. This assessment is essential for determining resource allocation and is used to bias the assessment of an asset's Y2K impact and risk. It should be noted that a large variety of asset types are being inventoried and a Lines of Code metric for size is not applicable to all assets, hence the inclusion of functionality. The purpose is to attempt to create a common size rating system for all assets. The following definitions/categories are provided as a guideline for assessing asset size.

1. Applications written and maintained by the Business unit or Corporate IS organization shall be assessed for size using the following categories:
  - a. Minor, 0 -1000 Lines of Code
  - b. Medium, 1001 - 10000 Lines of Code
  - c. Major, Greater than 10000 Lines of Code
2. Applications written and maintained by Vendors should be evaluated based on functionality if a Lines of Code count is not available. Assess size using the following categories:
  - a. Minor Vendor, 0 - 1000 Lines of Code, or very limited functionality, probably dedicated to a single, limited function, or limited to operating on a single CPU with limited memory resources
  - b. Medium Vendor, 1001 - 10000 Lines of Code, or moderate functionality, probably able to generate and print reports, perhaps handle multiple functions, or limited to operating on a single CPU with several megabytes of memory resources, or operating on a few CPUs with limited memory resources
  - c. Major Vendor, greater than 10000 Lines of Code, or incorporates major functionality, probably able to generate and print reports, maintain and manipulate data, has a sophisticated user interface, perhaps handles several major functions, or operates on a single CPU with large amounts

- of memory resources, or operates on several CPUs with large amounts of memory resources
3. Applications that are end user generated and maintained should be evaluated based on functionality if a Lines of Code count is not available. Assess size using the following categories:
    - a. Minor Ad hoc, 0 - 1000 Lines of Code or applications written to achieve a specific purpose such as generate a report from a database or performing a specific type of calculation using a spreadsheet format, or a single user, stand alone system that perhaps uses the network to access data, but has no networking capability of its own
    - b. Medium Ad hoc, 1001 - 10000 Lines of Code or applications written to perform complex user purposes but limited to a few reports, or a few data manipulations, or capable of supporting a small number of users in a small network or workstation
    - c. Major Ad hoc, greater than 10000 Lines of Code, or applications written to perform complex user purposes with large numbers of different reports and data manipulations, can provide what if type analysis, or capable of supporting large numbers of users in a organization wide network
  4. Applications that are purchased off the shelf should be evaluated based on functionality if a Lines of Code count is not available. Assess size using the following categories:
    - a. Minor Off Shelf, 0 - 1000 Lines of Code or applications written for a single user, single machine
    - b. Medium Off Shelf, 1001 - 10000 Lines of Code or applications written for a small number of users in a small network or workstation.
    - c. Major Off Shelf, greater than 10000 Lines of Code, or applications written for a large numbers of users in a organization wide network, or a client server application.
  5. Operating systems should be evaluated based on the platform they are for. Assess size using the following categories:
    - a. Minor Op Sys, Operating systems for PCs
    - b. Medium Op Sys, Operating systems for minis, work stations, or LANs
    - c. Major Op Sys, Operating systems for mainframes, client server, intranets, or WANs
  6. Embedded systems should be evaluated on functionality. Assess using the following categories:
    - a. Minor Embedded, single or limited function, has a single CPU

- b. Major Embedded, large amount of functionality, has multiple CPUs
7. Commercial products like programming languages/environments, database managers, spread sheets, and word processors should be evaluated based on the platform they are designed to service. Assess using the following categories:
- a. Minor Package, those designed to operate as stand alone on PCs
  - b. Medium Packages, those designed to operate on minis, workstations, or LANs.
  - c. Major Packages, those designed to operate on mainframes, client server, or WANs.
8. Miscellaneous assets such as PEXs, Data Acquisition Systems, Relays or other smart devices, CASE tools, etc. should be evaluated based on their perceived size. This is a quality judgment. Assess these components using the following categories:
- a. Minor Misc, those assets perceived to be of small size (example is a relay)
  - b. Medium Misc, those assets perceived to be of moderate size (example is a Data Acquisition System)
  - c. Major Misc, those assets perceived to be of major size (example is a PBX)

C. Assess Importance of the Asset to the Business unit

Use the following definitions to determine the importance of the asset to the Business unit:

Critical	<ul style="list-style-type: none"> <li>Has life threatening implications to employees/customer</li> <li>Required by regulatory agencies for Business unit/company operation</li> <li>Major implications on financial status/stability</li> <li>Major impact on service to customers</li> <li>Major impact on stockholders/public relations</li> <li>Is a binding contractual obligation to customer</li> <li>Daily loss of revenue of greater than \$750,000.00</li> </ul>
Severe	<ul style="list-style-type: none"> <li>Severe impact to Business unit/company operation; becomes more critical over time</li> <li>Business continues but with great difficulty</li> <li>Mandated by regulatory agencies but can be lost for short periods of time</li> <li>Cash flow implications increase as outage duration extends</li> <li>Lost productivity to most of the employees</li> <li>Daily loss of revenue of greater than \$500,000.00</li> <li>Asset is used solely as a backup to an asset of critical importance</li> </ul>

## Assessment Plan

NEI/NUSMG 97-07  
October 1997

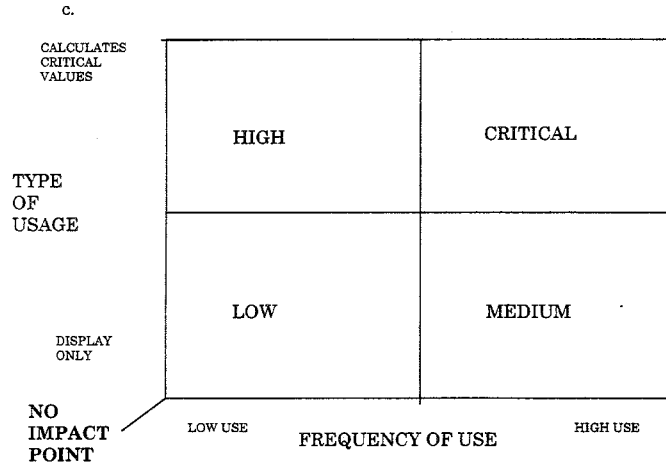
High	<p>Business operation continues but with serious difficulty Mandated by regulatory agencies but which have compensatory measures Lost productivity to a majority of employees Daily loss of revenue of greater than \$100,000.00 Asset is used solely as a backup to an asset of severe importance</p>
Medium	<p>Business operation continues but is cumbersome Compensatory measures are more costly to use than the asset Minimal impact on the Business unit/company's core business Minimal impact on cash flow Lost productivity to a significant number of employees Asset is used solely as a backup to an asset of high importance</p>
Low	<p>Minimal impact to Business unit operation Lost productivity to a minimal number of employees Customer service not affected Compensatory measures are minimally more costly to use than the asset Asset is used solely as a backup to an asset of medium importance</p>
None	<p>No impact to business operations No lost productivity Compensatory measures are no more costly to use than the asset Asset isn't being used or has no identified users Asset is used solely as a backup to an asset of low importance Asset has been replaced or superseded</p>

Assets determined to have no importance should be evaluated for abandonment. If it is determined that these assets can be abandoned then no further resources should be used in evaluating them.

## D. Assess Impact of Year 2000

1. This is done to solely assess the impact of year 2000 dates on the asset. Impact will not be used as the sole criteria for determining corrective actions.
2. Evaluate frequency of use of date/time data. Range of frequencies will be not used extensively. This is a qualitative judgment, for applications or systems with thousands of lines of code, infrequent use may be once per 1000 lines while frequent use may be once per 100 lines. Non-IT assets may be considered to use dates frequently if it is used once in PLCs, as part of the system clock, if used for timing, or if used to date stamp data.

3. Evaluate how the date/time data is used. Range of how used will be from display only to used to calculate critical values. Display only uses are for graphs, printouts, or screen displays that show a date, critical values would use dates to determine plant or process control functions, generate billing, control functions which could impact personnel safety, or if use of the date would cause the system or program to crash. Intermediate impact values include applications where dates are used to format record lengths, for forecasting, for determining reporting intervals, for generating required filings, for date stamping on legal records, controlling building access, generating trend reports or graphs, etc. These functions should be evaluated qualitatively for their importance to the business unit when determining where the function falls with relation to critical values and display uses only.
4. Several methodologies may be used to perform the above evaluations. The method that generates results with the highest level of confidence is testing. However, this method is time and resource intensive for large systems and may not be practical for non-IT assets. Other acceptable methods, in order of highest confidence to lowest confidence are use of a tool to evaluate code, vendor certifications of year 2000 compliance or notices of problems, code inspections, and engineering analysis. It is important to record the method used to perform the evaluation as that information will be used in evaluating risk.
5. Evaluate overall impact using the below grid and rules to classify year 2000 impact for each system.
  - a. Plot each asset on the grid. The asset may be represented by a series of points based on frequency of use.
  - b. Determine the overall impact of each asset by choosing the plotted point with the greatest impact. Note that any asset with a date influenced critical value will be given a critical impact rating. Also note that only assets that do not use date data will be rated as No Impact, any use of date data requires some ranking.



IMPACT EVALUATION GRID

E. Assess Risk of Year 2000

1. The purpose of assessing risk is to prioritize assets for determining resource allocation. Assets with the highest risk will have the most detailed corrective actions, will receive the most resources, and will be done first. Assets with lessor risk will have corrective actions and resources commensurate with their risk and will be done after the higher risk assets have been completed. Items with little risk may not be completed prior to the year 2000 but will have contingency/action plans in place so that productivity is minimally impacted. These assets will be completed to the year 2000 if resources permit.
2. Risk is determined based on a combination of asset importance and year 2000 impact. Four levels of risk have been established based on the below risk grid.
3. Note that assets with no importance and no impact will be assigned to the No Risk Point.
4. Risk combination pairs are read as standard Cartesian coordinates, i.e. (x,y) ordered pairs using the ordering (Importance, Impact)

5. The risk rating may be changed or biased based on the confidence in the assessment of impact. If there is low confidence in the methodology used to determine impact, or if the impact rating is suspect, than the risk rating should be raised a level. The risk rating may also be changed based on using the size and frequency of date use of an asset to bias the impact rating. As an example, an asset that is large with many date uses of a less important nature may have its impact rating raised a level due solely to the large number of lessor important type of usage items.

6.

YEAR 2000 IMPACT	High	<p><b>HIGH</b></p> <p>Critical, Medium Severe, High High, Critical High, High</p>	<p><b>STRATEGIC</b></p> <p>Critical, Critical Severe, Critical Critical, Severe</p>
	Low	<p><b>LOW</b></p> <p>Medium, Low Low, Critical Low, High Low, Medium Low, Low All, No Impact</p>	<p><b>MEDIUM</b></p> <p>Critical, Low Severe, Medium Severe, Low High, Medium High, Low Medium, Critical Medium, High Medium, Medium</p>
<b>NO RISK POINT</b>		Low	High
		<b>ASSET IMPORTANCE</b>	

**RISK EVALUATION GRID**

**F. Determine Corrective Actions**

1. The purpose of corrective actions is to ensure that the company is ready to operate with the asset once the year 2000 is reached.



<p><b>HIGH - 2<sup>nd</sup></b> Asset repaired/replaced prior to 2000 Asset tested prior to 2000 Asset has contingency plan should failure still occur  Optional: backup obtained prior to 2000</p>	<p><b>STRATEGIC - 1<sup>st</sup> Priority</b> Asset repaired/replaced prior to 2000 Asset tested prior to 2000 Asset has contingency plan with compensatory measures should failure still occur  Optional: backup obtained prior to 2000</p>
<p><b>LOW - 4<sup>th</sup> Priority</b>  Asset has a repair/replacement plan which may go beyond 2000 Asset has contingency plan with compensatory measures should failure still occur</p>	<p><b>MEDIUM - 3<sup>rd</sup></b>  Asset repaired/replaced prior to 2000 Asset tested prior to 2000 Asset has contingency plan should failure still occur</p>

**CORRECTIVE ACTION GRID**

2. Corrective actions can consist of repairing/replacing the asset, testing the asset, generating compensatory/action plans, doing nothing, or a combination of these items.
3. Corrective actions should be commensurate with the risk to the asset. The higher the risk the more extensive and proactive the actions. Only assets with low risk should be given actions that are reactive or post year 2000.
4. Minimum corrective actions are specified in the above corrective action table.
5. Format for action and contingency plans will be published in a later document.
6. Assets with no risk shall have nothing done unless the confidence in the no risk rating is low, for those assets a compensatory action plan should be prepared.

**IV. Document Results**

- A. The Business units shall report assessment results to the Corporate Project Office, G.O. 1, Room 115 addressed to Keith Wilcox or Murray Jennex
- B. Reports shall be in a Microsoft Excel/Access compatible format.

- C. The Corporate Project Office shall serve as the repository for all the reports and shall be responsible for generating the overall inventory as well as any required sorts of the inventory. The format for the final inventory will be decided using corporate data standards. However, it is anticipated that the final inventory will be published on the year 2000 web page (currently under development).
- D. Required data fields are as follows:
1. Asset Acronym: provided by the Business unit if one exists
  2. Asset Name: provided by the Business unit
  3. Asset Version: provided by the Business unit
  4. Asset Description: provided by the Business unit
  5. Asset Language, i.e. what language the asset is written in or uses: provided by the Business unit
  6. Asset Size: use rating from the assessment plan
  7. Asset Importance: use rating from the assessment plan
  8. Y2K Impact: use rating from the assessment plan
  9. Y2K Impact Assessment Basis: testing, vendor certification, inspection/engineering evaluation
  10. Asset Y2K Risk: use risk rating from assessment plan
  11. Correction Strategy: Business unit will stipulate, Corporate Project Office will review, disagreements to be resolved via consensus decision process
  12. Correction Priority: Corporate Project Office will establish this based on overall inventory results, Business units will review, disagreements to be resolved via consensus decision process.
  13. Correction Estimate: Business unit will stipulate, Corporate Project Office will review, disagreements to be resolved via consensus decision process
  14. Source Code Location: provided by the Business unit. Indicate the physical location where the source code is stored or indicate "Not Available" if the source code is not available. Availability of the source code should be taken into consideration when determining corrective actions. Replacement should be

**Assessment Plan**NEI/NUSMG 97-07  
October 1997

considered for any asset which does not have available source code. If the source code is not available because the vendor kept it, so indicate and the corporate project team will initiate actions to either obtain the source code, obtain assurance of compliance from the vendor. If an upgrade or replacement package is required then the Business unit will need to decide if the asset is to be upgraded or replaced and should initiate the appropriate actions.

15. **Primary Users:** indicates which organization or group is the primary users of an asset. This is provided by the Business unit
16. **Contact Name:** indicates the individual or lead individual responsible for maintaining the asset

Assessment Plan

NEI/NUSMG 97-07  
October 1997

## ***Year 2000 Detailed Assessment Package***

### **1. Purpose**

The purpose of this package is to guide the user through the Year 2000 Detailed Assessment Process of a particular application, and it also serves as documentation of the work performed. The purpose of a detailed assessment is to obtain enough information about an application to determine its expected performance beyond December 31, 1999. From this assessment, a decision is made (and documented) regarding any action needed to maintain continuous performance.

### **2. Application Information**

Information specific to this application is required in order to complete this detailed assessment. Enclosure A has been pre-populated with as much of that information as we currently have available.

2.1. Review Enclosure A for accuracy and fill in any missing information as applicable.

### **3. Scanning the Application**

In order to determine if an application is Year 2000 ready, scanning may be required. Scanning is a process (manual or automated) that locates all date references and potential calculations in an application. In order to be able to do scanning the source code of the application is required along with all of the applications associated with interfaces, modules, screen layouts, etc. Because of the complexity involved, only the application developer or comparable expert should undertake the process. If the number of lines of code exceeds 1000 then you can contact the NY2K Project Manager or your local NY2K Core Team member and they can make arrangements to have your code electronically scanned for date impacts. If you have <1000 lines you can manually view the code looking for date impacts

**NOTE:** *Testing is required for SDQA category A or B applications to ensure Year 2000 readiness. For those that are not Category A or B, the business sponsor should determine the appropriate level of scanning or testing, and document appropriately.*

3.1.1. Perform application scanning (if applicable) and complete Enclosure B.

### **4. Testing the Application**

In order to determine if an application is Year 2000 ready testing may be required. Testing involves taking the application out of the normal production environment (into a "safe" test environment where any failures have no impact on production) and performing a series of controlled scenarios that will mimic the application's performance in the Year 2000. Specific testing criteria have been established and documented by the Year 2000 program, and may be found in the Year 2000 Technical Compliance Criteria.

**NOTE:** *Testing is required for SDQA category A or B applications to ensure Year 2000 readiness. For those that are not Category A or B, the business sponsor should determine the appropriate level of scanning or testing, and document appropriately.*

## 4.1. Testing

**NOTE:** See Enclosure F for more information on testing.

- 4.1.1. Develop Test Plan. (See Enclosure E for additional Test Plan Information)
- 4.1.2. Identify and List All Application Components.
- 4.1.3. Identify Baseline Data with 19xx Dates.
- 4.1.4. Determine Appropriate Test Environment
- 4.1.5. Setup Test Environment
- 4.1.6. Follow Appropriate Change Control Procedures for Test Platform.
- 4.1.7. Load Application into Test Environment.
- 4.1.8. Perform Test Cycles
- 4.1.9. Restore Test Environment (if necessary).
- 4.1.10. Complete Enclosure C.

**5. Year 2000 Impact Sign Off**

The business sponsor is required to review the entire assessment package to this point (including enclosures), determine if application is Year 2000 Ready, and sign off Enclosure D

- 5.1. Review assessment package including enclosures
- 5.2. Determine if application is Year 2000 Ready.
- 5.3. Complete Enclosure D – Year 2000 Impact Sign Off.
- 5.4. Mail the completed Detailed Assessment to:

NY2K Project Manager

**NOTE:** If the application is not Year 2000 ready then complete a Year 2000 Business Case Package for the application.

**6. NY2K Project Management Review & Sign Off**

- 6.1. The NY2K Project Manager is required to review the entire assessment package to this point (including enclosures) for completion
- 6.2. Complete Enclosure D – Year 2000 Impact Sign Off.
- 6.3. File the completed Detailed Assessment.

**(ENCL A) APPLICATION SUMMARY**

The following information is required to complete the detailed assessment, and is/will be stored in the Database. Please complete any areas that have been left blank.

**General Application Information**

<b>Application Name:</b>	<i>application name</i>
<b>Application Number:</b>	<i>application number from Database</i>
<b>Functional Description:</b>	<i>Brief description of the application</i>
<b>Business Sponsor Name:</b>	<i>Sponsor name</i>
<b>Business Sponsor Area:</b>	<i>Sponsor location/organizational area</i>

**Programmer Information**

List the person who is currently responsible for the source code.

<b>Primary IT Contact Name</b>	
<b>Phone</b>	
<b>Team Name</b>	

**Vendor Information**

N/A

List vendor information (if applicable). Vendor may provide update/upgrade to software, operating system, etc., which may be necessary to achieve Year 2000 readiness.

<b>Vendor Name</b>	
<b>Contact Name</b>	
<b>Address</b>	
<b>City</b>	
<b>State</b>	
<b>Zip Code</b>	
<b>Phone Number</b>	

**User Information**

<b>User Groups</b>	
<b>User Sites</b>	

**(Encl B) Application Technical Summary**

(to be completed by application developer or support)

<b>Hardware Platform</b>	
<b>Operating System(s)</b>	
<b>Development Tool(s)</b>	
<b>For databases only: Database type &amp; name</b>	
<b>Server Name</b>	
<b>Executable File Name</b>	
<b>Executable Server Name</b>	
<b>Version Number</b>	<b>Date Implemented:</b>

**Application Component List**  **N/A**

List all components of the application (any of the separate pieces, such as programs, data tables, interfaces, or any other stand-alone modules that provide functionality to the application).

Component Name	Component Type	Language

**Application Interfaces (Internal)**  **N/A**

List any other applications within xxx company that may exchange information with this application (whether receive, provide input, or both), if applicable.

Interfacing Program	Interface Name	Scheduled Interface (Real Time, On Demand, Daily, etc.)	Description of the Interface

**Application Interfaces (External)**  **N/A**

List any applications or entities that are external to xxx company (vendors, government agencies, banks, etc.) that exchange information with this application (whether receive, provide input, or both), if applicable.

Interfacing Program	Interface Name	Scheduled Interface (Real Time, On Demand, Daily, etc.)	Description of the Interface



Detailed Assessment Package

NEI/NUSMG 97-07  
October 1997

**(Encl C) Scanning Results**

Was scanning conducted for this application?       Yes     No

Scan Summary

Was the scanning performed electronically?       Yes     No  
If YES, attach Detailed Scan Reports.

If NO, provide the following information:

Method used to scan code:	
Number of Lines Impacted:	
Program File Name:	
Line #	Contents of Line with Date Impact
Program File Name:	
Line #	Contents of Line with Date Impact
Program File Name:	
Line #	Contents of Line with Date Impact

**Testing**

Was testing used to determine Year 2000 Impact?     Yes     No

Testing Summary

*Provide a summary of the application test and results or attach a copy of the completed test plan.*

*Results Table:*

<b>Readiness Test</b>	<b>Pass</b>	<b>Fail</b>	<b>N/A</b>
Year 2000 Rollover Warm			
Year 2000 Rollover Gregorian Warm			
Year 2000 Rollover Julian Warm			
Year 2000 Rollover Cold			
Year 2000 Rollover Gregorian Cold			
Year 2000 Rollover Julian Cold			
Year 2000 Leap Year Rollover Warm			
Year 2000 Leap Year Rollover Gregorian Warm			
Year 2000 Leap Year Rollover Julian Warm			
Year 2000 Leap Year Rollover Cold			
Year 2000 Leap Year Rollover Gregorian Cold			
Year 2000 Leap Year Rollover Julian Cold			
High Risk Date 9/99/99			
Date Integrity 2/29/01			

Detailed Assessment Package

NEI/NUSMG 97-07  
October 1997

**(Encl D) Year 2000 Impact Sign Off**

This Line of Business (LOB) supported application has been assessed and is capable of functioning properly in the year 2000 and beyond, as defined in the Year 2000 Technical Compliance Criteria, and by the Business Project Manager. The signature below indicates Y2K certification.

This application is impacted by the Year 2000 and is not ready for 1/1/2000.

Business Sponsor \_\_\_\_\_ Date \_\_\_\_\_

Package Reviewed - Complete

NY2K Project Manager \_\_\_\_\_ Date \_\_\_\_\_

**(Encl E) Test Plans****Overview**

*Describe the overall testing approach.*

**Assessment Of Level Of Testing Required**

*The extent of testing required will depend on company's view of the level of confidence required that the application will function correctly through the Year 2000. This will influence the number and type of test cases produced for Century Test. Other considerations may include the SDQA level of the application.*

**Specific Aspects to be Tested and not to be Tested (i.e. Dead Code)**

*List any particular functions that must be tested or that do not need to be tested (i.e. on-line panels known to have critical date processing, batch processing - month-end, year-end, quarterly, weekly, etc.). List particular century test dates to be tested based on the application's date processing.*

**Quality**

*Describe when formal quality control checks are to be conducted and what these controls are (i.e. specific sign offs required and when, user involvement and when, etc.)*

**Acceptance**

*Describe any specific criteria for user (or support team) acceptance of this application (other than acceptable results of the no-damage testing).*

**Test Timeline**

*Give key dates in test cycle, where known, and staff involved (i.e. data ready, test environment in place, Unit Test completed, System Test completed, Century Test completed, Acceptance, and retrofits (if any)).*

**Application Test Environment****Summary of Hardware & Software**

- *Describe test areas/regions to be used and any necessary set up for those areas (i.e. CICS region setup, DB2 table setups, etc.).*
- *State hardware to be used for testing.*
- *Identify communication links if required.*
- *Describe access arrangements for testers and any other security issues to be resolved.*

- Describe operating system and the use of proprietary products i.e. packages such as Changeman.

**Test Data**

Describe what test data will be used and how this data will be captured. Describe any backup and restore jobs for this data and where the JCL and/or files reside. Describe any dependencies that this data may have upon another application's data, or common files between applications.

**Test Tools**

Describe how testing tool(s) are to be used, if at all, by staff involved.

**Test Control Procedure**

- Describe how problems will be logged in the Problem Tracking Database (application name used) and what statuses will be used for this application for tracking purposes.
- Describe how scripts will be developed and by whom. If multiple scripts are used, describe the order in which they must operate, and any other related dependencies.

**Test Team Organization and Responsibilities**

State who is involved and their responsibilities.

**Configuration Management**

State where all data files and JCL for application set up and testing reside. State where testing documentation and results will reside for this application. State the change control process to be used (i.e. Changeman checkout, Source Safe, etc.)

**Assumptions**

List assumptions. All decisions based on assumptions should be confirmed in light of new knowledge gained during the course of the project.

**(Encl F) Testing Considerations**

The following is a guideline for defining the major steps in performing Year 2000 tests on applications. The same process can be followed whether it is for Century Testing or User Acceptance Testing. These steps apply to verifying applications that claim to be Year 2000 ready as well as those that have just been remediated.

- ❖ Identify and List All Application Components.
  - Programs
  - Files
  - Database Tables
  - JCL
  - Scripts
  - Sort And Other Utility Control Statements
  - Special Devices (Scanners, Magnetic Strip Readers, Etc.)
- ❖ Identify Baseline Data with 19xx Dates.
  - Transaction File Data
  - Test Scripts
  - Test Results (Reports, Screens, Etc.)
- ❖ Determine Appropriate Test Environment
  - Determine All Hardware Platform Components Required That Can Be Set To Year 2000 Date(s).
    - Mainframe
    - Midrange
    - Database Server
    - LAN Server
    - Notes Server
    - Workstation
    - Intelligent Peripheral Devices
  - Determine All Components Of The Operating Environment
    - Operating System
    - System Utilities (Sorts, DBMS, Etc.)
    - Run Time Components For All Platforms
  - Perform Sizings To Determine If Adequate Resources Are Available On Test Platform (DASD, Communications, Etc.)
  - Determine If All Components Other Than The Application Are Year 2000 Ready. If Any Are Not Year 2000 Ready, Assess The Risk Of Proceeding With The Test With Platform Elements That Are Not Year 2000 Ready.
- ❖ Setup Test Environment
  - Schedule Equipment Required For Test. Make Sure Date(s) for System Initialization Are Clearly Specified.
  - Verify That All Supporting System Software and Components of Other Required Applications Are Properly Installed and Date Initialized.

Detailed Assessment Package

NEI/NUSMG 97-07

October 1997

- If Production Equipment Is Used, Make Sure That Safeguards Are In Place To Keep Test Data From Bleeding Into Production Environment.
- Obtain Security Access if necessary.
- Schedule Any Equipment Interconnects Required.
- ❖ Follow Appropriate Change Control Procedures for Test Platform.
- ❖ Load Application into Test Environment.
  - Load Programs, Files, Database Tables, Etc.
  - Warp Dates if necessary.
- ❖ Perform Test Cycles.
- ❖ Restore Test Environment if necessary.
  - Remove All Test Programs, Data, Etc.
  - Verify That Everything Is Reset To Pre-Test Conditions (IP Addresses, Etc.)
- ❖ Obtain Test Sign-Offs.

If these test are on code that has been remediated, then any non-Year 2000 changes that have been made since the code was first checked out for Year 2000 remediation have to be applied. Year 2000 testing should then be re-run to verify that these latest changes have not corrupted the Year 2000 readiness. After all final sign-offs have been received that application can then be put into production.

If a production application was reported to be Year 2000 ready and the tests confirmed that it is, then the process is complete.

All new applications purchased by xxx company are to be Year 2000 ready. Year 2000 tests must constitute part of the normal acceptance testing and the above process should be followed to verify that readiness.





**NUCLEAR UTILITY YEAR 2000 READINESS**

**Appendix F**

**TEST SPECIFICATIONS**



## EMBEDDED SYSTEMS TESTING

### 1. INTRODUCTION

In any Year 2000 project, testing is perhaps the key element of the project. There are two distinct phases in testing.

The first phase is *Investigative testing* to ascertain whether a software program, product or integrated system complies with a predetermined set of specifications for the Year 2000.

The second phase is *Post remediation testing* to establish that any modifications made as a result of errors found either in the first phase of testing or by other analytical methods, are valid and the system, product or program can be certified to comply with the Year 2000 specification.

Year 2000 compliance may be defined differently for different purposes. In addition, local installations will vary in the way dates and times are formatted and represented. These differences notwithstanding, the kind of compliance testing that needs to be performed can be categorized into date and date-and-time functionality testing.

Most "traditional" business processing environments are concerned more with the date-category than with the date-and-time-category of functionality. In an Instrumentation & Control environment, the date-and-time-category functionality takes on more importance because of the "hard" real-time requirements of process and device control, monitoring, event signaling etc. performed by embedded systems. Of course, some functionality in these systems is centered on (real) time, with no date-related requirements. Since this functionality is not considered a year 2000 compliance issue, it is not addressed here.

This document presents a comprehensive set of test guidelines and methodology for the testing of embedded systems. In the first section, some generally accepted standards and a brief background of date and time notation is laid out. This is followed by a consideration of the unique challenges presented by the embedded systems. Then a set of specifications based on industry standard guidelines is set out. This forms the basis from which test parameters and methods are drawn.

Testing strategy, which includes precautions, preparations, and considerations of functionality, is then explained. This is followed by the detailed test procedures.

Finally extracts from industry sources such as the IEEE and the NIST along with references for further reading are included in the appendix.

### 2. BACKGROUND OF DATE AND TIME NOTATION

#### 2.1 *International calendar*

The international calendar currently followed in almost all countries is the *Julian calendar* with the Gregorian correction, or simply called the *Gregorian calendar*.

This is a solar calendar i.e. a year is based on the time taken for the earth to revolve round the sun. It consists of 12 months in a year. Each month consists of a specified number of days. Only the second month February consists of 28 days in common years and 29 in leap years. Thus common years have 365 days and leap years have 366 days.

**2.2 Definition of a leap year**

A leap year is a year where is an extra day (i.e. February 29<sup>th</sup>). This intercalation of day is to adjust for the discrepancy arising out of the normal year period of 365 days and the actual solar year based on the earth's revolution which is 365.242199 (365 days, 5 hours, 48 minutes and 46 seconds).

**2.3 How is a leap year determined?**

As per the Julian Calendar every year divisible by four was a leap year. This led to a discrepancy of 3.12 extra days over four centuries. Pope Gregory corrected this in 1582. As per the correction century years are leap years only if they are divisible by 400. There was also a further refinement, which stated that years divisible by 4000 are common years or non-leap years. With these refinements, the discrepancy between the calendar time and the actual solar time is reduced to one day over four thousand years.

As per the current Gregorian calendar the determination of a leap year is as follows:

1. All non-century years divisible by four are leap years.
2. All century years divisible by 400 are leap years.  
This means that 1900 and 2100 are not leap years, while 2000 is a leap year.
3. As per the refinement to the Gregorian calendar we also have the additional clause: All years divisible by 4000 are common years or non-leap years.

**2.4 Julian representation of a date**

The Julian representation of a date is the format DDD, YY or DDD, YYYY where DDD is a number from 1 to 365 or 366 depending on whether the year was a leap year or a common year and YY or YY is the two digit or four digit representation of the year.

**2.5 Gregorian representation of a date**

The Gregorian representation of a date is the format DD/MM/YY, MM/DD/YY or any of the other common formats currently used that incorporate date, month and year.

In a system, dates may be stored in Gregorian or Julian representation, or a combination of both. There are also situations where all internal representation and calculations are done using the Julian representations and all external interfaces and displays use the Gregorian representation.

**3 THE CHALLENGE OF EMBEDDED SYSTEMS**

Embedded systems pose many challenges for testing and remediation of the Year 2000 problem. These can be broadly categorized as follows:

**3.1 Architectural**

- There is a wide prevalence of four bit and eight bit processors such as those manufactured by Intel, Zilog and Advanced Micro Devices. Many of these have a limited instruction set. Many of these microcontrollers have a two-digit date representation for arithmetic and logical operations.
- Date representation may be different for 'power on' conditions and in battery backup condition
- There is no standard way to encode dates between different vendors.

**3.2 Programming**

- Source code is not available for many of these systems.
- Object code may be stored in different levels of firmware i.e. Programmable logic arrays (PLA's), Flash ROM, CMOS or BIOS.
- Object code may be hard coded, reloadable or re-entrant.
- Program may be recording real time intervals based on calendar dates rather than actual dates themselves.

**3.3 Configuration**

- System may be consisting of upstream and downstream devices that have data interfaces between them.
- Downstream devices may have dates that are set or overridden by upstream devices.
- System may have external interfaces that transmit and receive date information.

**3.4 Operational**

- The system may be in a production environment that it cannot be taken out of without severe impact.
- Backup systems may not be available, in case of failure during testing.
- Many systems may not revert back to current dates after dates are advanced during testing.
- Warranties, inspection and service logs may be voided by date advancement.

**4 SPECIFICATIONS FOR CENTURY COMPLIANCE**

The rules that follow are taken from the following source:

<http://www.year2000.com/archive/gte-article/NFgte-table3.html>

They resemble but are not identical with the rules issued by BSI/DISC. In particular the BSI/DISC rules explicitly cover the point that Year 2000 is a Leap Year. However the rules below have been cited by a English lawyer as a possible standard; and given the source, they might be assumed to be a de facto standard for North America. These rules are also currently being studied by the IEEE as the framework for an IEEE specification on Century Compliance.

**4.1. General integrity**

No value for current date will cause interruptions in normal operation. As a system date advances normally on a system, each system date must not lead to erroneous operation of the system or its software processes. The best recognized high-risk date change is the roll over to 2000. However there are a number of high risk dates such as 9/9/99, 2/28/00, etc. which must also be considered.

**4.2. Date integrity**

All manipulations of calendar-related data (dates, durations, days of week, etc.) will produce desired results for all valid date values within the application domain.

**4.3. Explicit century**

Date elements in interfaces and data storage permit specifying (i.e. specification of the) century, to eliminate date ambiguity. This criterion essentially requires the capability to store explicit values for the century. It must be noted that this must be interpreted as applicable to embedded systems. Not all embedded systems and their component microcontrollers will have this capability.

**4.4. Implicit century**

For any date element without century, the correct century is unambiguous for all manipulations involving that element. This last criterion requires that if the century is not explicitly provided, its value can be correctly inferred with 100% accuracy from the date provided.

Although the four criteria defined above fully define century compliance, it must be noted that compliance represents a balance between cost and risk rather than an absolute measure. The application of these criteria will vary depending on the system, the criticality to the line of business, the availability of the system for testing and certification, and the test process itself.

**5 TESTING STRATEGY**

The testing strategy can be divided into several areas:

**5.1 Test Parameters.**

Based on the compliance criteria defined above, each individual device or system must be studied to determine the characteristics of the device that will certify functionality. It must be noted that not all the functional characteristics of the device need be tested, such as real time functionality or other characteristics that do not have a time related impact.

To illustrate the kind of functionality, from which testbeds can be drawn, testing can be further categorized by functionality as shown below. These examples are not exhaustive of the kind of functionality found in each category. Subject matter experts should be used to determine what date and time related functions need to be tested for a given device or system.

Conversion and Extraction Functionality

The kind of routines to be tested here include such functionality as:

**DayOfYear (YYYYMMDD).** This kind of routine might be invoked in systems where dates are represented at some point inside a program using the Julian date format. For example, `dayOfYear(20000101)` should return 1, whereas `dayOfYear(20000229)` should return 60. Error conditions are candidates for testing here too. For example, `dayOfYear(20010229)` should *not* return 59, 60, 61 or any other number, as the input is *not* a valid date. Testing for this kind of condition may be difficult, since a fully year 2000-compliant system should *not* allow the system date to be set to an invalid date!

Conversely, routine such as **date (YYYYJJJ)** and **month (YYYYJJJ)** should correctly convert to Gregorian equivalents of Julian dates. For example, `date(1999365)` should return 31 and `month(1999365)` should return 12, or

'DEC' or 'DECEMBER,' depending on the system requirements. Similarly, date (2000060) should correspond to February 29th, *not* March 1st. As before, although testing may be difficult, error conditions should be detected and handled; for example, 19990, 1997-10, 2004366, 2020367 etc.

Systems may differ in terms of whether they represent date and time information independently of each other, or compounded into some kind of timestamp structure. (Some systems may use both representations for different purposes.) In the case of compounded, timestamp representations, routines similar to these may be defined over inputs of the form **YYYYJJJhhmmss** or **YYYYMMDDhhmmss**. In real-time systems, representations may typically be defined to greater levels of precision than seconds.

Depending on how a system boundary has been drawn, date and/or date-and-time *formatting* may need to be tested. Date and/or time outputs may appear on terminals, printers, LED and LCD displays, analog meters, digitally simulated analog meters etc. Even if date and/or time data does not display directly, it may be used to derive or calibrate data that is displayed on these types of device, or data that is used for annunciation. These systems should be validated for year 2000 compliance through to the data display portion of the system boundary, particularly if some critical operator intervention might depend on the accuracy of the data.

#### Arithmetic Functionality

The kind of routines to be tested here include such functionality as:

**daysBetween (startDate, endDate)**. This kind of routine might be invoked on a regular basis by software that calculates inspection, maintenance, replacement schedules etc. or that statistically analyzes raw data. Year 2000 compliance testbeds should test for correctness of cases such as days between (19991231, 20000301), which should calculate 61.

**addDays (startDate, numberOFDays)**. Again, this kind of routine might be relevant in systems where schedules are being set as well as forecasting systems, simulators etc. A testbed might include addDays (1999365, 2), which should return 20002.

**subtractDays (startDate, numberOFDays)**. SubtractDays would be relevant in systems similar to those where addDays might be a part of the system functionality.

The same considerations apply to arithmetic routines as well as conversion and extraction routines when date and time representations are compounded. Of particular importance here is the consideration of correctly interpreting the time 12:00 as midnight or noon when a 12-hour time representation is used.

#### Date Comparison Functionality

The kinds of routines to be tested here include standard sorting and searching functionality. This kind of processing represents the majority of date usage in software

**sort (list, ascending)**. Given a list of dates, or time-and-date timestamps, returns a list sorted correctly in ascending or descending order, depending on the second parameter.

**LessThan (YYYYMMDD, YYYYMMDD)**. No sorting routine can exist without complementary comparison routines to support it. Comparison routines are at the heart of the entire year 2000 compliance issue. These routines should be tested thoroughly.

**5.2 Test Environment.**

This involves preparation of a test environment to test the functional characteristics. This can be further categorized as follows:

- Device level testing – Testing of a device in an environment isolated from its normal production environment.
- System level testing – Testing of a complete system

It would always be preferable to test a device or complete system *in situ*, i.e. in the normal production environment. This may however not always be possible for various reasons – the system cannot be taken off-line, the time to prepare a test setup in the production environment may be excessive, error recovery may not be possible, etc. Subject matter experts should be consulted for preparation of a valid test environment. Some additional guidelines on preparation of a test environment are as follows:

1. If the test environment is a modified production environment, error recovery procedures must be clearly laid out.
2. All data and software where applicable, must be backed up prior to testing.
3. If a separate test environment is being set up, it must be ensured that all hardware models, revision levels of software etc., are exactly the same as the production environment.
4. All external data interfaces must be isolated so as to avoid any clash or discrepancy with any dates from other systems.

**5.3 Control Group testing.**

Following the setup of a test environment, testing must be carried out using current dates. This will establish the validity of the test environment.

A different kind of control group testing will need to be carried out for post remediation testing. In this case the modified system should first be tested using current dates to establish that no new errors arise.

**5.4 Century testing**

Following the successful completion of the control group testing, the system should be tested for century compliance based on the test parameters defined earlier.

**6 TESTING PROCEDURES**

The guidelines will be used for century testing of devices are defined below. These guidelines are based on the four century compliance criteria defined in Section 4. It must be noted that for each individual system all tests may not apply, and that a checklist should be drawn up based on functionality and the specific application that the system is performing.

**6.1 Definitions**

Century date – Jan 01 2000  
Leap Year – Year 1996, 2000, 2016  
High-risk dates – 12/31/98, 9/9/99, 12/31/99, 2/28/00, 2/29/00, 3/01/00



**6.2 Testing Guidelines****6.2.1 Date setting and Representation.**

- System can be set to any date in a range e.g. between 1995 and 2005.
- System can be set to dates both in Julian and Gregorian formats where applicable
- System can be set to high risk dates
- System can be re- initialized from cold start using high risk dates

**6.2.2 Date Rollover**

- System rolls over correctly on high risk dates
- System rolls over correctly both in powered up and powered down states
- System rolls over correctly both in Gregorian and Julian formats where applicable

**6.2.3 Date Arithmetic**

- System correctly calculates elapsed dates on either side of century rollover
- System correctly calculates days of the week, based on dates
- System correctly computes leap year dates
- System correctly converts between Julian and Gregorian representations

**6.2.4 Date Comparison**

- System is able to make correct date comparison e.g. 99 < 00
- System is able to correctly sort date fields on both sides of century.

**6.2.5 Date Interface**

- System is correctly able to pass date values to external devices and systems
- System is correctly able to maintain date information in the upstream/downstream chain



## A MILLENNIUM SURVIVAL GUIDE FOR IT PERSONNEL

### OVERVIEW

#### Failure to resolve Millennium issues will:

- Compromise our commitment to the health and safety of our workers and the public
- Force generating plant shutdowns
- Impair our ability to deliver energy
- Adversely impact how we realize and account for revenue
- Create consequential liabilities

The *Millennium Survival Guide* is a document that provides the Application Developer with an understanding of the Year 2000(Y2K) date problem, and methods to resolve today's non-compliant code problems and methods to prevent non-compliant application development in the future.

The company has over 1500 applications. Each application has to be reviewed and a millennium strategy decision has to be made for each. Is the application acceptable as is? Does the application require coding modifications? Is the application obsolete? Will we replace the application? Does the application require a version upgrade?

A recommended approach is to first read the guide in its entirety. Then, depending on whether you are developing a new application, validating an application for Y2K compliance, converting a non-compliant application, replacing a non-compliant application, or upgrading a non-compliant vendor package, follow the appropriate steps outlined in the *Action List* section.

### THE PROBLEM

The Year 2000 problem is easy enough to describe. Most computer systems represent dates in the format MMDDYY, where 12/31/95 represents December 31, 1995. The century is not represented in the date, and we simply assume that 12/31/95 refers to 12/31/1995. Most computer programs that perform arithmetic and logic operations on these date fields use only the last two digits of the year when they make their calculations. As long as all the dates in question are in the same century, this works fine. Problems arise, however, when the century changes. Subtracting 12/31/95 from 12/31/05 to determine someone's age, for example, does not produce the correct answer of 10. It actually produces a result of -90.

Although the problem is easy to describe, it is very difficult to solve for a number of reasons, and can be compared to looking for a needle in a haystack. The visual image of looking through hay is not difficult to conjure up, but the painstaking execution of the solution is awesome. The sheer size of the problem is the first of these. Dates are everywhere, which means that all program code must be examined to determine if a change is necessary. Utilities, like most large corporations, has thousands of programs containing millions of lines of code. A programmer will have to examine each of those lines and make a decision as to whether or not it has to be changed for the Year 2000. A date field can be called date, or it can be called ball game. Many people in the data processing industry, when confronted with the Year 2000 issue, refuse to believe the size or scope of the problem. Many of them argue that changing dates to include a century should be a relatively easy process. This fails to take into account the large number of changes that must be made, as well as, the coordination and testing of those changes. Ownership of the problem is critical to its solution.

#### **DEFINITION OF MILLENNIUM COMPLIANT**

The term, "**Millennium Compliant**," is the quality of a system to provide all of the following functions:

- Handle date information before, during, and after January 1, 2000, including, but not limited to, accepting date input, providing date output, and performing calculations using dates or portions of dates
- Function accurately and without interruption before, during, and after January 1, 2000, without any change in operations associated with the advent of the new century
- Respond to two-digit year date input in a way that resolves the ambiguity as to century in a disclosed, defined, and predetermined manner
- Store and provide output of date information in ways that clearly define century

#### **PURPOSE OF THE MILLENNIUM PROGRAM**

The Millennium Program has been put in place to ensure against the unacceptable business consequences of computer systems failing as a direct result of millennium date incompatibility.

The Millennium Program has been put in place to protect and preserve investment in information technology by preventing significant computer system failures that would result from the inability of existing systems to accurately manage dates in the Year 2000 and beyond.

The Millennium Program will provide focus and consulting to business units in their efforts to fix non-IT equipment. IT equipment is any equipment that is under the maintenance and support accountability of any professional IT provider in the company or a contractor thereto.

The Millennium Program will provide focus, standards, program management, and resources to the IT community to fix all computer systems which they and the business unit system owners determine will fail as a direct result of millennium date incompatibility resulting in unacceptable business consequences.

The Millennium Program will seek out and require all computer system vendors to certify compliance of their systems in writing to the company, or, in the absence of such certification, will recommend a course of action to the appropriate managers.

The Millennium Program will budget all costs associated with enterprise level initiatives (e.g., awareness campaigns, outsourcing of work), as well as costs to analyze, define, design, test, implement, and verify compliance.

Costs associated with any end user labor resources needed to validate the business functionality of the systems will be budgeted by the business units.

Costs associated with fixing non-IT equipment will be budgeted by the business units.

#### WHO DO I CALL FOR HELP?

The Millennium Team is here to help. We welcome your questions, comments, suggestions, and ideas. We are all located at XXXX. Here is how to contact us:

	<u>Internet Address</u>	<u>Telephone</u>
Name	xxxxxx	XXXX

#### YEAR 2000 TESTING

Year 2000 testing requires that the Application Developer develop test cases primarily for input data testing of numerous conditions including leap year, date transaction validation, day/week/month in week/month/year calculations, data integrity, sequencing (i.e., JCL sort parameters, internal program sort), and time-sensitive data. In addition, every user must determine that his/her PC's system clock is Year 2000 compliant. Conditions at the Application Environment and Platform levels must be taken into account, as well.

The Software Millennium Test Development Guidelines Section should assist you in preparing these test cases:

- This section contains testing conditions that application developers must consider in preparing for YEAR 2000 changes.

- It also provides test conditions and associated date values—valid or invalid—for test cases especially applicable to unit testing. This is an ever-changing document and is updated and stored on the Lotus Notes *Millennium Document Library* under “Y2K Software Millennium Test Development Guidelines”.

### Conversion Methods

The Millennium Team is identifying and categorizing all applications by surveying application owners and compiling an application inventory. Application owners were able to identify their applications as applications that are required to be in service after the Year 2000, applications that are intended to be rewritten or replaced with a vendor package, or applications that are no longer necessary and considered obsolete.

All applications that are deemed required after the Year 2000 can be broadly categorized as either compliant (correctly processes date logic) or non-compliant (incorrectly processes date logic). These applications must be tested for compliance regardless of whether the application was originally categorized as compliant or non-compliant. From a high level perspective the following must occur for each application required to be in service after the Year 2000:

1. Identify the application as needed to be Year 2000 validated or modified to make it Year 2000 Compliant.
2. Develop and run a Year 2000 Test appropriate for the application.
3. Evaluate results. The process is complete if the Year 2000 Test proves that one of the following conditions is true:
  - *The application is compliant.*
  - or*
  - *The Year 2000 non-compliance is such that we can continue to use the application and do our work without the need for additional work. In other words, if the consequence of non-compliance is acceptable (i.e., a minor problem such as a report date or system that will only be non-compliant for a short period of time) the system may not be converted.*

***The process will continue with the remaining steps only if the Year 2000 Test proves that all or a portion of the application needs further work***

1. Run a Baseline Test—using an existing (modified, if necessary) or a new Baseline Test—to provide a reference to ensure that the functionality of the application has not changed after the code has been changed. This Baseline Test can be limited to only those portions of the code that have been changed.
2. Direct the programmers to make the Year 2000 coding changes.

3. Rerun both the Baseline Test and the Year 2000 Test to guarantee that there are no functionality changes and that the application is Year 2000 compliant.

The actual conversion (Step 5 above) can take place several different ways. We can convert an application with in-house resources, supplement in-house resources with contractors, or package the application and send it through the Conversion Factory that has been established. The Millennium Team will ensure a smooth conversion.

The Millennium Team has developed several detailed methodology templates for conversions and validations for both mainframe and client server applications. Each methodology addresses different situations by including different steps to follow to complete the conversion/validation. Each template has an associated checklist of detail procedures to follow for each of the steps. The following is a list of the currently developed templates and a brief description.

### **Detailed Methodology Templates**

#### ***Mainframe Full Conversion Vendor with Baseline***

A mainframe application will be converted by the selected conversion vendor off-site or on COMPANY premises. *(Template #1)*

#### ***Mainframe Full Conversion In-house With Baseline***

A mainframe application will be converted by company personnel. *(Template #2)*

#### ***Mainframe Limited Conversion In-house Without Baseline***

A mainframe application will be converted by company personnel. *(Template #3)*

#### ***Mainframe Validation With Baseline***

A mainframe application will be validated for Year 2000 compliance by company personnel. *(Template #4)*

#### ***Mainframe Validation Without Baseline***

A mainframe application will be assessed for Year 2000 compliance by the selected conversion vendor. *(Template #5)*

**Mainframe Vendor Package Validation with Baseline**

A mainframe application will be validated for Year 2000 compliance by company personnel. (*Template #6*)

**Mainframe Vendor Package Validation Without Baseline**

A mainframe application will be assessed for Year 2000 compliance by the selected conversion vendor. (*Template #7*)

**Non-Mainframe Validation**

A non-mainframe application will be validated for Year 2000 compliance by company personnel. (*Template #8*)

**Non-Mainframe Conversion**

A non-mainframe application will be converted by company personnel. (*Template #9*)

These templates can be found in the Lotus Notes *Millennium Document Library* under "Conversion Templates." If you do not have access to the Millennium Document Library or do not have access to Lotus Notes, please contact a representative of the Millennium Team for assistance.

**Overview of the Conversion Options**

Once an application has been identified, and a methodology template has been chosen, the application developer must decide upon the specific technique to be used to bring each application program into compliance. The specific techniques include bridging, windowing, or date expansion, or simply not convert. The following briefly describes each technique:

**Bridging**

Bridging is the conversion method of choice if there are more than a few dates within a program. Bridging logic is added at the beginning of each program to expand the year to include the century. Bridging logic is also added at the end of each program to remove the century from the year. Therefore, data files coming in and going out of the program will remain in the same



format. The century will be determined by a common program that will be accessed by each program in the application. Century will be determined by the following rule:

- If a year field is greater than 35 (e.g., "36" through "99"), "19" will be assumed to be the century. However, if the year is less than or equal to 35 (e.g., "00" through "35"), "20" will be assumed to be the century. This rule applies only if the application does not use dates prior to 1935.

*The previously mentioned bridging process requires substantial setup such as cloning copybooks, creating new modules, and adding program logic containing a series of "Moves." Thus, the bridging process is not efficient unless there are more than a few dates.*

### **Windowing**

Windowing is the conversion method of choice if there are only a few dates within a program. Instead of adding logic at the beginning and end of the program, Windowing logic is added following each date reference in the program. As in Bridging, each date is expanded to include the century. Again, data files coming in and going out of the program will remain in the same format. The century will not be determined by a common program; it will be determined by its own logic. The following rule will be used to determine the century:

- If a year field is greater than 35 (e.g., "36" through "99"), "19" will be assumed to be the century. However, if the year is less than or equal to 35 (e.g., "00" through "35"), "20" will be assumed to be the century. This rule applies only if the application does not use dates prior to 1935.

### **Date Expansion**

Expanding the field in a file or column in a database is another conversion option. With this approach data will be physically expanded to reformat dates to a four digit year or other compliant format (DATE data type). *This is not a recommended method for mainframe applications.*

### **No Conversion**

As a final option, company may choose not to convert an application that is non-compliant. Company may choose to accept a certain level of non-compliance if the consequence of non-

compliance is acceptable (i.e., a minor problem exists, such as a report date or system that will only be non-compliant for a short period of time).

## DATE STANDARDS RECOMMENDED TO BE YEAR 2000 COMPLIANT

As the need to exchange information across network boundaries increases, lack of common standard practices will become a formidable barrier to interoperability. It was identified that there are a variety of date standards being used within Company's IT complex. Depending on the environment and software/language or coding method, each application seems to maintain its own technique of expressing and storing date data. Many applications maintain different formats for input, output, display, and storage. Some have Julian formats, other have Gregorian formats, and even among those Julian and Gregorian formats, there are differences in representations (e.g., MMDDYY, YYMMDD, YYDDD). Some applications maintain numeric date formats as *binary, display, or packed* and others have alphanumeric representations. Applications sharing different date formats may be subject to additional risk of failure such as DATE data being distributed between different technologies (i.e., DB2, SYBASE) or downline feeds (i.e., Indus to other ad hoc applications).

**For data input, report output, and screen displays, the USA standard date is to be utilized at COMPANY.** This standard provides consistency for viewing and entering date data. The format of the USA Standard is:

Std	Name	Format	Length	Display
USA	IBM USA Standard	MM/DD/YYYY	10	01/15/1996

**For data storage, most applications should use the current System date/time data type format supplied by their software.** The advantage to this is that numbers representing dates and times can be stored in columns with numeric data types. Applications such as DB2 or SQL Servers (i.e., SYBASE) have the ability to recognize and load date or time values from outside sources, converting valid input values to their internal format. Another advantage is that they can store date and time information from January 1, 1753 through December 31, 9999.

**There are some applications that cannot conform to a date data type format (i.e., ADABAS), and, therefore, should default to a character "8" ISO format (listed below).** Although some COMPANY applications areas developed ADABAS systems in the past, the use of ADABAS is not the strategic direction for the company. In the future, as the larger ADABAS systems get replaced by packages and the smaller ones are converted into existing client server applications, the inconsistency between the two formats will become less of an issue. The format of the ISO Standard is:

Std	Name	Format	Length	Display
ISO	International Standards Organization	YYYYMMDD	8	19960115

## ACTION LISTS

For any application developer at COMPANY, surviving the Y2K challenge will mean developing new applications that are Y2K compliant, validating existing applications for Y2K compliance, version upgrading for a non-compliant vendor package, replace with new vendor package or the actual conversion of applications for Y2K compliance. From a high level perspective, the following items should be performed for each unique application challenge.

### ***New application development requires the following:***

#### Understand the problem

Application developers must first understand the Y2K issues outlined in the beginning of the survival guide. Please refer to *Background*, *Magnitude of Problem*, and *Definition of Millennium Compliant* in the Survival Guide.

#### Understand Application Conditions

There are many things that an application can do that can cause non-compliance. Please refer to the *Application Conditions* section of the Survival Guide

#### Follow COMPANY date standards

The Millennium Team has developed display and storage date standards. Please refer to *Date Standards at COMPANY* section of the Survival Guide.

#### Develop new application using COMPANY date standards

Develop an application following all COMPANY standards and guidelines for new development including COMPANY date standards to ensure Y2K compliance.

#### Validate compliance using Y2K test plan

Develop a test plan that ensures all application transactions and conditions are Y2K compliant. Please refer to *Year 2000 Test Conditions* section of the Survival Guide or Step

4 Prepare Baseline/Y2K test cases in any methodology template identified in *COMPANY Conversion Method* section of the Survival Guide.

***Version Upgrading of existing applications requires the following:***

**Understanding the problem**

Application developers must first understand the Y2K issues outlined in the beginning of the survival guide. Please refer to *Background, Magnitude of Problem, and Definition of Millennium Compliant* in the Survival Guide.

**Check for new version application conditions that may cause non-compliance**

There are many things that an application can do that can cause non-compliance. Please refer to the *Application Conditions* section of the Survival Guide

**Validate compliance using Y2K test plan**

Develop a test plan that ensures all application transactions and conditions are Y2K compliant. Please refer to *Year 2000 Test Conditions* section of the Survival Guide or Step 4 Prepare Baseline/Y2K test cases in any methodology template identified in *COMPANY Conversion Method* section of the Survival Guide.

***Replacing with new vendor applications requires the following:***

**Understanding the problem**

Application developers must first understand the Y2K issues outlined in the beginning of the survival guide. Please refer to *Background, Magnitude of Problem, and Definition of Millennium Compliant* in the Survival Guide.

**Ensure that the Millennium compliance language is in contract with vendor.**

Company requires that all purchased and/or leased products meet date compliance requirements into and beyond the Year 2000 , with no interruption of service or additional expense. Any and all costs including, but not limited to, product upgrades and direct expenses incurred due to failures caused by the change in century, shall be the responsibility of the vendor.

If the product is, or will not be designed to meet Year 2000 compliance, the vendor must notify in writing prior to entering into any purchase agreement.

**Check for application conditions that may cause non-compliance**

There are many things that an application can do that can cause non-compliance. Please refer to the *Application Conditions* section of the Survival Guide.

**Validate compliance using Y2K test plan**

Develop a test plan that ensures all application transactions and conditions are Y2K compliant. Please refer to *Year 2000 Test Conditions* section of the Survival Guide or Step 4 Prepare Baseline/Y2K test cases in any methodology template identified in *Conversion Method* section of the Survival Guide.

***Converting non-compliant applications requires the following:*****Understand the problem**

Application developers must first understand the Y2K issues outlined in the beginning of the survival guide. Please refer to *Background, Magnitude of Problem, and Definition of Millennium Compliant* in the Survival Guide.

**Check for application conditions that may cause non-compliance**

There are many things that an application can do that can cause non-compliance. Please refer to the *Application Conditions* section of the Survival Guide

**Follow the recommended standards for conversion**

The Millennium Team has identified several methodology templates for conversions and validations for both mainframe and client server applications. Please refer to the *Conversion Method* section of the Survival Guide to select the appropriate methodology template.

**Validate compliance using Y2K test plan**

Develop a test plan that ensures all application transactions and conditions are Y2K compliant. Please refer to *Year 2000 Test Conditions* section of the Survival Guide or Step 4 Prepare Baseline/Y2K test cases in any methodology template identified in *Conversion Method* section of the Survival Guide.

**Y2K Millennium Project****Roles and Responsibilities**

<b>High Level Tasks</b>	<b>Y2K Team</b>	<b>IT Staff Managers</b>	<b>Software Owner</b>
<b>Planning</b>			
1. Take ownership of the problem.		X	X
2. Validate for completeness the inventory of all applications.	X	X	X
3. Identify all developed application software.	X	X	X
4. Identify all vendor hardware and software.	X	X	X
5. Assume responsibility for a selected set of applications - Management Staff Responsibility (MSR) List		X	
6. Identify applications that are maintained by IT staff Managers.	X	X	X
7. Identify quality software/applications.	X	X	X
8. Initiate vendor Y2K compliance process.	X		
<b>Scheduling</b>			
1. Choose project conversion option.		X	X
2. Determine whether the work can be done by programming environment, or supplemented by the Y2K team resources. Find resources if staff is not available.	X	X	X
3. Identify/Commit/Coordinate resource to do the validation and/or conversion work.	X	X	X
4. Provide start date and a projected completion date for application to be validated or converted.		X	X
<b>Conversion/Validation</b>			
1. Provide Departmental Instructions for application testing or conversion.	X		
2. Develop a test plan for the applications for which you have responsibility.		X	X
3. Convert/Validate the application.	X	X	X
4. Test application for Y2K compliance.	X	X	X
<b>Sign Off</b>			
1. Sign off on the application indicating that it is obsolete, compliant, or ignored.		X	X



**SOFTWARE MILLENNIUM TEST DEVELOPMENT GUIDELINES**

Software Title: \_\_\_\_\_ Revision No. \_\_\_\_\_

Application (if different from Software Title): \_\_\_\_\_

Software Owner, Title: \_\_\_\_\_

Prepared By, Title: \_\_\_\_\_

During the process of testing, apply a combination of verification and validation techniques. These techniques include:

1. **Unit Testing**
  - 1.1. Testing the System Clock
  - 1.2. Input Testing
  - 1.3. Data Testing
2. **System Testing**
  - 2.1. Stress Testing
  - 2.2. Recovery Testing
  - 2.3. Regression Testing
  - 2.4. Error Handling Testing
  - 2.5. Manual Support Testing
  - 2.6. Parallel Testing
3. **Integration Testing**
  - 3.1. Intra- and inter-System Testing
4. **PC Testing**

The following sections will cover some useful testing techniques and scenarios for Year 2000 testing. They are not meant to be all inclusive. Therefore, it is important that additional tests be developed, as appropriate, for the application.

**Attention:** By nature, Year 2000 exposures are time-sensitive and time-driven. Be cautious before resetting the system timer. Some system resources and functions are time-sensitive and may be activated or de-activated when the system clock is reset. Such effects can occur when the system clock is either set forward or backward. Without careful planning, you could cause the loss of these system resources and/or functions, some of which might contaminate the production system or production data bases when running various test scenarios.



Test Applicable <small>(if check is valid)</small>		Compliant		Test	Test Applies to:	Comments
Yes	No	Yes	No			
				1. Expiration Test	Mainframe/Client Server	
				- User IDs		
				- Passwords		
				- Authorization/protection access		
				- Network access		
				- Automation functions		
				- SMS (System Managed Storage)/HSM (Hierarchical Storage Management) migrated data sets earlier than expected		
				2. Label driven tape datasets - are tapes expired earlier than expected? (i.e., validate label parameter expiration (99365, 99366))	Mainframe/Client Server	
				3. Archiving data expired earlier than expected?	Mainframe/Client Server	
				4. (12/31/1999 23:55 hrs) Monitor screen and transaction behavior	Mainframe/Client Server	

**Unit Testing**

Unit test is performed on one piece of software module at a time and is an exhaustive test of all logic within the module to demonstrate correctness and adherence to applicable specification and design requirements. Unit test should focus on exposing defects within the module logic (try to make it fail).

**Testing the System Clock** - This test involves resetting the system clock to identify problems which could occur (software, firmware, hardware, system access, etc.) when the century changes.

Unit Testing-Continued					
Test Applicable ( <i>eg</i> check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			- Validate that dates are calculated and displayed correctly (i.e., 1999 rolls into 2000, <b>not</b> 1900)		
			5. Validate End of Processing logic to see if dates will be incorrectly interpreted and/or used.	Mainframe/Client Server	

Input Testing - Apply requirements testing to verify that the system performs its function correctly and that it remains functional over a continuous period of time.					
Test Applicable ( <i>eg</i> check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			1. Will program respond correctly if "00" or "2000" is entered.	Mainframe/Client Server	
			2. Is a 4-digit year accepted or is it truncated?	Mainframe/Client Server	
			3. Ensure xx/xx/xx date =xx/xx/xxxx after expansion or conversion for all databases and tables.		

**Data Testing** - Set the clock to test process cycles and automatic functions that are activated on a regular basis. These scenarios can be used to identify Year 2000 exposures that need to be fixed as well as to validate programs after applying Year 2000 solutions.

Test Applicable (☐ Check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			1. Leap Year - Ensure that year 2000 is processed as a leap year. - 1996/2/29 should pass (1996 is a leap year) - 2000/2/29 should pass (2000 is a leap year) - 2004/2/29 should pass (2004 is a leap year)	Mainframe/Client Server	
			2. Invalid Leap Year Test - 2/29/1999 non-leap year - 2/29/2001 for non-leap year	Mainframe/Client Server	
			3. Date Transaction Validation - (01/01/2000) Test processing for the first calendar day of the year - (01/31/2000) Test and validate processing for the last business and calendar day of the month	Mainframe/Client Server	
			4. Day-in-year calculation test - Does year 2000 have 366 days (not 365)?	Mainframe/Client Server	

Data Testing - Continued				Test	Test Applies to:	Comments
Test Applicable (or check if valid)	Compliant		Test			
	Yes	No				
			5. Day-of-the-week calculation test	Mainframe/Client Server		
			- 02/28/2000 should be a Monday			
			- 03/01/2000 should be a Wednesday			
			- 01/03/2000 First business day of week			
			- 01/03/2000 First business day of month			
			- 01/03/2000 First business day of year			
			- 01/07/2000 Last business day of week			
			6. Week-of-the-year calculation test	Mainframe/Client Server		
			- The 11th week of the year 2000 is 3/5 to 3/11			
			7. End-of-Week Test	Mainframe/Client Server		
			- 01/08/2000 should be a Saturday			
			- 01/09/2000 should be a Sunday			

Data Testing - Continued		Test	Test Applies to	Comments
Test Applicable (☑ check if valid)	Compliant Yes No			
		8. Data Integrity - Are years 1800, 1900, 2000 distinguishable between one another? - Validate for hard coded century occurrence of "19" and/or "20" in program code. - Calculations - Look at programming logic to see if the usage of dates/date ranges in calculations will be correct - Calculations - Check calculation when extends coverage into Year 2000 and verify future billing amounts are not impacted.	Mainframe/Client Server	
		9. JCL/DCL CONTROL LANGUAGES - Ensure sorts use dates properly in processing - Validate and test sort parameters - Review sorts internal to programs - Validate sort data sequence - Record length adjusted - validate that increase records size are reflected in Record Length (LRECL - Logical Record Length) field. - Validate that Blocksizes a multiple of LRECL	Mainframe/Client Server	

Survival Guide for IT Personnel

Data Testing - Continued				Test	Test Applies to:	Comments
Test Applicable (or check if valid)	Compliant		Test			
	Yes	No				
			10. Age Test	Mainframe/Client Server		
			- Use 12/31/1999 to verify age and date of birth calculations			
			- Validate processing for roll-over to 2001			
			11. Time-sensitive data (may not be applicable to some applications)	Mainframe/Client Server		
			a.) Use current system clock and test data with dates.			
			- Before 01/01/2000			
			- After 01/01/2000			
			b.) Set system clock to 12/31/1999 and test data with dates:			
			- Before 01/01/2000 (12/15/1999) validate transaction calculations are correct within 10, 15, and 30 day period			
			- After 01/01/2000 validate that everything behaves normally as 2000 approaches			

Data Testing - Continued					
Test Applicable (☐ check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			c.) Set system clock after 01/01/2000 and test data with dates: - Before 01/01/2000 validate backdated calculations are correct within 10, 15, and 30 day period) - After 01/01/2000 Test - Set system clock to (02/29/2000) validate backdated calculations are correct within 45, 60 and 90 day period - Set system clock to (03/31/2000) validate processing for the last business and calendar day of the quarter - Set system clock to (03/31/2000) validate processing for the last business and calendar day of the quarter		

<b>System Testing</b>			
System Testing ensures sufficient testing of a function's implementation and helps determine that all structures of the system are integrated to form a cohesive unit.			
<b>Stress Testing</b> - apply stress testing to determine if the system can function when transaction volumes are larger than normally expected. The typical areas that are stressed include disk space, transaction speeds, output generation, computer capacity, and interaction with people. When testing Year 2000 changes, it is essential to verify that the existing resources can handle the normal and abnormal volumes of transactions after the restructuring of the code and the possible expansion of the data fields. For example, apply stress tests to determine:			
Test Applicable (if check is valid)	Compliant		Test
	Yes	No	
			1. Can environment sufficiently accommodate the additional disk space required to support 2 to 4 digit expansion (DASD)?
			2. Are additional CPU cycles required to support code conversion (i.e., 2 digit encoding/compression scheme) region size?
			3. Is response time adequate to support user turn around time?
			4. Do file definitions need to be reformatted (i.e., CI Splits, Data Dictionaries)?
			Test Applies to: Mainframe/Client Server
			Test Applies to: Mainframe/Client Server
			Test Applies to: Mainframe/Client Server
			Test Applies to: Mainframe/Client Server
			Test Applies to: Mainframe/Client Server
			Test Applies to: Mainframe/Client Server



**Recovery Testing - Recovery Testing** is used to ensure that the system can restart processing after losing system integrity. This is essential for systems in which the continuity of operation is critical to end users. Recovery processing normally involves the ability to go back to the last checkpoint, then reprocess up to the point of failure. Can system restart processing after losing system integrity?  
 Any data integrity or unresolved exposures that lead to inconsistent data or code after you have implemented appropriate Year 2000 solutions will affect the completeness of backup data.

Test Applicable (If check is valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			1. Can application go back to the last check point then reprocess up to the point of failure?	Mainframe/Client Server	
			2. Is documentation complete to support the manual manipulation of data?	Mainframe/Client Server	
			3. Can the system handle unconverted data (bridging available)?	Mainframe/Client Server	
			4. Verify results when a date is entered in one format (e.g. yymmddccymmdd) and displayed in a different format (e.g. mmddyy/mmddccyy). (2-byte MF...4-byte CIS format). Test for Julian dates, especially for calculations and Job Schedule Calendar.	Mainframe/Client Server	

**Regression Testing.** Ensures that all aspects of a system remain functionally correct after changes have been made to a program in the system. Because the potential exists for a tremendous amount of data and programs to be involved in your Year 2000 transaction, any change to an existing program in the system can have a snowballing or cascading effect on other areas in the system. A change that introduces new data or parameters, or an incorrectly implemented change can cause a problem in previously tested parts of the system, simply because of the way data can be shared between software entities.

Test Applicable (or check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			1. Are user requirements followed (i.e., quality assurance)?	Mainframe/Client Server	
			2. Changes meet design specifications?	Mainframe/Client Server	
			3. Changes compliant with organization's policies and procedures?	Mainframe/Client Server	
			4. Validate data output records - data field following date field expansion.	Mainframe/Client Server	
			5. Validate data output records - data field in front of date field expansion.	Mainframe/Client Server	
			6. Validate on-line screen display field for error.	Mainframe/Client Server	
			7. Ensure all scheduling based on date return the same results before and after Y2K changes.	Mainframe/Client Server	
			8. Ensure conditions cover time zone differences.	Mainframe/Client Server	
			9. Ensure all extracting basedate returns the same results before and after Y2K changes.	Mainframe/Client Server	

Regression Testing- Continued				Test	Test Applies to:	Comments
Test Applicable (or check if valid)	Compliant		Test			
	Yes	No				
			10. Ensure all index processing based on date returns the same results before and after Y2K changes.	Mainframe/Client Server		
			11. Ensure all subscripting based on e returns the same results before and after Y2K changes.	Mainframe/Client Server		

**Error Handling Testing** - Determines if the system can properly process incorrect transactions that can be reasonably expected as types of error conditions. Error-handling testing is necessary to determine the ability of the system to properly process incorrect transactions that can be reasonably expected as types of error conditions. For example, programs that accept only 4-digit year data entry format need to provide error messages for data entry in 2-digit year format, and vice versa for programs that accept only 2-digit year data entry format. When changing from 2-digit year format to 4-digit year format, you need to apply error-handling testing to verify the appropriate error-handling functions.

Test Applicable (or check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			1. Normal error handling for current 4 digit year data entry when 2 digit data entry occurs.	Mainframe/Client Server	
			2. Normal error handling for current 2 digit year data entry when 4 digit data entry occurs.	Mainframe/Client Server	

**Manual Support Testing** - Evaluate the process by which the end user handles new data generated from the automated applications with Year 2000 support. Types of data from these applications include data entry and report generation. Any new data format should be easy to understand and *not* ambiguous. This method includes testing the interfaces (for example screens, procedures, operation manuals, and online HELP panels) between end users and the application

program. End users should be trained and use procedures provided by the system personnel. Testing should be conducted without any other assistance.

Test Applicable (Ez check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			1. Are new field on on-line screens ambiguous?	Mainframe/Client Server	
			2. Operation manuals updated with new procedures?	Mainframe/Client Server	
			3. On-line HELP panels updated?	Mainframe/Client Server	

Test Applicable (if check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			1. Validation output report - Determine if data displays will be acceptable (compliant) in Year 2000 - Date fields - Non-date fields - Report headers - Report footers	Mainframe/Client Server	
			2. Validate on-line screens - Determine if data displays will be acceptable (compliant) in Year 2000 - Date fields - Non-date fields - Screen headers - Screen footers - On-line screen help	Mainframe/Client Server	
			3. Validate that hard-coded dates or century indicators are <b>not</b> located in output records.	Mainframe/Client Server	

Parallel Testing - Continued					
Test Applicable (☒ check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			4. Validate that hard-coded dates or century indicators are <b>not</b> located on output reports.	Mainframe/Client Server	
			5. Validate that hard-coded dates or century indicators are <b>not</b> located on screen displays.	Mainframe/Client Server	
			6. Validate output reports for zero suppression (i.e., year "00" would <b>not</b> display).	Mainframe/Client Server	
			7. Validate screen displays for zero suppression (i.e., year "00" would <b>not</b> display).	Mainframe/Client Server	
			8. Verify that the portion of the system that have <i>no</i> changes still runs properly as changes are made to other portions of the system.	Mainframe/Client Server	
			9. Verify that the program handles all its transactions correctly and remain stable for a defined period of time.	Mainframe/Client Server	
			10. Ensure that programs (or table subscripts) can handle date ranges that cross Millennium - Some programs used dates as subscripts. (i.e., "00" for Year 2000 would be an invalid entry, September 1999 "999" may be considered as an end of file marker.)	Mainframe/Client Server	

<b>Integration Testing</b>				
<b>Intra- and Inter-System Testing</b> - Applications are frequently connected with other applications to provide a higher or deeper level of functionality. Data may be shared between applications or systems. Inter-system testing is required to ensure that the connection functions properly between the applications. This test determines that the proper parameters and data are correctly passed between applications, and proper coordination and timing of each function exists between applications.				
Test Applicable (if check is valid)	Compliant		Test Applies to:	Comments
	Yes	No		
			Mainframe/Client Server	
			Mainframe/Client Server	
			Mainframe/Client Server	

Test Applicable (☐ Check if valid)		Compliant Yes No		Test	Test Applies to:	Comments
<p align="center"><b>PC Testing</b></p> <p>Some older models of the PC may <b>not</b> have the capability to set or roll over the system clock beyond the year 2000 because the Basic Input/Output System (BIOS) is unaware of the century digit. ( Ex. ROMBIOS in most older PCs can <b>not</b> handle the year 2000 rollover correctly. Different versions of BIOS behave in different manners. Some roll the date to 1/4/00 or 3/1/00. Some roll the date to 1/1/80 or 3/1/80. Some just leave the date at 12/31/99)</p>						
				1. Test if the system clock can be set beyond the year 2000. - Set the system clock to 01/01/2000, reboot PC and recheck the date.	PC	
				2. Test system clock automatic update function. a.) Test the system clock automatic update function when the power is on. - Set clock to 12/31/1999, 23:58:00, keep power on, validate date when clock reaches the year 2000. - Power off PC and recheck the DOS date. b.) Test the system clock automatic update function when the power is off. - Set system clock to 12/31/1999, 23:56:00, power off PC and wait until the clock reaches the year 2000. - Power on PC and recheck the DOS date.	PC	



PC Testing - Continued		Test	Test Applies to:	Comments
Test Applicable (E) check if valid)	Compliant Yes No			
		3. Test time update by the operating system a.) Update After Suspension of a time-sensitive program. - Set system clock to 12/31/1999, 23:58:00; suspend a time display program without a "wake up" timer; keep power on; wait until the clock reaches the year 2000; resume time display program; and check the date. b.) Update After Suspension and Wake Up of time-sensitive program: - Set system clock to 12/31/1999, 23:58:00; suspend a time display program with a "wake up" timer set at 01/01/2000, 00:01:00; keep power on; wait until the time display program "wakes up"; check the date.	PC	
		4. Leap Year Test a.) Change date 02/29/2000. If an error occurs, then BIOS is incorrect.	PC	
		5. Test CPU a.) Use different machines (286/386, etc.) when executing tests to ensure processing time isn't impacted.	PC	

NEI/NUSMG 97-07  
October 1997

Survival Guide for IT Personnel

## Assessing Computer Software for Millennium Compliance

### 1. OBJECTIVE

This instruction establishes a method for assessing computer software to ensure software will be millennium compliant by the year 2000. The assessment consists of testing, and if required, the effort necessary to bring non-millennium compliant software into compliance (i.e., "conversion"). "Millennium Compliant" is the capability of a system to provide the following functions, if applicable to the system:

NOTE: Date processing is obvious when the date is entered manually. However, the date may be input into software automatically (e.g., the date can be a value from another software program, the software can 'read' a device that provides the date, or it can be calculated using an offset from a pre-established entry.

- Process date information before, during, and after January 1, 2000, including, but *not* limited to:
  - ◊ the ability to enter the date,
  - ◊ the ability to output the date, and
  - ◊ the ability to perform calculations on, or using, the date or portions of the date.
- Operate accurately and without interruption before, during, and after January 1, 2000, without any change in operations associated with the advent of the new century.
- Recognize a two-digit year date input (e.g., '98', '99', '00') in a way that resolves the ambiguity as to century.
- Store and provide output of date information in ways that will *not* be ambiguous between the centuries 1900 and 2000. For example, many computer programs perform arithmetic and logic operations on their data field and use only two digits of the year instead of four. This presents a problem when the century changes. For example, subtracting 12/31/95 from 12/31/05 to determine someone's age does *not* produce the correct answer of 10. It actually produces a result of -90, therefore missing the intent of that calculation.

**2. REFERENCES and ATTACHMENTS****References**

- 2.1 DC 11, "Computer System Use and Control"
- 2.2 DC 14, "Administration of Controlled Software"
- 2.3 ACP-QA-2.27, "Infrequently Performed Tests and Evaluations"
- 2.4 ACP-QA-9.03, "Inservice Plant Testing"
- 2.5 NGP 3.12, "Safety Evaluations"
- 2.6 NRC Notice Nuclear Safety Engineering Report, "Year 2000 Effect on Computer Systems" (web site: <http://www.nrc.gov/NRC/NEWS/in96070.txt>)
- 2.7 Year 2000 Understanding the Problem (Copy available from Computer Services department)
- 2.8 A Survival Guide For IT Personnel in Application Development (Copy available from Computer Services department)
- 2.9 NGP/QS-11, "Quality Software Manual (QSM)"

**Attachments**

Attachment 1.0 - DEFINITIONS AND ACRONYMS

Attachment 2.0 - SOFTWARE MILLENNIUM TESTING

Attachment 3.0 - SOFTWARE MILLENNIUM TEST DEVELOPMENT GUIDELINES

**3. PROCEDURE****3.1. Assign Software Owner and Obtain Assistance.**

3.1.1. IF not already assigned, ASSIGN Software Owner in accordance with DC 11, Rev 1, Section 1.2.

**NOTE:** The Millennium Project Team (MPT) was created to ensure software applications are qualified for operation during and beyond the year 2000. The MPT can be contacted by calling the Administrative Assistant,

3.1.2. IF assistance is required in performing any steps of this instruction, CONSULT the individual who has Management Staff Responsibility (MSR) for the application. CALL, for the name of the MSR for a specific application.

**3.2. Document if Software will be retired prior to date related problems or is currently retired.**

3.2.1. IF software will be retired prior to any date related problems, PERFORM the following:

- a) INDICATE on Attachment 2, "Software Millennium Test Signoff," that software will be retired prior to date related problems.
- b) PROVIDE a contingency plan if the software will not be retired prior to date processing problems, affix plan to Attachment 2.
- c) OBTAIN appropriate signatures on Attachment 2.
- d) SEND a copy of Attachment 2 with contingency plan to the MSR.
- e) IF Quality Software, include Attachment 2 with contingency plan in the Software Document file.
- f) IF Controlled Software, MAINTAIN Attachment 2 with contingency plan.
- g) IF Quality or Controlled Software, SEND a copy of attachment 2 with contingency plan to Nuclear Document Services.
- h) EXIT this procedure.

3.2.2. IF software is currently retired, **PERFORM** the following:

- a) **INDICATE** on Attachment 2, "Software Millennium Test Signoff," that Software is retired.
- b) **OBTAIN** appropriate signatures on Attachment 2.
- c) **SEND** a copy of Attachment 2 to the MSR.
- d) IF Quality Software, include Attachment 2 in the Software Document file.
- e) IF Controlled Software, **MAINTAIN** Attachment 2.
- f) IF Quality or Controlled Software, **SEND** a copy of attachment 2 to Nuclear Document Services.
- g) **EXIT** this procedure.

### 3.3 Determine if Vendor Certification of Compliance is Available

3.3.1. IF vendor supplied software, **CONTACT** MSR to determine if MSR has a record that vendor certified the software as millennium compliant.

3.3.2. IF vendor software is millennium compliant, **PERFORM** the following:

- a) **INDICATE** on Attachment 2, "Software Millennium Test Signoff," that millennium testing was **not** performed as "vendor certified software is millennium compliant."
- b) **OBTAIN** appropriate signatures on Attachment 2.
- c) **SEND** a copy of Attachment 2 and vendor certification to the MPT.
- d) IF Quality Software, **INCLUDE** Attachment 2 and vendor certification in Software Document File (SDF).
- e) IF Controlled Software, **MAINTAIN** Attachment 2 and vendor certification.

- f) IF Quality or Controlled Software, SEND a copy of attachment 2 and vendor certification to Nuclear Document Services.
- g) EXIT this procedure.

#### 3.4 Determine if Software Performs Date Input, Output, or Processing

- 3.4.1. EVALUATE -developed software and vendor software that has **not** been certified millennium compliant to determine if date input, output, or processing is performed by software.
- 3.4.2. IF it has been determined that software does **not** perform date input, output, or processing, PERFORM the following:
  - a) INDICATE on Attachment 2, "Software Millennium Test Signoff," that millennium testing was **not** performed as software does **not** perform date input, output, or processing.
  - b) OBTAIN appropriate signatures on Attachment 2.
  - c) SEND a copy of Attachment 2 to the MSR.
  - d) IF Quality Software, INCLUDE Attachment 2 in the Software Document file.
  - e) IF Controlled Software, MAINTAIN Attachment 2.
  - f) IF Quality or Controlled Software, SEND a copy of attachment 2 to Nuclear Document Services.
  - g) EXIT this procedure.

#### 3.5. Document if Software Can **not** be Tested and Millennium Compliance Can **not** be Determined

- 3.5.1. IF software can **not** be tested AND it can **not** be determined that date processing is performed by software, PERFORM the following:
  - a) INDICATE on Attachment 2, "Software Millennium Test Signoff," that software can **not** be tested.
  - b) PROVIDE a reason testing can **not** be performed with Attachment 2.

- c) Refer to RP4 (Corrective Action Program) and initiate CR (Condition Report).
- d) If Quality Software refer to QS-11, "Error Reporting and Corrective Action for Quality Software", and perform any additional error reporting activities.
- e) PROVIDE a contingency plan if software fails due to date processing problems, affix plan to Attachment 2.
- f) OBTAIN appropriate signatures on Attachment 2.
- g) SEND a copy of Attachment 2 with contingency plan to the MSR.
- h) IF Quality Software, include Attachment 2 with contingency plan in the Software Document file.
- i) IF Controlled Software, MAINTAIN Attachment 2 with contingency plan.
- j) IF Quality or Controlled Software, SEND a copy of attachment 2 with contingency plan to Nuclear Document Services.
- k) EXIT this procedure.

**3.6. Develop and Perform Millennium Test, Document Results, and Perform Conversion, if Applicable**

NOTE: Attachment 3, "Software Millennium Test Guidelines," lists different types of date processing performed by software. This attachment will be used to help determine appropriate date processing tests for the software being evaluated.

- 3.6.1. Refer To Attachment 3, "Software Millennium Test Development Guidelines," determine and check-off which software tests are applicable to the software being evaluated.

NOTE: Testing on some plant systems require special test procedures to be developed, reviewed and approved.



3.6.2. Refer to the following, as applicable for software, and DEVELOP a Software Millennium Test:

- Attachment 3, "Software Millennium Test Development Guidelines"
- IF applicable, ACP-QA-9.03, "Inservice Plant Testing"
- IF applicable, ACP-QA-2.27, "Infrequently Performed Tests or Evolution's"

3.6.3. IF required by DC-12, Refer To NGP 3.12, "Safety Evaluation" and PERFORM the following:

- a) ENSURE a 10CFR50.59 Safety Evaluation Screening on the test has been performed by a qualified safety evaluation screener.
- b) IF required by the 10CFR50.59 Safety Evaluation Screening, ENSURE a 10CFR50.59 Safety Evaluation on the test is performed by a qualified safety evaluator.

NOTE: Testing on many systems (e.g., plant system) will require use of AWO (Automated Work Order). Ensure proper approval of AWO prior to start of work.

3.6.4. Refer To Applicable work process and PERFORM Software Millennium Test.

3.6.5. INDICATE results of software testing on Attachment 2, "Software Millennium Test Signoff."

3.6.6. IF software is **not** millennium compliant:

- a) INDICATE on Attachment 2 if conversion will be performed.
- b) INCLUDE contingency plan if conversion **not** performed or **not** complete prior to date impact.
- c) Refer to RP4 (Corrective Action Program) and initiate CR (Condition Report) to indicate the software is not millennium compliant.
- d) If Quality Software refer to QS-11, "Error Reporting and Corrective Action for Quality Software", and perform any additional error reporting activities.

3.6.7. OBTAIN appropriate approvals on Attachment 2.

3.6.8. SEND a copy of completed and approved Attachment 2 to MSR.

3.6.9. PERFORM the following:

- IF software is Quality Software, MAINTAIN Software Millennium testing documentation in Software Document file.
- IF software is Controlled Software, MAINTAIN millennium test documentation.
- IF Quality or Controlled Software, SEND a copy of Millennium Test Documentation to Nuclear Document Services.

NOTE: 1. Effort to bring non-millennium compliant software into compliance (i.e., "conversion") may take different methods which depend upon the change required and the type of software (e.g., business application versus plant system). Some examples of possible conversion methods are software upgrades from a vendor, in-house code modifications, purchase of replacement software, or total system replacement. Use of the Design Control Process, prescribed in the DCM, may be required based upon the system impacted.

2. Replacement of software, systems containing software, vendor upgrades, and in-house software modifications all require the use of DC 11, "Computer System Use and Control."

3.6.10. IF testing results indicate millennium conversion is required AND conversion is desired, PERFORM the following:

- a) IF applicable, Refer to "Design Control Manual", and ENSURE appropriate corrective actions are performed.
- b) Refer To DC 11, "Computer System Use and Control" and PERFORM activities necessary to acquire, modify, upgrade, or develop software to satisfy millennium conversion.
- c) DETERMINE if step 3.1 applies. If it applies, PERFORM steps 3.1.1 through 3.1.2. to ASSIGN Software owner for new/converted software.

- d) DETERMINE if step 3.3 applies. If it applies, PERFORM steps 3.3.1 through 3.3.2. to determine if vendor certification of compliance is available for new/converted software.
- e) DETERMINE if step 3.4 applies. If it applies, PERFORM steps 3.4.1 through 3.4.2.
- f) EXIT procedure.

**Attachment 1****4. DEFINITIONS AND ACRONYMS**  
(Page 1 of 5)

Acceptance Testing - A test of the entire software program with data for production readiness.

Assign - To transfer or appoint to another resource/individual

AWO - Automated Work Order

Bridging - A method used to convert data to an acceptable format, external to the program logic.

Buffer - An area in memory in which data is stored temporarily to facilitate output or processing later.

Client Server - A network architecture in which each computer or process on the network is either a client or a server. Servers are powerful computers or processes dedicated to managing disk drives (file servers), printers (print servers), or network traffic (network servers). Clients are less powerful PCs or workstations on which users run applications. Clients rely on servers for resources, such as files, devices, and even processing power.

Computer - Programmable electronic device that can store, retrieve, and process data.

Computer Owner - The individual responsible for maintenance and operations of a computer system. The Computer Owner may be the Software Owner.

Contingency Plan - A formal document which contains an alternate course of action to be implemented when original plans can not be met. For example, the original application may have to be converted if the replacement project fails to meet Year 2000.

Controlled Software - See DC 11, "Software and Data Classification," to determine if software is controlled. Software that is **not** identified as Quality Software and is any of the following:

- Important to plant operation
- That whose erroneous output could impact plant operations
- For all Plant Process Computers, all software **not** identified as Quality Software is considered Controlled Software

CPU - Central Processing Unit - The central processor of the computer that controls the processing routines, performs arithmetic functions, and maintains memory.

**Attachment 1**  
**DEFINITIONS AND ACRONYMS**  
(Page 2 of 5)

DASD - Direct Access Storage Device (i.e. magnetic disk drives)

DATA - Information of any type, including binary data, hexadecimal numbers, integers, character strings, ASCII characters, etc.

DCB - Data Control Block - Properties that set dataset configuration.

DCL - Digital Control language, used by Digital Equipment Corporation (DEC)

DISK - A magnetic disk used to store information.

Error - A departure from the validated function of the Quality Software.

Firmware - Software contained on non-volatile media, such as Programmable Read-Only Memories (PROMs) and erasable PROMs (EPROMs).

Functional Testing - Functional testing is designed to ensure that the system and end-user requirements and specifications are achieved. Functional testing focuses on the results of processing rather than how processing is implemented. To accomplish this, create test cases to evaluate the functional correctness of the system and programs.

HSM - Hierarchical Storage Management - a group of software components that transparently manages files between magnetic disk or some other storage device.

Integration Testing - A test of a related group of program modules.

Interface - An exchange of information between one device and another or the device that makes such exchanges possible.

JCL - Job Control language, used by International Business Machines (IBM).

LRECL - Logical Record Length.

Mainframe Systems - Hardware and Software associated with centralized computer systems. Included are the following:

- Time Sharing Option (TSO)
- Customer Information Control Systems (CICS)
- Conversational Monitor System (CMS)

Media - Material on which data may be stored, such as magnetic tape, paper, or disks.

Modify - To change or alter.

MPT - Millennium Project Team

**Attachment 1**  
**DEFINITIONS AND ACRONYMS**  
(Page 3 of 5)

MS-DOS - Microsoft Disk Operating System

MSR - Management Staff Responsibility, individual who has overall responsibility for millennium compliance for a particular software application.

Operating System (OS) - Software that controls program execution, resource allocation, scheduling, scheduling, input/output control and data management.

Peripheral - A device controlled by the processor that is external to the Computer. Some peripheral devices include video display, disk drives, and printers.

Personal Computer (PC) - Hardware and Software associated with single-user Microprocessor-based computer.

Plant Process Computer - Any real-time sensor-based monitoring or control computer system that assists nuclear unit operation. Included are the following:

- Systems traditionally known as a "unit Plant Process Computer"
- Other plant process computers, such as special - purpose computers, mini-computers, microprocessor computers, programmable logic controllers, programmable logic devices, application specific integrated circuits, etc. based instrumentation monitoring and process control systems
- Station security computer system

Quality Software - Software whose output is used in Quality applications. Refer to DC 11, "Computer System Use and Control" for lists of Utility's Quality software. Quality applications, as a minimum, include:

- The design process associated with Category I structures, systems, or components.
- Support of Technical Specifications related to category I structures, systems, components, or design-basis analyses.
- Verification of compliance with Technical Specifications related to design basis analyses, when used as the sole or principle means of verification.
- Support of plant licensing with respect to Category I structures, systems, components, or design-basis analysis.
- Implementation of a safety function of a Category I system.
- Implementation of 10CFR50 Appendix B requirements.

**Attachment 1**  
**DEFINITIONS AND ACRONYMS**  
**(Page 4 of 5)**

Retired Software - Applications no longer in service (obsolete).

ROMBIOS - Read Only Memory Basic Input Output System - a collection of routines (usually stored in ROM) that control items such as the video display, disk drives, and keyboard.

Special Use Workstation - Desktop device, other than a PC, used for a single specific function. Examples include CAD and technical procedure publishing workstations.

Software - Sequence of instructions suitable for processing by a computer. Examples of software includes database applications, volatile electronic programs and non-volatile electronic programs, such as those stored in Programmable Read-Only Memories (PROMs), i.e. Firmware.

Software Document File - The file that provides or points to documentation and history of Quality Software.

Software Implementation Package - The name for the collection of all the required documentation specific to the installation of the new or modified software. The Software Implementation Package contains, as a minimum, all the documentation indicated as required on the implementation package check list. Some departments use the Software Document File itself as their Software Implementation Package. This is an acceptable substitution. For more information see DC-11.

Software Millennium Test - Test used to demonstrate compliance of software with millennium test cases developed using Attachment 3, "Software Millennium Test Development Guidelines."

Software Millennium Test Report - Document that contains results of Software Millennium Test.

Software Owner - employee responsible for specific software. For Quality Software, the individual must be qualified in accordance with NGP 2.26, "Departmental Training," for the purpose of preparation and performance of procedures, design packages, or validation and verification tests. The Software Owner may employ others to perform software-related tasks, but retains overall responsibility.

SMS - System Managed Storage - An environment that helps automate and centralize the management of storage. This is achieved through a combination of hardware, software, and policies.

**Attachment 1**  
**Definitions and Acronyms**  
(Page 5 of 5)

Stress Testing - A test to determine if the system can function when transaction volumes are larger than normally expected.

System Testing - A test of the integration and cohesiveness of the application.

Unit Testing - A test of a single program module.

Validation - Process that evaluates functional characteristics of Software, and certifies achievement of acceptable comparisons with Objective Evidence.

Validation Test - A test that assesses functionality of Software to the extent that Validation is accomplished.

Verification - Process that confirms that the performance of Quality Software is unchanged from that demonstrated by Validation, or that Database quality information is accurate.

Verification Test - Test that confirms the performance of Software is unchanged from that demonstrated by validation or test that confirms database quality information is correct.





**Attachment 3**  
**SOFTWARE MILLENNIUM TEST DEVELOPMENT GUIDELINES**

Software Title: \_\_\_\_\_ Revision No. \_\_\_\_\_

AR No. \_\_\_\_\_

Application (if different from Software Title): \_\_\_\_\_

Software Owner, Title, Phone #: \_\_\_\_\_

Prepared By, Title, Phone #: \_\_\_\_\_

During the process of testing, apply a combination of verification and validation techniques. These techniques include:

1. **Unit Testing**
  - 1.1. Testing the System Clock
  - 1.2. Input Testing
  - 1.3. Data Testing
2. **System Testing**
  - 2.1. Stress Testing
  - 2.2. Recovery Testing
  - 2.3. Regression Testing
  - 2.4. Error Handling Testing
  - 2.5. Manual Support Testing
  - 2.6. Parallel Testing
3. **Integration Testing**
  - 3.1. Intra- and Inter-System Testing
4. **PC Testing**
5. **Your Own Tests**

The following sections will cover some useful testing techniques and scenarios for Year 2000 testing. They are not meant to be all inclusive. Therefore, it is important that additional tests be tailored, as appropriate, for the application.

**Attention:** By nature, Year 2000 exposures are time-sensitive and time-driven. Be cautious before resetting the system timer. Some system resources and functions are time-sensitive and may be activated or de-activated when the system clock is reset. Such effects can occur when the system clock is either set forward or backward. Without careful planning, you could cause the loss of these system resources and/or functions, some of which might contaminate the production system or production data bases when running various test scenarios.

Test Applicable (☑ check if valid)		Compliant		Test	Test Applies to:	Comments
Yes	No	Yes	No			
				1. Expiration Test	Mainframe/Client Server	
				- User IDs		
				- Passwords		
				- Authorization/protection access		
				- Network access		
				- Automation functions		
				- SMS (System Managed Storage)/HSM (Hierarchical Storage Management) migrated data sets earlier than expected		
				2. Label driven tape datasets - are tapes expired earlier than expected? (i.e., validate label parameter expiration (99365, 99366))	Mainframe/Client Server	
				3. Archiving data expired earlier than expected?	Mainframe/Client Server	
				4. (12/31/1999 23:55 hrs) Monitor screen and transaction behavior	Mainframe/Client Server	

**Unit Testing**

Unit test is performed on one program at a time and is an exhaustive test of all logic within the program to demonstrate correctness and adherence to applicable specification and design requirements. Unit test should focus on exposing defects within the module logic (try to make it fail).

**Testing the System Clock** - This test involves resetting the system clock to identify problems which could occur (software, firmware, hardware, system access, etc.) when the century changes.

Unit Testing-Continued					
Test Applicable (☐ check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			- Validate that dates are calculated and displayed correctly (i.e., 1999 rolls into 2000, not 1900)		
			5. Validate End of Processing logic to see if dates will be incorrectly interpreted and/or used.	Mainframe/Client Server	

Input Testing - Apply requirements testing to verify that the system performs its function correctly and that it remains functional over a continuous period of time.					
Test Applicable (☐ check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			1. Will program respond correctly if "00" or "2000" is entered.	Mainframe/Client Server	
			2. Is a 4-digit year accepted or is it truncated?	Mainframe/Client Server	
			3. Ensure xx/xx/xx date =xx/xx/xxxx after expansion or conversion for all databases and tables.		

Test Applicable ( <i>for check if valid</i> )	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			1. Leap year - Ensure that year 2000 is processed as a leap year. - 1996/2/29 should pass (1996 is a leap year) - 2000/2/29 should pass (2000 is a leap year) - 2004/2/29 should pass (2004 is a leap year)	Mainframe/Client Server	
			2. Invalid Leap Year Test - 2/29/1999 non-leap year - 2/29/2001 for non-leap year	Mainframe/Client Server	
			3. Date Transaction Validation - (01/01/2000) Test processing for the first calendar day of the year - (01/31/2000) Test and validate processing for the last business and calendar day of the month	Mainframe/Client Server	
			4. Day-in-year calculation test - Does year 2000 have 366 days (not 365)?	Mainframe/Client Server	

Data Testing - Continued					
Test Applicable (or check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			5. Day-of-the-week calculation test	Mainframe/Client Server	
			- 02/28/2000 should be a Monday		
			- 03/01/2000 should be a Wednesday		
			- 01/03/2000 First business day of week		
			- 01/03/2000 First business day of month		
			- 01/03/2000 First business day of year		
			- 01/07/2000 Last business day of week		
			6. Week-of-the-year calculation test	Mainframe/Client Server	
			- The 11th week of the year 2000 is 3/5 to 3/11		
			7. End-of-Week Test	Mainframe/Client Server	
			- 01/08/2000 should be a Saturday		
			- 01/09/2000 should be a Sunday		

Data Testing - Continued					
Test Applicable (E) check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			8. Data Integrity	Mainframe/Client Server	
			- Are years 1800, 1900, 2000 distinguishable between one another?		
			- Validate for hard coded century occurrence of "19" and/or "20" in program code.		
			- Calculations - Look at programming logic to see if the usage of dates/date ranges in calculations will be correct		
			- Calculations - Check calculation when extends coverage into Year 2000 and verify future billing amounts are not impacted.		
			9. JCL/DCL CONTROL LANGUAGES	Mainframe/Client Server	
			- Ensure sorts use dates properly in processing		
			- Validate and test sort parameters		
			- Review sorts internal to programs		
			- Validate sort data sequence		
			- Record length adjusted - validate that increase records size are reflected in Record Length (LRECL - Logical REcord Length) field.		
			- Validate that Blocksize a multiple of LRECL		

Data Testing - Continued				Test	Test Applies to:	Comments
Test Applicable (if check is valid)	Compliant					
	Yes	No				
			10. Age Test		Mainframe/Client Server	
			- Use 12/31/1899 to verify age and date of birth calculations			
			- Validate processing for roll-over to 2001			
			11. Time-sensitive data (may not be applicable to some applications)		Mainframe/Client Server	
			a.) Use current system clock and test data with dates:			
			- Before 01/01/2000			
			- After 01/01/2000			
			b.) Set system clock to 12/31/1999 and test data with dates:			
			- Before 01/01/2000 (12/15/1999) validate transaction calculations are correct within 10, 15, and 30 day period			
			- After 01/01/2000 validate that everything behaves normally as 2000 approaches			



Data Testing - Continued			Test	Test Applies to:	Comments
Test Applicable (or check if valid)	Compliant				
	Yes	No			
			c.) Set system clock after 01/01/2000 and test data with dates. - Before 01/01/2000 validate backdated calculations are correct within 10, 15, and 30 day period) - After 01/01/2000 Test - Set system clock to (02/29/2000) validate backdated calculations are correct within 45, 60 and 90 day period - Set system clock to (03/31/2000) validate processing for the last business and calendar day of the quarter - Set system clock to (03/31/2000) validate processing for the last business and calendar day of the quarter		

Test Applicable (☑ check if valid)		Compliant		Test	Applies to:	Comments
		Yes	No			
<b>System Testing</b>						
System Testing ensures sufficient testing of a function's implementation and helps determine that all structures of the system are integrated to form a cohesive unit.						
<p><b>Stress Testing</b> - apply stress testing to determine if the system can function when transaction volumes are larger than normally expected. The typical areas that are stressed include disk space, transaction speeds, output generation, computer capacity, and interaction with people. When testing Year 2000 changes, it is essential to verify that the existing resources can handle the normal and abnormal volumes of transactions after the restructuring of the code and the possible expansion of the data fields. For example, apply stress tests to determine:</p>						
				1. Can environment sufficiently accommodate the additional disk space required to support 2 to 4 digit expansion (DASD)?	Mainframe/Client Server	
				2. Are additional CPU cycles required to support code conversion (i.e., 2 digit encoding/compression scheme) region size?	Mainframe/Client Server	
				3. Is response time adequate to support user turn around time?	Mainframe/Client Server	
				4. Do file definitions need to be reformatted (i.e., CI Spills, Data Dictionaries)?	Mainframe/Client Server	

**Recovery Testing** - Recovery Testing is used to ensure that the system can restart processing after losing system integrity. This is essential for systems in which the continuity of operation is critical to end users. Recovery processing normally involves the ability to go back to the last checkpoint, then reprocess up to the point of failure. Can system restart processing after losing system integrity?  
Any data integrity or unresolved exposures that lead to inconsistent data or code after you have implemented appropriate Year 2000 solutions will affect the completeness of backup data.

Test Applicable (if check is valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			1. Can application go back to the last check point then reprocess up to the point of failure?	Mainframe/Client Server	
			2. Is documentation complete to support the manual manipulation of data?	Mainframe/Client Server	
			3. Can the system handle unconverted data (bridging available)?	Mainframe/Client Server	
			4. Verify results when a date is entered in one format (e.g. yymmddccyyymmdd) and displayed in a different format (e.g. mmddyy/mmddccyy) (2-byte-MF...4-byte-C/S format). Test for Julian dates, especially for calculations and Job Schedule Calendar.	Mainframe/Client Server	

**Regression Testing** - Ensures that all aspects of a system remain functionally correct after changes have been made to a program in the system. Because the potential exists for a tremendous amount of data and programs to be involved in your Year 2000 transaction, any change to an existing program in the system can have a snowballing or cascading effect on other areas in the system. A change that introduces new data or parameters, or an incorrectly implemented change can cause a problem in previously tested parts of the system, simply because of the way data can be shared between software entities.

Test Applicable (☒ check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			1. Are user requirements followed (i.e., quality assurances)?	Mainframe/Client Server	
			2. Changes meet design specifications?	Mainframe/Client Server	
			3. Changes compliant with organization's policies and procedures?	Mainframe/Client Server	
			4. Validate data output records - data field following date field expansion.	Mainframe/Client Server	
			5. Validate data output records - data field in front of date field expansion.	Mainframe/Client Server	
			6. Validate on-line screen display field for error.	Mainframe/Client Server	
			7. Ensure all scheduling based on date return the same results before and after Y2K changes.	Mainframe/Client Server	
			8. Ensure conditions cover time zone differences.	Mainframe/Client Server	
			9. Ensure all extracting basedata returns the same results before and after Y2K changes.	Mainframe/Client Server	

Regression Testing - Continued				Test Applies to:	Comments
Test Applicable (☐ check if valid)	Compliant		Test		
	Yes	No			
			10. Ensure all index processing based on date returns the same results before and after Y2K changes.	Mainframe/Client Server	
			11. Ensure all subscripting based on e returns the same results before and after Y2K changes.	Mainframe/Client Server	

**Error Handling Testing** - Determines if the system can properly process incorrect transactions that can be reasonably expected as types of error conditions. Error-handling testing is necessary to determine the ability of the system to properly process incorrect transactions that can be reasonably expected as types of error conditions. For example, programs that accept only 4-digit year data entry format need to provide error messages for data entry in 2-digit year format, and vice versa for programs that accept only 2-digit year data entry format. When changing from 2-digit year format to 4-digit year format, you need to apply error-handling testing to verify the appropriate error-handling functions.

Error Handling Testing				Test Applies to:	Comments
Test Applicable (☐ check if valid)	Compliant		Test		
	Yes	No			
			1. Normal error handling for current 4 digit year data entry when 2 digit data entry occurs.	Mainframe/Client Server	
			2. Normal error handling for current 2 digit year data entry when 4 digit data entry occurs.	Mainframe/Client Server	

**Manual Support Testing** - Evaluate the process by which the end user handles new data generated from the automated applications with Year 2000 support. Types of data from these applications include data entry and report generation. Any new data format should be easy to understand and *not* ambiguous. This method includes testing the interfaces (for example screens, procedures, operation manuals, and online HELP panels) between end users and the application program. End users should be trained and use procedures provided by the system personnel. Testing should be conducted without any other assistance.

Test Applicable ( <i>check if valid</i> )	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			1. Are new field on on-line screens ambiguous?	Mainframe/Client Server	
			2. Operation manuals updated with new procedures?	Mainframe/Client Server	
			3. On-line HELP panels updated?	Mainframe/Client Server	

**Parallel Testing** - Determine whether the processing and results of an application's new program version are consistent with old program version. Parallel testing requires that the same input data be run through the two versions of the application. However, if the new application changes data formats, such as reformatting the year-date notation to 4-digit format, you must modify test input data before testing.

Test Applicable (if check is valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			1. Validation output report - Determine if data displays will be acceptable (compliant) in Year 2000 - Date fields - Non-date fields - Report headers - Report footers	Mainframe/Client Server	
			2. Validate on-line screens - Determine if data displays will be acceptable (compliant) in Year 2000 - Date fields - Non-date fields - Screen headers - Screen footers - On-line screen help	Mainframe/Client Server	
			3. Validate that hard-coded dates or century indicators are <i>not</i> located in output records.	Mainframe/Client Server	

Parallel Testing - Continued					
Test Applicable (or check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			
			4. Validate that hard-coded dates or century indicators are <i>not</i> located on output reports.	Mainframe/Client Server	
			5. Validate that hard-coded dates or century indicators are <i>not</i> located on screen displays.	Mainframe/Client Server	
			6. Validate output reports for zero suppression (i.e., year "00" would <i>not</i> display).	Mainframe/Client Server	
			7. Validate screen displays for zero suppression (i.e., year "00" would <i>not</i> display).	Mainframe/Client Server	
			8. Verify that the portion of the system that have <i>no</i> changes still runs properly as changes are made to other portions of the system.	Mainframe/Client Server	
			9. Verify that the program handles all its transactions correctly and remain stable for a defined period of time.	Mainframe/Client Server	
			10. Ensure that programs (or table subscripts) can handle date ranges that cross Millennium. - Some programs used dates as subscripts. (i.e., "00" for Year 2000 would be an invalid entry, September 1999 "999" may be considered as an end of file marker.)	Mainframe/Client Server	



<b>Integration Testing</b>				
<b>Intra- and Inter-System Testing</b> - Applications are frequently connected with other applications to provide a higher or deeper level of functionality. Data may be shared between applications or systems. Intersystem testing is required to ensure that the connection functions properly between the applications. This test determines that the proper parameters and data are correctly passed between applications, and proper coordination and timing of each function exists between applications.				
Test Applicable (if check is valid)	Compliant		Test Applies to:	Comments
	Yes	No		
			Mainframe/Client Server	
			Mainframe/Client Server	
			Mainframe/Client Server	



PC Testing - Continued		Test	Test Applies to:	Comments
Test Applicable (if check, if valid)	Compliant Yes No			
		3. Test time update by the operating system. a.) Update After Suspension of a time-sensitive program: - Set system clock to 12/31/1999, 23:58:00; suspend a time display program without a "wake up" timer; keep power on; wait until the clock reaches the year 2000; resume time display program; and check the date. b.) Update After Suspension and Wake Up of time-sensitive program: - Set system clock to 12/31/1999, 23:58:00; suspend a time display program with a "wake up" timer set at 01/01/2000, 00:01:00; keep power on; wait until the time display program "wakes up"; check the date.	PC	
		4. Leap Year Test a.) Change date 02/29/2000. If an error occurs, then BIOS is incorrect.	PC	
		5. Test CPU a.) Use different machines (286/386, etc.) when executing tests to ensure processing time isn't impacted.	PC	

Use This Section To Document Your Own Tests					
Test Applicable (or check if valid)	Compliant		Test	Test Applies to:	Comments
	Yes	No			

**NUCLEAR UTILITY YEAR 2000 READINESS**

**Appendix G**

**READINESS TRACKING PROCESS**









**NUCLEAR UTILITY YEAR 2000 READINESS**

**Appendix H**

**COMPLIANCE CHECKLIST**



**YEAR 2000 COMPLIANCE CHECKLIST**

This checklist helps application owners, application managers and the Year 2000 Program team evaluate Year 2000 compliance of an application. The checklist should be jointly reviewed and completed by both business subject matter experts and technical team members who are responsible for support of the application. Please answer all questions as thoroughly as possible. Include any documents that will help in the evaluation process, such as requirement definition, test plans, test results, etc. The answers will determine if an application is compliant.

After the Year 2000 Compliance Checklist has been completed, the application business unit owner, the application maintenance support, and the Year 2000 Program QA/QC Manager will review the checklist results. If the application is found to be Year 2000 compliant, sign-off by both the application business unit owner and the application maintenance support group will be required. If the application is found not to be in compliance, then the application business unit owner and the application maintenance support group will have two options:

1. have your application support group bring it into compliance
- or
2. turnover the application to the Year 2000 Program Team to bring the application into compliance.

If the option is to have the application support personnel bring the application into compliance, all Year 2000 Program standards must be followed. The Year 2000 Program Team must be included in the setting up of timelimes, deliverables, and certification process. If the option is to turnover the application to the Year 2000 Program Team for certification, the Year 2000 Program Team will take complete responsibility for bringing the application into compliance.

---

**1. Application Identification**

Please provide application information.

- A. Application Name \_\_\_\_\_
- B. Business Unit Owner of the Application \_\_\_\_\_
- C. Sponsoring Department of the Application (VP Org.) \_\_\_\_\_
- D. Application Subject Matter Expert Name \_\_\_\_\_
- E. Application Technical Expert Name \_\_\_\_\_
- F. Is the application in operation today? \_\_\_\_\_

Additional Comments: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**2. Year 2000 Dates**

Applications work with dates that are weeks, months, and years into the future, or may reference dates in the past. For example, inventory applications may need to process data that spans from 1950 to the present and need to keep its records for at least 50 years. Please verify your application's ability to successfully process data containing dates, with no adverse effect on the application's functionality and with no impact on the customer or end user. Can your application successfully process:

	VERIFIED	NO	N/A
a. Dates in 20th century (1900s)	_____	_____	_____
b. Dates in 21st century (2000s)	_____	_____	_____
c. Dates across century boundary (mix 1900s and 2000s)	_____	_____	_____
d. Crosses 1999 to 2000 successfully	_____	_____	_____

YES NO

Are test data sets available for regression testing on the next application release for any of the above?

\_\_\_\_\_

Are test results and reports available for review for any of the above?

\_\_\_\_\_

Additional Comments: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**3. Other/Indirect Date Usage**

Have you verified date handling process (and corrected if necessary):

	VERIFIED	NO	N/A
a. Dates embedded as parts of other fields	_____	_____	_____
b. Dates used as part of a sort key	_____	_____	_____
c. Usage of values in date fields for special purposes that are not dates (for example, using 9999, 0000, 99 or 00 to mean "never expire")	_____	_____	_____
d. Date dependent activation or deactivation of passwords, accounts, rates, etc.	_____	_____	_____
e. Date representation in the operating system's file system (creation dates and modification dates of files and directories)	_____	_____	_____
f. Date dependent utilities	_____	_____	_____
g. Date dependencies in encryption/decryption algorithms	_____	_____	_____
h. Date dependent random number generators	_____	_____	_____
i. Hardware and/or operating system does not reset the year to 1980 or 1984 on reboots after 31 December 1999 ( <i>corrections by operating system utilities allowed</i> )	_____	_____	_____

YES NO

Are test data sets available for regression testing on the next application release for any of the above? \_\_\_\_\_

Are test results and reports available for review for any of the above? \_\_\_\_\_

Additional Comments: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

---

**4. Internal Dates**

Dates and date fields must be clear and explicit within the applications which use them.

	VERIFIED	NO	N/A
a. Display of dates is clear and explicit (the ability to correctly determine to which century a date belongs either by explicit display, i.e. 4-digit year, or application or user inference, such as applications that only process and maintain year-to-date data)	_____	_____	_____
b. Printing of dates is clear and specific, such as dates in report headings	_____	_____	_____
c. Input of dates is clear and distinct to the application using them	_____	_____	_____
d. Storage of dates is clear to the application that uses them.	_____	_____	_____
e. Date compares and date manipulations within the application are processed correctly.	_____	_____	_____

YES      NO

Are test data sets available for regression testing on the next application release for any of the above?

\_\_\_\_\_

Are test results and reports available for review for any of the above?

\_\_\_\_\_

Additional Comments: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

---

**5. External Interfaces**

External interfaces are identified and validated to correctly function for all dates passed from your application.

	VERIFIED	NO	N/A
a. Verified that interfacing application functions the same when the data passed to that interface is generated from your application (for example, an interface is two-digit year and another is four-digit year).	_____	_____	_____
b. For each interface that exchanges date data, you and the responsible organization have discussed and verified that you have implemented consistent Year 2000 corrections that will correctly process date data passed between your applications.	_____	_____	_____

	YES	NO
Are test data sets available for regression testing on the next application release for any of the above?	_____	_____
Are test results and reports available for review for any of the above?	_____	_____

Additional Comments: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_



---

**6. Date Field Type**

Describe the type of date fields used by the application, in either application software or data bases.

- |  | VERIFIED | NO    | N/A   |
|--|----------|-------|-------|
| a. Does the application use two-digit year data fields?  | _____    | _____ | _____ |
| b. Does the application use four-digit year data fields? | _____    | _____ | _____ |
| d. When will the windowing logic fix fail?               | _____    |       |       |

- |   | YES   | NO    |
|---|-------|-------|
| e. If two-digit, does the application use a windowing logic technique to correctly infer the century? | _____ | _____ |
| If yes, what windowing date ranges does it use:   | _____ |       |
| From _____ To _____   |       |       |

- |   |       |       |
|---|-------|-------|
| f. Are there any internal data types for date? Such as character or variable character? | _____ | _____ |
| If yes, what is the range of dates that the date field can represent?                   | _____ |       |
| Minimum Date _____ Maximum Date _____   |       |       |

If character type date, what process does the application use to convert the date data?

\_\_\_\_\_

\_\_\_\_\_

- |   | YES   | NO    |
|---|-------|-------|
| Are test data sets available for regression testing on the next application release for any of the above? | _____ | _____ |
| Are test results and reports available for review for any of the above?                                   | _____ | _____ |

Additional Comments: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

---

**7. Vendor Provided Software**

Please provide the following information with regard to "Vendor Provided" software components.

YES NO N/A

- a. Does the application use vendor provided software packages or infrastructure components? \_\_\_\_\_

If yes, what is the software's name? \_\_\_\_\_

- b. Has the vendor provided software been verified to be year 2000 compliant? \_\_\_\_\_

- c. How was Year 2000 compliance determined? (certified by vendor or contractor, tested in-house, etc.) \_\_\_\_\_

Additional Comments: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

---

**8. Year 2000 Testing Information**

Please provide the following information with regard to testing the application for Year 2000 compliance:

- a. Testing Organization \_\_\_\_\_
  - b. Name of QA/QC Manager \_\_\_\_\_
  - c. Date that Year 2000 compliance testing was completed \_\_\_\_\_
  - d. How was Year 2000 compliance determined? (certified by vendor or contractor, tested in-house, inspected but not tested, etc.) \_\_\_\_\_
- YES    NO
- e. Do you follow a defined process for tracking the status of all Year 2000 problems reported, changes made, testing done, compliance verified, and applications returned to production? \_\_\_\_\_

Additional Comments: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

---

**9. Summary of Results**

Your application is Year 2000 compliant if any of the following statements are true. Please mark as appropriate.

- You completed a full independent testing of the application and you answered all the questions with a positive response (except for either 7a or 7b). \_\_\_\_\_
- An independent audit of your application was completed and you answered all questions with a positive response (except for either 7a or 7b). \_\_\_\_\_
- Your application was not tested or audited but, your application uses only **four-digit century** date fields and you answered all questions with a positive response except for 7a. \_\_\_\_\_

Your application is **NOT** Year 2000 compliant if any of the following statements are true. Please mark as appropriate.

- Your application was **not** tested or audited and, your application uses only two-digit century fields. You answered all questions with positive responses except for 7b. \_\_\_\_\_
- Your application was **not** tested or audited and, your application has ambiguous usage of dates. Questions 5-a,b,c or d (Internal Dates section) were answered with negative responses. \_\_\_\_\_
- Your application was **not** tested or audited and your application needs additional work before Year 2000 processing can be assured with any level of reliability. If any of the sets of questions, 2, 3, 4, 5, or 7b were answered with negative responses. \_\_\_\_\_
- Your application cannot be certified or has not yet been certified as compliant. \_\_\_\_\_

---

**9. Year 2000 Compliance Sign-off**

After review of application name, the undersigned certify that application name is Year 2000 Compliant. Attached is a listing of all certified programs associated with this application.

---

**Sign-off Information**

Business Application Owner (Manager)	Date
Application Support (Manager)	Date
Year 2000 QA/QC Manager	Date
Internal Auditor Manager	Date

Compliance Checklist

NEI/NUSMG 97-07  
October 1997

**Year 2000 Compliance  
Certification Checklist, Non-IS Supported**

Instructions: A checklist must be completed for each version of each application, equipment or system before it can be certified for continued production use. Fill out Section 1, and if the equipment or system is digitally-controlled or otherwise operates from firmware, fill out Section 2. When completed, return this checklist to the Y2K Coordinator.

The checklist will then be used to prioritize and schedule actual Y2k Compliance Testing per Section 3. This testing may be performed by the user, or by the NMIS Y2k Team. When Compliance Testing is completed, this checklist MUST be signed by the Key User Contact Supervisor or a representative of the NMIS Y2k Team and returned to the Y2K Coordinator.

This information will be reviewed by the Year 2000 QA Team and you will be notified when your application has completed the certification process. If you have any questions or comments, please add this information at the bottom of page 5.

**Section 1**

Site: \_\_\_\_\_ Dept/Wkgrp: \_\_\_\_\_

Application, Equipment or System Name: \_\_\_\_\_

Application Function: \_\_\_\_\_

Version: \_\_\_\_\_ Vendor: \_\_\_\_\_

# & Location(s) of Other Licensed Copies: \_\_\_\_\_

Hardware Platform: \_\_\_\_\_

Operating System/File Type: \_\_\_\_\_

Key User Contact: \_\_\_\_\_ Ext: \_\_\_\_\_

Key User Supervisor: \_\_\_\_\_ Ext: \_\_\_\_\_

Outline strategy for implementing compliance (i.e., warranty upgrade, purchase upgrade, migrate to different application, date roll-back, windowing, field expansion):

	Cat I			
	Cat II			
	Cat III			
For NMIS Use Only	Cat III	Cat II	Cat I	

Please check the appropriate response.

Yes No N/A

1. Is this Version of the application or system the current Production Version?

\_\_\_\_\_ Skip to Question 5.

Non-IS Supported Compliance Checklist

NEI/NUSMG 97-07  
October 1997

Please check the appropriate response.

Yes No N/A

2. Is the Software License for application or system renewed periodically?  
Specify Period and Vendor: \_\_\_\_\_

3. The application or system:  
Is, of itself, Nuclear Safety-Related or NSSS  
Provides Direct Control of Nuclear Safety-Related/NSSS Items  
Is Capable of Forcing Immediate or Near-immediate Plant Shutdown  
Is used for Nuclear Safety-Related Activities/Calculations  
Provides Automatic Control of Critical Plant Functions  
If Inoperative, Directly/Indirectly Leads to LCO's of 48 hrs or Less  
Is used to Protect the Health and Safety of the General Public

4. The application or system:  
Is used to Protect the Health and Safety of Plant Personnel  
Provides Control of Plant Habitability Systems  
If Inoperative, Directly/Indirectly Leads to LCO's > 48 hrs  
Is used for Control/Tracking of Other Critical Plant Information/Operations  
(Specify:)

5. The application or system:  
Provides Direct Control of Other Plant Systems  
Is used for Control/Tracking of Other Plant Information/Operations  
Is NOT the current Production Version

6. The application or system:  
Contains Date/time Stamped Data  
Is Used for long-term Averaging, Integrating, Trending, Scheduling, or Reporting

7. Is the Application or System Used for short-term Averaging, Integrating, Trending, Scheduling, or Reporting?

8. Is the Application or System Used for Time-Independent Calculations/Operations?

9. Does this Application or System interface with other applications?  
Specify Send or Receive and App/System: \_\_\_\_\_



Non-IS Supported Compliance Checklist

NEI/NUSMG 97-07  
October 1997

**Section 2** For every piece of equipment or system that is a PLC, digitally-controlled instrument or M&TE, or otherwise operates from Firmware, complete Section 2. Otherwise STOP, and return this checklist to the Y2K Coordinator.

Equipment or System Type: \_\_\_\_\_ MFR: \_\_\_\_\_

Equipment or System Serial #: \_\_\_\_\_

Model #: \_\_\_\_\_ Asset Tag #: \_\_\_\_\_

Detailed System Location: \_\_\_\_\_

CPU Mfr/Type: \_\_\_\_\_ Date Code: \_\_\_\_\_

# & Type of ROM/PROM/EPROM's: \_\_\_\_\_

Date Code(s): \_\_\_\_\_

Firmware Version Installed: \_\_\_\_\_ Firmware Vendor: \_\_\_\_\_

Vendor's Current Firmware Version: \_\_\_\_\_

Source Code Version: \_\_\_\_\_

Please check the appropriate response.

Yes No N/A

10. Does the Equipment or System have an EPN or EID number?  
Specify: \_\_\_\_\_

11. Is the Equipment or System Part of, Installed on, or Interface to a system having an EPN or EID number?  
Specify: \_\_\_\_\_

12. Is the Equipment or System under Warranty?

13. Does the Equipment or System have a Maintenance Contract?  
Specify Vendor: \_\_\_\_\_

14. Does the Equipment or System Operating History, Vendor Technical Manual, Restart Procedure, or Maintenance or Calibration Procedure indicate any form of Date Input or Date Check?  
Specify: \_\_\_\_\_

15. Does the Equipment or System Operating History, Vendor Technical Manual, or Maintenance or Calibration Procedure indicate that Batteries are used for Retention of Default or Setup Information?  
Specify: \_\_\_\_\_

Non-IS Supported Compliance Checklist

NEI/NUSMG 97-07  
October 1997

Please check the appropriate response.

Yes No N/A

16. Does the Equipment or System have a Data or an Event Historian?

17. Does the Equipment or System Perform Trending?

18. Does the Equipment or System Perform Time-dependent Calculations, such as Averaging or Integration?

19. Does the Equipment or System Print reports that include the date?

Describe the nature or use of the Historian, Trend, Calculation, or Report, including any Tech Spec, Regulatory, or Station Commitments that it is used to fulfill. \_\_\_\_\_

Section 3

Please check the appropriate response.

Yes No N/A

20. Does the application use four digits (YYYY) to represent the year?

If it does not, can the century be logically determined and dates correctly processed?

21. Does the application perform date duration calculations? This includes the following calculations:

- a) the duration between two dates
- b) the date based on starting date and duration
- c) the day of week, day within year, week within year

22. Will the application properly process decisions that require comparisons of dates from before and after the year 2000?

23. The application has been tested with the following date data and can successfully roll over to the next date:

- a) 09/09/1999 - could be set to mark end of file
- b) 12/31/1999 - ability to roll over to year 2000
- c) 01/01/2000 - Saturday (In 1900, this is a Monday)

Non-IS Supported Compliance Checklist

NEI/NUSMG 97-07  
October 1997

- d) 01/02/2000 - Sunday
- e) 01/03/2000 - Monday (The 1st workday of year)
- f) 02/28/2000 - 2000 is a leap year (Monday)
- g) 02/29/2000 - Tuesday (Leap Day)
- h) 03/01/2000 - Wednesday
- i) 04/01/2000 - Saturday
- j) 12/31/2000 - ability to roll over to year 2001
- k) 01/01/2001 - Monday, first day of year

- 24. The application can successfully convert between date representations (YYMMDD to Julian).
  
- 25. If date/time date is stored as an offset since a base date/time, the storage capacity has been checked so that it will work correctly through the 21 century.  
Indicate Storage Cap'y End Date \_\_\_\_\_
  
- 26. Does the application use special date values as logical flags? (for example, "99" to mean "no end date" or "00" to mean "does not apply")
  
- 27. Do reports print correctly? Specifically, reports do not contain any hard coded literals such as '19' for the century.
  
- 28. Do screens contain four digit years or can the correct century be inferred?  
NOTE: Screens should not contain any hard coded literals such as '19' for the century.
  
- 29. Will the application correctly sort by date when the dates are from both before and after the year 2000?
  
- 30. Has the key function or calculation been tested? Have the results been verified with the appropriate technical support group?

Testing Performed By: \_\_\_\_\_ Date: \_\_\_\_\_

Key User Supervisor Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Title: \_\_\_\_\_

Additional Comments:



---

NEI/NUSMG 98-07

**NUCLEAR UTILITY  
YEAR 2000 READINESS  
CONTINGENCY PLANNING**



**August 1998**

268

**NEI/NUSMG 98-07**

**Nuclear Energy Institute  
Nuclear Utilities Software Management Group**

**NUCLEAR UTILITY  
YEAR 2000 READINESS  
CONTINGENCY PLANNING**

**August 1998**

*Nuclear Energy Institute, 1776 I Street N.W., Suite 400, Washington D.C. 202.739.8000*

NEI/NUSMG 98-07  
August 1998

### **ACKNOWLEDGMENTS**

This document, *Nuclear Utility Year 2000 Readiness Contingency Planning*, NEI/NUSMG 98-07, was developed with the assistance of a task force of industry managers dealing with Year 2000 readiness issues. Timely development of this document was facilitated by use of the combined resources and expertise of the Nuclear Energy Institute and Nuclear Utilities Software Management Group. NEI and NUSMG wish to acknowledge the extensive efforts of the individuals who authored this document. Members of the industry's Contingency Planning Task Force include:

Terry Baxter	Union Electric
Doug Cremer	PECO Energy Company
James Davis	Nuclear Energy Institute
Wayne Glidden	Duquesne Light Company
Anne Houck	Duke Energy Corporation
Morgan Libby	Northeast Utilities
Don Lokker	Southern California Edison Company
Rich Lomax	Nebraska Public Power District
Bill Olsen	Nuclear Utilities Software Management Group
John Walderhaug	Southern California Edison Company

### **NOTICE**

Neither NEI, nor any of its employees, members, supporting organizations, contractors, or consultants make any warranty, expressed or implied, or assume any legal responsibility for the accuracy or completeness of, or assume any liability for damages resulting from any use of, any information apparatus, methods, or process disclosed in this report or that such may not infringe privately owned rights.

**EXECUTIVE SUMMARY**

Contingency planning for Year 2000-induced events has recently received a high level of attention from the government and in the press. A number of different, and often conflicting, approaches to contingency planning have been proposed. This document provides a focused approach to effective contingency planning that builds on the year 2000 readiness program nuclear utilities already have in place. Insights from ongoing industry readiness programs were extensively used in preparing this manual.

The primary goal of this document is preparation of an integrated contingency plan that allows the plant operating staff to mitigate any Y2K-induced events that might occur at key rollover dates. The principal date will be the rollover to January 1, 2000. Each facility will need to evaluate whether there are other dates of concern. The assessment and remediation program elements provide many of the insights needed to identify and quantify the Year 2000 rollover date risks at a facility.

The integrated contingency plan is developed from individual contingency plans developed for specific risks from internal and external sources, as well as remediation program insights. Internal risks can be assessed from the complexity of a digital system and its importance to plant operations. External risks have the added factor of supplier readiness and evaluating readiness programs that are not under the facility's control. The integrated plan provides a comprehensive perspective of risks to the facility and the resources and staff required to implement mitigation strategies.

This document also recommends that during the remediation phase, where there is a significant risk that remediation cannot be completed in the time available, that alternate remediation strategies be identified to ensure the facility can achieve Year 2000 readiness before a key rollover date.



NEI/NUSMG 98-07  
August 1998

**TABLE OF CONTENTS**

<b>Executive Summary .....</b>	<b>i</b>
<b>1 INTRODUCTION.....</b>	<b>1</b>
<b>2 PURPOSE AND SCOPE .....</b>	<b>1</b>
2.1 PURPOSE .....	1
2.2 SCOPE.....	1
<b>3 DEFINITIONS.....</b>	<b>2</b>
3.1 BUSINESS CONTINUITY.....	2
3.2 CONTINGENCY PLAN .....	2
3.3 CONTINGENCY PLAN MATRIX .....	2
3.4 INTEGRATED Y2K CONTINGENCY PLAN (ICP) .....	2
3.5 KEY ROLLOVER DATE.....	2
3.6 MITIGATION STRATEGY.....	3
3.7 REMEDIATION.....	3
3.8 RISK MANAGEMENT .....	3
3.9 Y2K COMPLIANT .....	3
3.10 Y2K-INDUCED EVENT.....	3
3.11 Y2K READY.....	3
<b>4 Y2K CONTINGENCY PLANNING MANAGEMENT .....</b>	<b>4</b>
4.1 CONTINGENCY PLAN COORDINATION .....	4
4.2 INDIVIDUAL CONTINGENCY PLANS.....	5

NEI/NUSMG 98-07  
August 1998

4.3	INTEGRATED CONTINGENCY PLAN.....	5
4.4	PROJECT REPORTS.....	5
<b>5</b>	<b>REMEDATION RISKS.....</b>	<b>6</b>
5.1	RISK IDENTIFICATION.....	6
5.2	ANALYSIS.....	6
5.3	RISK MANAGEMENT.....	6
5.4	VERIFICATION.....	7
<b>6</b>	<b>CONTINGENCY PLANNING FOR INTERNAL FACILITY RISKS.....</b>	<b>7</b>
6.1	RISK IDENTIFICATION.....	7
6.2	EVENT ANALYSIS.....	8
6.3	RISK MANAGEMENT.....	8
6.4	VERIFICATION.....	8
<b>7</b>	<b>CONTINGENCY PLANNING FOR EXTERNAL RISKS.....</b>	<b>9</b>
7.1	RISK IDENTIFICATION.....	9
7.2	EVENT ANALYSIS.....	10
7.3	RISK MANAGEMENT.....	10
	7.3.1 Risk Notification.....	10
	7.3.2 Mitigation Strategy Selection.....	11
7.4	VERIFICATION.....	11
<b>8</b>	<b>INTEGRATED Y2K CONTINGENCY PLAN.....</b>	<b>11</b>
8.1	INTEGRATED Y2K CONTINGENCY PLAN DEVELOPMENT.....	12
8.2	INTEGRATED Y2K CONTINGENCY PLAN CONTENT.....	12

**APPENDICES**

**A. PROGRAM INTEGRATION ..... A-1**

**B. EXAMPLES OF REMEDIATION RISK PLANNING ..... B-1**

**C. EXAMPLES OF INTERNAL CONTINGENCY PLANS ..... C-1**

**D. EXAMPLES OF EXTERNAL CONTINGENCY PLANS ..... D-1**

**E. INTEGRATED CONTINGENCY PLAN MATRIX ..... E-1**

**F. BOUNDARY ANALYSIS AND SUPPLY CHAIN READINESS ..... F-1**

## 1 INTRODUCTION

The nuclear utility industry has embarked on a program to identify and remediate Year 2000 (Y2K) problems that could affect facility operations. Despite these efforts, there is some risk of Y2K-induced events. *Nuclear Utility Year 2000 Readiness* (NEI/NUSMG 97-07), which provided a programmatic approach for identifying and addressing Y2K problems, recognized this risk and included a recommendation for contingency planning.

Effective contingency planning provides a process for reducing the risks associated with Y2K-induced events. This document provides an acceptable method for nuclear utility contingency planning by addressing contingency plan management, development and integration. It divides contingency plan elements into three categories based on the source of the risk:

- **Remediation Risks**—Remediation risks result from circumstances, such as component availability, that challenge the preferred remediation strategy.
- **Internal Facility Risks**—Internal facility risks are associated with facility digital systems that, although remediated, may be subject to a Y2K-induced event at key rollover dates.
- **External Risks**—External risks result from circumstances, conditions, or events that are not under the direct control of station management.

An integrated contingency plan should be developed from individual contingency plans to provide a comprehensive action plan to mitigate Y2K-induced events that could occur on key rollover dates.

## 2 PURPOSE AND SCOPE

### 2.1 PURPOSE

This document provides guidance for establishing a contingency planning process. It recommends management controls, preparation of individual contingency plans and development of an integrated contingency plan that allows the utility to manage the risks associated with Y2K-induced events.

### 2.2 SCOPE

This document addresses Y2K contingency planning as applied to nuclear generating stations and includes generating facility systems, resources and external influences. This document assumes that the facility already has an effective Y2K management program similar to that outlined in NEI/NUSMG 97-07. Contingency plans should support enterprise business continuity efforts. Appendix A provides an example of one way to integrate the various program elements.

NEI/NUSMG 98-07  
August 1998

### **3 DEFINITIONS**

The context of many of the terms used in discussing Year 2000 problems has shifted significantly over the past year. Different groups are using the same terms in discussing business continuity and contingency planning, but each group often applies significantly different meanings to key terms. In developing this document, the following definitions were used.

#### **3.1 BUSINESS CONTINUITY**

Business continuity is a high-level business strategy that provides senior management with an enterprise-wide overview of Year 2000 business risks and solutions. Business continuity is achieved through planning efforts that focus on reducing the risk of Y2K-induced business failures and addressing the organization's ability to provide the acceptable level of service in the event of Y2K-induced failure in internal or external systems.

#### **3.2 CONTINGENCY PLAN**

A contingency plan is a document that defines the necessary resources, actions and data for responding to the potential loss or degradation of a service or function due to a Y2K-induced event in a component or system. The objective of the contingency plan is to provide a pre-defined response to mitigate the effects and allow recovery from a Y2K-induced event in a system or component.

#### **3.3 CONTINGENCY PLAN MATRIX**

A contingency plan matrix is a document that identifies individual contingency plan actions, critical information, documentation, timing, key contact personnel and staffing requirements for inclusion in the integrated contingency plan.

#### **3.4 INTEGRATED Y2K CONTINGENCY PLAN (ICP)**

An integrated Y2K contingency plan is a document that includes essential elements from all contingency plans for the site or facility. Its purpose is to ensure the continuity of safe power production in the event of a Y2K-induced event. The integrated Y2K contingency plan is the final product of the contingency planning process.

#### **3.5 KEY ROLLOVER DATE**

A key rollover date is a date change on which digital systems may be susceptible to Y2K-induced events. These dates are identified from a facility detailed assessment. For example, December 31, 1999, to January 1, 2000, is a key rollover date.

February 28, 2000, to February 29, 2000, has also been identified as a key rollover date by some facilities.

**3.6 MITIGATION STRATEGY**

Mitigation strategy is a management process that results in documented instructions for reducing the effects of postulated or actual Y2K-induced events.

**3.7 REMEDIATION**

Remediation is the process of retiring, replacing or modifying software or devices that have been determined to be affected by the Y2K problem.

**3.8 RISK MANAGEMENT**

Risk management is an ongoing activity through which management: (1) identifies and tracks internal and external risks to the organization and outside parties resulting from Y2K-related problems, (2) assesses Y2K project and program effectiveness, and (3) develops contingency plans for mitigating the effect of potential Y2K-related failures.

**3.9 Y2K COMPLIANT**

Computer systems or applications that accurately process date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, the years 1999 and 2000, leap-year calculations and off-power on scenarios.

**3.10 Y2K-INDUCED EVENT**

A Y2K-induced event is a date-related problem that is experienced by a software system, software application, or digital device at a key rollover date at which time the system or device does not perform its intended function.

**3.11 Y2K READY**

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.

NEI/NUSMG 98-07  
August 1998

#### 4 Y2K CONTINGENCY PLANNING MANAGEMENT

The management of contingency planning requires coordination of a broad range of internal and external resources and interfaces. To meet this challenge, the Y2K project manager should consider contingency planning as an integral activity to the Y2K project plan that implements NEI/NUSMG 97-07. Because of the importance and complexity of this task, the project manager should consider assigning an individual as the single point of contact for the contingency planning process.

Contingency planning is a process that begins during the Y2K detailed assessment phase and continues throughout the program. The following are the recommended steps in the process:

- **Risk identification**—determines which items present a critical risk to the facility from Y2K-induced events.
- **Event analysis**—reviews identified risks, determines potential failure modes and consequences, and documents pertinent information.
- **Risk management**—uses information from event analysis to determine mitigation strategies. It should consider Y2K-induced events and their interdependencies.
- **Verification**—reviews the risk management results and provides confidence that the contingency plan will effectively mitigate the risk.

Contingency plans should be documented, reviewed and approved by management.

##### 4.1 CONTINGENCY PLAN COORDINATION

Y2K contingency plan coordination is a component of the facility Y2K project plan. Coordination activities ensure that each responsible organization develops individual contingency plans for identified risks. Recommended coordination activities include:

- contingency plan training
- assignment of appropriate resources
- development and coordination of individual contingency plans by responsible organizations
- tracking individual contingency plan status and progress
- assembling an integrated contingency plan
- reporting progress to the Y2K project sponsor



**4.2 INDIVIDUAL CONTINGENCY PLANS**

Individual contingency plans are prepared for items, systems or events. Plans should be identifiable and traceable to a risk. The following information should be included in individual contingency plans:

- inventory number or other unique identifier
- risk description
- subject matter expert identification
- event analysis
- period of vulnerability
- priority
- risk mitigation strategy and actions
- resources
- implementation timing and, if needed, an exit strategy
- training requirements
- any special Y2K procedures required
- identification and documentation of verification
- approval.

Individual contingency plans should be subject to appropriate elements of the facility Y2K readiness program such as quality assurance, management reviews and document retention. Individual contingency plans should be submitted to the Y2K project manager when completed.

**4.3 INTEGRATED CONTINGENCY PLAN**

The integrated contingency plan provides facility management with a comprehensive perspective of the risks associated with Y2K-induced events. The Y2K project manager should ensure a facility-specific integrated contingency plan is developed as described in Section 8 (see page 11).

**4.4 PROJECT REPORTS**

The Y2K project manager documents the progress of the contingency planning effort in status reports to the Y2K project sponsor and other appropriate management. Reports should include key performance indicators such as schedules, status, expenditures and any known issues with interfacing organizations, both internal and external.

NEI/NUSMG 98-07  
August 1998

## **5 REMEDIATION RISKS**

Each facility's Y2K project will remediate those systems within the project scope prior to Year 2000. However, remediation efforts for some systems may involve challenges to completion. Under these situations, it is prudent to develop alternate remediation strategies as a contingency. These strategies are within the scope of the NEI/NUSMG 97-07 remediation process. This section provides a method that can be used to evaluate these remediation challenges and determine whether development of alternate strategies is appropriate. Examples are provided in Appendix B.

### **5.1 RISK IDENTIFICATION**

Remediation efforts may be challenged by a number of factors, including:

- availability of replacement components
- concern over vendor support
- scarcity of resources.

The Y2K project should identify those systems whose remediation strategies are subject to risk. These strategies will undergo further risk analysis.

### **5.2 ANALYSIS**

Analysis is performed to understand the nature of the challenges to the selected remediation strategy. Alternative remediation strategies should be evaluated to determine their suitability and any further risks that their selection might introduce. For example, if replacement is the selected remediation strategy, the risk of late delivery should be considered. If the alternative remediation strategy is date rollback, then any risk posed by this alternative should also be evaluated.

Key performance indicators (KPIs) may be used to provide a mechanism for monitoring the progress of the remediation effort. In some cases this may be as simple as the component delivery date.

### **5.3 RISK MANAGEMENT**

Using the results of the analysis phase, management should identify an alternate remediation strategy. Using the selected KPIs, management should select criteria for initiating the alternate remediation strategy. Schedule constraints and system complexity will be key factors in establishing the initiation date.

**5.4 VERIFICATION**

The selected risk management strategy should be verified. This process ensures that the strategy is capable of achieving the intended purpose, can be accomplished in the time available and identifies personnel necessary to execute it.

**6 CONTINGENCY PLANNING FOR INTERNAL FACILITY RISKS**

The inventory, assessment and remediation phases of the Y2K project are designed to provide identification and remediation for items that could degrade, impair or prevent operability of the nuclear facility. However, there remains some risk that digital systems could still be subject to a Y2K-induced event that affects facility operations. The purpose of internal risk contingency planning is to provide a logical approach to anticipate and prepare for such events and reduce their impact on facility operations.

An example of an internal facility risk is a control system that relies upon process computer signals, embedded devices, and complex interfaces to other systems. These relationships become evident in the inventory and assessment process. Based on the importance of this system and its complexities, management may elect to develop an individual contingency plan for it. Contingency plans should identify failure modes and mitigation strategies. See Appendix C for samples.

Y2K contingency planning should also consider the potential that the problem results in a common cause failure that could potentially affect many systems or components, including essential infrastructure services.

**6.1 RISK IDENTIFICATION**

Risk identification for internal facility events includes a review of the Y2K inventory and assessment results for devices and software. The risk is a function of the short-term challenge to continued facility operation, the complexity of the system and the degree of remediation that may have been required. The following are examples of factors to consider:

- systems or components whose failure places the unit at short-term risk for continued operation
- systems with multiple, integrated digital control devices or software subsystems
- systems that use digital input from other systems
- systems for which significant remediation effort was required

NEI/NUSMG 98-07  
August 1998

## 6.2 EVENT ANALYSIS

Event analysis is used to determine failure modes and their consequences. Analytical processes may include review of existing safety analyses and probability risk assessments (PRA). Simulations and experience-based judgments may be used to understand the implications of failure modes. For each event consider the following:

- consequence of the event on safety or operability, including safe shutdown operations
- likelihood of the occurrence of the event
- importance to the objectives of the facility
- when event consequences occur—immediate, delayed with a known or unknown time-to-occurrence
- long-term effect of the event.

## 6.3 RISK MANAGEMENT

Risk Management uses the information from event analysis to determine the mitigation strategies that will reduce the effect of a Y2K-induced event. It may consider Y2K interdependencies. For internal facility risks, risk mitigation requires a wide range of technical and operations skills. Mitigation strategies to consider include:

- augmented staff
- implementing manual control
- placing backup or standby systems in service
- developing special procedures
- establishing specific training requirements
- monitoring systems to ensure proper operation following a key rollover date.

The facility should leverage existing procedures and practices when developing mitigation strategies.

## 6.4 VERIFICATION

Individual contingency plans should be verified. This process provides confidence that the strategy selected is capable of achieving the intended purpose, can be accomplished coincident with other strategies and includes personnel who are able to execute it. The methods that may be used for this evaluation include management assessments, independent reviews, and peer evaluations.

**7 CONTINGENCY PLANNING FOR EXTERNAL RISKS**

External risks result from circumstances, conditions, or events that are not under the direct control of facility management. The purpose of external risk contingency planning is to provide an awareness of such risks and the means for mitigation. Examples in this area are provided in Appendix D.

**7.1 RISK IDENTIFICATION**

Risk identification considers how external Y2K events could compromise the safety or continued operation of the facility due to Y2K-induced events. One technique that may be used is boundary analysis.

Boundary analysis postulates a boundary surrounding the facility. Items, signals, information, or data that cross the boundary are candidates for investigation. Examples include transmission lines, communications, consumables and services. This technique may result in a detailed examination of facility supply chains for a limited number of critical services and consumables for vulnerability to disruption by a Y2K-induced event. Particular attention should be given to facility services or equipment that are jointly administered, either in concert with the facility or by more than one external supplier. Further discussion is provided in Appendix F.

There are many documents and existing contingency activities that may be used to identify external events that may be of concern to the Y2K project. Examples include existing plans such as those for:

- disaster recovery
- resumption of business
- station blackout
- grid restoration
- emergency preparedness
- storm restoration.

The following list includes external events that a facility should consider for contingency planning:

- **transmission/distribution system events**—loss of off-site power, grid instability and voltage fluctuation, load fluctuations and loss of grid control systems
- **loss of ultimate heat sink**—river water level control
- **depletion of consumables**—bottled gasses, hydrogen, carbon dioxide, nitrogen, diesel fuel and demineralizer resins

NEI/NUSMG 98-07  
August 1998

- **loss of essential services**—telephones, microwave, domestic water, satellite, networks, select vendors, security, police and fire fighting
- **loss of emergency plan equipment and services**—pagers, radios, sirens and meteorology.

## 7.2 EVENT ANALYSIS

The purpose of external event analysis is to understand and evaluate the implications of external events to the facility. For each event, the responsible organization should consider the following:

- consequence of the event on safety or operability, including at-power or safe shutdown conditions
- likelihood of occurrence of the event
- potential for an event inducing other events, or changing the probability of their occurrence
- when event consequences occur—immediate, delayed with a known or unknown time-to-occurrence
- priority for resumption of the service
- long-term effect of the event.

Events should be investigated with consideration of the effect that complex supply or support chains may have on the mitigation strategy. A supplier may have a reliance on another supplier or service that is subject to Y2K-induced events. A chain of failures in a complex supply chain may compromise more than is readily apparent by looking only at the final source.

## 7.3 RISK MANAGEMENT

Risk management uses the information from event analysis to determine the mitigation strategies that will reduce the effect of a Y2K-induced event. It ensures that the risks posed by external Y2K-induced events are identified and are reduced to an acceptable level. Risk management may mitigate the risk or may extend the period of facility service pending resumption of the service or subsidence of the event. This management function requires input from business and technical specialists. The two phases of risk management are risk notification and selection of mitigation strategy.

### 7.3.1 Risk Notification

For external events, it is important to communicate to the responsible external organization the risk significance of an event to the facility. The external organization may be requested to provide a description of its Y2K project elements that address the event. The facility Y2K project should consider this

information in determining the mitigation strategy. The evaluation should consider the potential for the external organization's Y2K remediation or contingency planning to be successful as a mitigation strategy.

### 7.3.2 Mitigation Strategy Selection

More than one mitigation strategy may be appropriate and employed for an event. Some mitigation strategies that may be appropriate for consideration are:

- **facility alignment**—Preset facility load or capacity to reduce the consequences to the facility of grid instability or voltage fluctuations. High-risk evaluations, such as reduced reactor coolant inventory operations or emergency diesel generator planned maintenance, should be scheduled to avoid Y2K key rollover dates, when possible.
- **minimized dependency**—Stockpile consumables to support continued facility operation.
- **an alternate source**—Most consumables are available from multiple sources.
- **an alternate process**—Some services such as telecommunications may be accomplished using alternate methods. For example, portable radios may be used to compensate for the loss of phone service.
- **rapid resumption of service**—Where a proactive mitigation strategy is unobtainable or impractical, the management team may adopt rapid resumption of service as the recovery strategy. An example might be a system that will be interrupted by the Y2K-induced event but is easily restarted with support of the external organization.

### 7.4 VERIFICATION

The risk management strategy should be verified. This process provides confidence that the strategy selected is capable of achieving the intended purpose, can be accomplished coincident with other strategies and includes personnel who are able to execute it. Methods that can be used for this evaluation may include management assessments, independent reviews, peer evaluations, external organization reviews, walk-throughs, drills or simulations.

## 8 INTEGRATED Y2K CONTINGENCY PLAN

The integrated Y2K contingency plan is a compilation of individual Y2K contingency plans and includes any remediation actions planned during key rollover dates. It is a comprehensive document that will be used to manage the resources required to support the facility leading up to and during key rollover dates.

NEI/NUSMG 98-07  
August 1998

Using this information, facility management determines the resources required to properly staff for key rollover dates. Inputs required for development of the integrated plan include:

- organizational sponsorship and key contacts
- identification of required internal and external organizational support
- coordination with internal and external interfaces
- identification of conflicts among individual contingency plans
- identification of resources necessary to implement individual contingency plans.

#### 8.1 INTEGRATED Y2K CONTINGENCY PLAN DEVELOPMENT

The Y2K project manager is responsible for the development of the integrated Y2K contingency plan. As individual contingency plans are developed, staffing requirements and actions are extracted and documented in the integrated contingency plan matrix. This matrix is then used to determine the overall resource requirements for the facility. This process begins during the assessment phase and continues throughout the Y2K program. A sample matrix is provided in Appendix E.

The final integrated Y2K contingency plan should be reviewed and approved by management.

#### 8.2 INTEGRATED Y2K CONTINGENCY PLAN CONTENT

The integrated Y2K contingency plan should include the following topics:

**purpose and scope**—includes the purpose and reasons for integrating the resources for a facility-wide approach to mitigate Y2K-induced events. The scope establishes the boundaries for the plan.

**integrated contingency plan matrix**—provides the relationship between the individual contingency plans.

**responsibilities**—assigns responsibility for managing the implementation of the integrated contingency plan. This may include the following key responsibilities:

- integrated Y2K contingency plan coordinator—assembles teams and manages the implementation of the plan
- implementation teams—identifies personnel designated to carry out actions specified in individual contingency plans



- **advisory teams**—identifies personnel familiar with the technical content and details associated with mitigation strategies

**resource scheduling**—the plan coordinates timing and resources necessary for implementation of the elements of the ICP. This includes coordination between departments, groups and outside agencies. Plans should specify items such as facilities, communications, status tracking and infrastructure support.

**event response coordination**—identifies the key decision-making processes for responding to Y2K-induced events as they occur.

**integrated action plan**—summarizes the actions associated with the restoration of facility systems, components, and equipment affected by Y2K-induced events.

**integrated Y2K contingency plan training and awareness**—identifies any specific Y2K-related training requirements. General facility awareness training on Y2K critical dates and associated contingencies should also be considered.

**APPENDIX A****Program Integration**

Contingency planning needs to be integrated with the other elements of the facility's overall Year 2000 readiness program. This appendix provides one way that these elements can be integrated to support the overall objective of reducing risk from Year 2000 problems.

NEI/NUSMG 97-07 *Nuclear Utility Y2K Readiness* provides guidance on managing the Y2K project, identifying contingency planning as one of management planning. Figure A-1 shows the relationship of contingency planning to the overall Y2K project.

As the figure shows, deliverables of the Y2K program assessment and remediation phases support developing Y2K contingency plans for the critical systems, devices and applications. This process involves the development of alternate remediation plans and contingency plans. Existing contingency plans may be used or augmented with Y2K event considerations.

Individual Y2K contingency plans are incorporated into an integrated contingency plan, which provides a comprehensive document to be used to manage risks at key rollover dates. The integrated contingency plan should support any enterprise level business continuity planning efforts.

Integration of the contingency planning effort into the overall Y2K readiness program time line is also important. Figure A-2 illustrates the overall time line for one facility. The timeline shows the relations of individual phases of the Y2K project. In this case, the project started in the fourth quarter of 1997. The relationship of one phase to another, not the absolute schedule, is what is important. For any given facility, actual time planned for each phase will depend on variables such as the number of operating units, available personnel and number of digital systems.

Development of the integrated Y2K contingency plan depends on completion of individual contingency plans for the identified risk categories. Contingency plan development for Y2K remediation activities and internal risks may be performed throughout the assessment and remediation phases of the Y2K project. This process is described in Sections 5 and 6. Assessing external risks as described in Section 7 involves cooperation of organizations outside of the control of the facility.

NEI/NUSMG 98-07  
August 1998

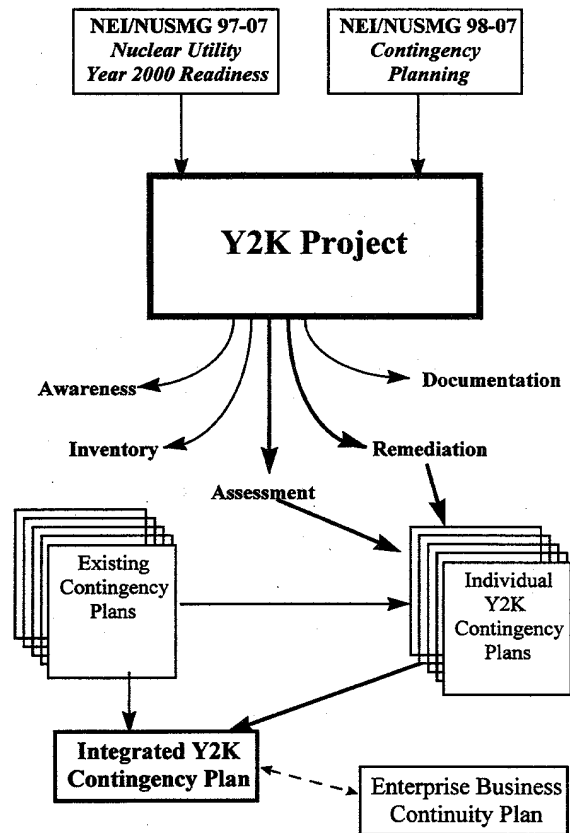


Figure A-1: Program Integration

NEI/USMC 98-07  
August 1998

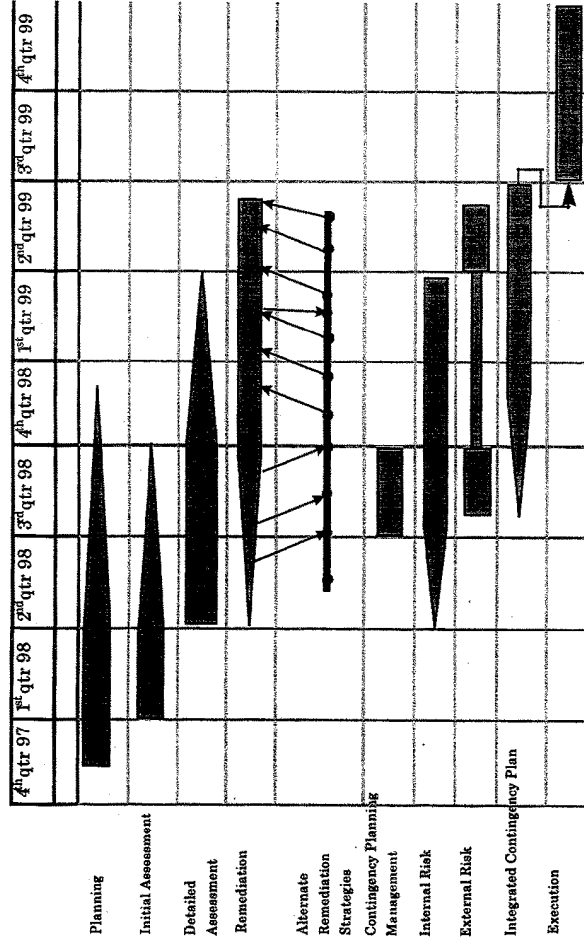


Figure A-2: Typical Year 2000 Project Time Line

NEI/NUSMG 98-07  
August 1998

A-4

**APPENDIX B****Examples of Remediation Risk Planning**

The information in this appendix illustrates the types of remediation risks, described in Section 5, to which planned Y2K remediation efforts may be exposed. These sample contingency plans demonstrate remediation risks from vendor concerns, resource limitations and scheduling difficulties. As for all of the sample contingency plans in these appendices, these plans are written for illustration purposes only to demonstrate the contingency planning process in different scenarios.

The first example, identified as B-1, demonstrates an alternative remediation plan based on a concern that a vendor may not successfully deliver and implement the primary remediation solution. The strategy recommended in this situation is to set the system clock back 28 years.

The second example, identified as B-18, demonstrates a situation where an enterprise-wide solution will ultimately replace a plant application that contains a Y2K weakness. In this case, the alternate remediation is to fix the software if the enterprise-wide solution does not meet the implementation schedule, even though the plant application will ultimately be replaced.

The third example, identified as B-179, documents a Y2K weakness with a database, where reports do not correctly render the four-digit year, even though all calculations and values are correct. This example represents a cosmetic problem only, therefore the accept-as-is alternate remediation option is specified.

B-1



NEI/NUSMG 98-07		<b>Year 2000 Contingency Plan</b>	
Plan No.:	Item/Component/System:	Priority	
B-18	Work Management and Maintenance Scheduling	3B	
<b>Risk Description:</b> The primary remediation strategy is the installation of an enterprise-wide work management system. The new system will replace a plant system that is currently maintained by plant computer personnel. Because of the broad scope of this project and the resources required, there is a concern that the target date of 12/31/1998 will not be met.			
<b>Risk Analysis Summary:</b> The present application will not schedule work and maintenance items past 1/1/2000. Some of these work items are required one year in advance and are used in support of technical specifications. Manual scheduling of these items is not feasible. An alternative to the primary remediation strategy is required.			
<b>Risk Mitigation Strategy:</b> The alternate remediation strategy is to correct the software problems in the current work management system. It is <u>crucial</u> that this work be completed by the end of 1998 so that year 2000 work items can be generated beginning in 1999. Because of this critical timing issue, the alternate remediation may have to be started before the status of the enterprise-wide solution is known.			
<b>Implementation:</b>  <b>Period of Vulnerability:</b> 1/1/1999 until acceptance of enterprise-wide application <b>Implementation Timing:</b> Must begin by 10/1/1998 to complete by 12/31/1998. <b>Resource Requirement:</b> 4.5 man months application design, coding, implementation. 1 man month for administrative support. <b>Subject Matter Expert:</b> J. L. Programmer <b>Training Required:</b> N/A <b>Completed:</b> _____ <b>Exit Strategy:</b> N/A			
<b>Verification &amp; Approval:</b> Verify operability of existing system by testing of added features and by an integration surveillance test using approved procedures.			
<b>Verified By:</b> _____		<b>Date:</b> _____	
<b>Approved By:</b> _____		<b>Date:</b> _____	



NEI/NUSMG 98-07  
August 1998

NEI/NUSMG 98-07		<i>Year 2000 Contingency Plan</i>	
Plan No.:	Item/Component/System:	Priority	
B-179	HR Database(xxx)	6	
<b>Risk Description:</b> Certain reports from the human resources database do not correctly display dates beyond 1999. Project XYZ has been initiated to correct this problem but, because of low priority, may not be completed by 1/1/2000.			
<b>Risk Analysis Summary:</b> The human resources applications provide reports to the fitness for duty and security access systems. Tests have shown that reports with dates beyond 1/1/2000 show up as "*****". The only problem is in the reports. All stored and calculated data is correct.			
<b>Risk Mitigation Strategy:</b> The problem is cosmetic. The alternate remediation is to accept as is.			
<b>Implementation:</b>  Period of Vulnerability: N/A Implementation Timing: N/A Resource Requirement: N/A Subject Matter Expert: H. R. Manager Training Required: N/A Exit Strategy: N/A Completed: _____			
<b>Verification &amp; Approval:</b> Verification is N/A.			
Verified By: _____		Date: _____	
Approved By: _____		Date: _____	

**APPENDIX C****Examples of Internal Contingency Plans**

The information provided in this appendix illustrates the types of risks that Y2K events may pose to systems under the control of the facility even after remediation has been accomplished. These were discussed in Chapter 6 of the basic document. Each example is followed by the related Year 2000 contingency planning form.

**Example 1: Contingency Plan for the Facility Computer Network**

**Risk Identification** - The information technology (IT) computer network and server farm is a system with multiple digital control devices and software subsystems that do not furnish diversity and cannot be operated manually. This system also uses digital input from other systems to perform its intended functions.

While this system has been individually evaluated, it has many complex interfaces and an enormous number of possible interactions and conditions that exist with any given transaction. A single failure in one of the components has the potential for impacting the entire data communications structure and therefore should receive additional attention in the form of contingency planning.

**Event Analysis** - Although each component and application has been assessed and no Y2K weaknesses were identified, the large number of interactions described above are of concern. Therefore, IT will augment staffing during the critical time periods to immediately respond to any abnormal conditions. The abnormal conditions could include hardware and/or software, so the augmented staff must include both programmers and technical support personnel.

**Risk Management** - The contingency plan for a Y2K event in the IT system includes the following mitigation strategies:

- Mitigation strategy from IT for potential failure of computer component(s). (IT will provide augmented staffing for the critical dates of 12/31/99 – 1/1/2000 and 2/28/2000 – 2/29/2000.)
- Each department has evaluated the impact and has developed mitigation strategies in the event of the loss of data communications capabilities. Those currently identified include:
  - Operations has developed a methodology to provide worker protection assurances (WPA) manually.
  - Maintenance has developed a mitigation strategy to obtain replacement parts manually.

NEI/NUSMG 98-07  
August 1998

- Stores has developed a mitigation strategy to access and distribute replacement parts manually.
- Emergency Preparedness has identified a mitigation strategy which is an alternate method for computer based notification and call out of personnel.
- Health Physics Operations will utilize manual methods for RCA entry as per existing procedure.
- Health Physics Technical Support's mitigation strategy is to use alternate radiation spectroscopy methods.

Each department has provided appropriate mitigation strategies for Y2K-induced events.

**Verification** - Examples of contingency plan verification of a few of the potentially impacted departments include:

**Operations** - The IT department has planned a computer outage for the platform on which the WPA application is located. Operations has developed a manual process to implement and track WPA. They will conduct a test of the process prior to the planned computer outage and implement during the outage to verify operability of the process.

**Emergency Preparedness (EP)** - EP will pre-stage emergency personnel, as listed on the attached list, for the key rollover dates as a contingency for this and other potential Y2K-induced events. As this does not require any new processes, no additional verification is required.

**Health Physics Operations (HPOPS)** - HPOPS has an existing procedure to manually control access to the RCA and track personnel dose. This procedure is a part of the training curriculum and has been successfully used by the current technical staff. Since implementation of this procedure has successfully been completed, no further verification is necessary.

NEI/NUSMG 98-07		<b>Year 2000 Contingency Plan</b>	
<b>Plan No.:</b> EX-01	<b>Item/Component/System:</b> Facility Local Area Network File Server System		<b>Priority:</b> HIGH
<b>Risk Description:</b> Possible loss of network communications and network based software applications.			
<b>Risk Analysis Summary:</b> Individual network components have been assessed and determined to be Y2K ready; however, integrated testing could not simulate all possible combinations of software interaction. Any network anomalies are likely to manifest shortly after Y2K rollover. Restoration of the network may require software and hardware expertise.			
<b>Risk Mitigation Strategy:</b> Augment IT staffing on Y2K rollover dates with network engineer and network hardware technician to perform restart of network servers, routers, and software applications as necessary. Perform full network backup on 12/31/1999.			
<ul style="list-style-type: none"> <li>• Mitigation strategy from IT for potential failure of computer component(s). (IT will provide augmented staffing for the critical dates of 12/31/99 – 1/1/2000 and 2/28/2000 – 2/29/2000.)</li> <li>• Each department has evaluated the effect and has developed mitigation strategies in the event of the loss of data communications capabilities. Those currently identified include: <ul style="list-style-type: none"> <li>• Operations has developed a mitigation strategy to provide worker protection assurances (WPA) manually.</li> <li>• Maintenance has developed a mitigation strategy to obtain replacement parts manually.</li> <li>• Stores mitigation strategy is to access and distribute replacement parts manually.</li> <li>• Emergency Preparedness mitigation strategy is an alternate method for computer based notification and call out of personnel.</li> <li>• Health Physics Operations will use manual methods for RCA entry as per existing procedure.</li> <li>• Health Physics Technical Support will use alternate radiation spectroscopy methods.</li> </ul> </li> </ul>			
Each department has provided appropriate mitigation strategies for the potential Y2-induced events.			

NEI/NUSMG 98-07  
August 1998

<b>Plan No.:</b> EX-01	<b>Item/Component/System:</b> Facility Local Area Network File Server System	<b>Page</b> 2
<b>Implementation:</b> Periods of Vulnerability: <u>12/31/1999 – 01/01/2000, 2/28/2000 – 2/29/2000</u> Implementation Timing: <u>Swing shift 12/31/1999, swing shift 2/28/2000</u> Resource Requirements: <u>One network engineer, one network hardware technician</u> Subject Matter Expert: <u>S. T. Trainer</u> Training Required: <u>None</u> Completed: _____ Exit Strategy: <u>The exit strategy is to discontinue manual methods when automated system is restored and verified. The use of alternate methods will be discontinued when primary methods are restored and verified.</u>		
<b>Verification &amp; Approval:</b> Adequate implementation of manual methods will be verified by supervisory oversight. Alternate methods usage will be verified by performing a calibration procedure. Verified By: _____ Date: _____ Approved By: _____ Date: _____		

**Example 2: Contingency Plan for Condensate Polisher System**

**Risk Identification** - The full flow condensate polisher (FFCP) system provides chemical conditioning of the condensate water while on line to enhance steam generator water chemistry control. The FFCP has a large number of integrated programmable logic controllers (PLC) and a known Y2K deficiency involving PLC halts when system time rolled over from 12/31/99 to 01/01/00. Remediation was accomplished with a firmware upgrade from the vendor for the PLC. Individual components were tested and validated for Y2K readiness.

**Event Analysis** - Failure of the FFCP system could cause transients in steam generator water level with possible reactor protective system activation and safety system activation if steam generator level control is lost. Extended loss of the FFCP will result in degraded steam generator water chemistry conditions.

If any Y2K-induced event were to occur, the control room annunciator alarm "FFCP TROUBLE" would be received indicating an abnormal operating condition. Automatic operation of the condensate polisher would halt with control valves failing "as-is." Numerous process alarms would be received on the local control panel.

**Risk Management** - Several strategies will be used in the contingency plan to mitigate any unforeseen Y2K-induced event.

- Neutralize and discharge all FFCP sumps on 12/31/99 to ensure maximum sump capacity. Regenerate cation resin in the week prior to Y2K rollover.
- Operate FFCP in passive cleanup mode during Y2K rollover (no resin regeneration or sump neutralization operation).
- Post an additional operator to assist in restoring or bypassing FFCP.
- Train control room staff and FFCP operators in probable failure modes and alarms indicating Y2K-induced failure.
- Perform walkdown of FFCP following Y2K rollover to verify proper operation.

Implementation dates for contingency plan are:

- 12/25/99 - Perform feed and condensate water conditioning per operating procedure XXXXX. Secure clean-up when feed and condensate conductivity is XXXX :mhos.
- 12/29/99 - Regenerate cation resin per operating procedure XXXXX.
- 12/30/99 - Perform acid neutralization of FFCD neutralization sump and discharge water to the outfall per operating procedure XXXX.
- 12/31/99 - Station additional operator at FFCD control station on swing shift.
- 01/01/00 - Verify proper system operation by performing walkdown of system using special operating procedure XXXX.

**Verification** - All of the planned evolutions are currently part of plant procedures. Since no new process or procedure is required, no further verification is required.

NEI/NUSMG 98-07  
August 1998

NEI/NUSMG 98-07		<b>Year 2000 Contingency Plan</b>	
<b>Plan No.:</b> EX-02	<b>Item/Component/System:</b> Full Flow Condensate Polisher System		<b>Priority:</b> MEDIUM
<b>Risk Description:</b> Full flow condensate polisher system (FFCP) may experience Y2K related failure due to complex interaction of multiple programmable logic controllers in the FFCP automated control system.			
<b>Risk Analysis Summary:</b> Failure of the FFCP may cause steam generator level transients due to flow perturbations in the feed and condensate system. Extended loss of the FFCP will result in degraded steam generator water chemistry conditions. Indications of FFCP failure will be "FFCP TROUBLE" annunciator in the main control room. Numerous process control alarms will be received on the local control panel.			
<b>Risk Mitigation Strategy:</b> Neutralize and discharge all FFCP sumps on 12/31/99 to ensure maximum sump capacity in event of a process upset. Regenerate cation resin in the week prior to Y2K rollover. Operate FFCP in passive cleanup mode during Y2K rollover (no resin regeneration or sump neutralization operation). Post additional operators to assist in restoring or bypassing FFCP in event of Y2K failure. Train control room staff and FFCP operators in probable failure modes and alarms indicating Y2K related failure. Perform walkdown of FFCP following Y2K rollover to verify proper operation of control systems.			
Trigger dates for implementation			
12/25/99 - Perform feed and condensate water conditioning per operating procedure XXXXX. Secure clean-up when feed and condensate conductivity is XXX :mhos or less.			
12/29/99 - Regenerate cation resin per operating procedure XXXXX.			
12/30/99 - Perform acid neutralization of FFCD neutralization sump and discharge water to the outfall per operating procedure XXX. Ensure neutralization sump level is less than 5 percent by 12/31/99.			
12/31/99 - Station additional operator at FFCD control station on swing shift.			
01/01/00 - Verify proper system operation by performing walkdown of system using special operating procedure XXXX.			

Plan No.: EX-02	Item/Component/System: : Full Flow Condensate Polisher System	Page 2
<p><b>Implementation:</b>  <b>Periods of Vulnerability:</b> <u>12/31/1999 – 01/01/2000, 02/28/2000 – 02/29/2000</u>  <b>Implementation Timing:</b> <u>See trigger dates in Risk Management section</u>  <b>Resource Requirements:</b> <u>One plant equipment operator</u>  <b>Subject Matter Expert:</b> <u>O. N. Engineer</u>  <b>Training Required:</b> <u>QPS - FFCP manual operation</u> Completed: _____  <b>Exit Strategy:</b> <u>N/A</u></p>		
<p><b>Verification &amp; Approval:</b> Verification will be accomplished by a tabletop review by facility operations staff in conjunction with the training department and the Y2K project manager.</p> <p>Verified By: <u>N/A</u> Date: _____          Approved By: _____ Date: _____</p>		



NEI/NUSMG 98-07  
August 1998

### **Example 3: Contingency Plan for Plant Monitoring System Computer**

**Risk Identification** - The plant monitoring system computer is multiprocessor, multi-tasking, and real time redundant minicomputer system providing display, alarm, trending and reports of plant operating parameters. The core limits calculator system (CLCS) module is required for power operation greater than 80 percent reactor power. The operating system was upgraded by the computer manufacturer to achieve Y2K compliance. The real-time data acquisition and display software module was modified by a third-party vendor to be Y2K compliant. Trending software was modified in-house to be Y2K ready. Integrated testing of all components was accomplished using an off-line system and simulated field inputs.

A contingency plan is deemed appropriate due to potential facility forced power reduction if CLCS is unavailable and because of the complex real time interactions of multiple software applications.

**Event Analysis** - Any possible Y2K computer failure would be expected to occur within minutes of Y2K rollover. Possible problems include:

- Unexpected computer halt - Indication of a PMS computer failure would be the PMS watchdog timer alarm on main control room annunciator panel.
- Application stall or abort - Application modules such as TRENDS and CLCS may not complete execution within allocated task schedule. The task manager may abort individual tasks that do not respond to scheduled interrupts. Indication of application stall could be lack of response to user request to display trend data or failure of display information to update. Display of module status on system console would show tasks as INACTIVE.
- Invalid calculation results - RCS leak rate calculations may indicate extreme or illogical leak rates. Smooth reactor power averages may show a step change in value due to ring buffer errors.
- Loss of trend display continuity - Trend displays of plant data may appear inappropriate due to ring buffer errors.

**Risk Management** - Contingency plans to address potential Y2K problems include:

- Unexpected PMS computer halt - Switch CLCS display to backup computer system. System date for the backup computer system is to be set 28 years back from current date as a diverse remediation strategy.

- Application stall or halt - PMS computer system engineer or computer technician shall monitor the task scheduler for proper program execution. Reset or restart stalled applications manually. For unresolved CLCS stall, follow same procedure for PMS computer halt.
- Invalid calculation result - Follow contingency plan for PMS computer halt if CLCS output contains an invalid calculation of process parameters. Perform RCS leak rate calculations manually.
- Loss of trend display continuity - Accept as is. Short-term trend display buffer will recycle after two hours. Long-term trend display recycles after 7 days.

Implementation dates for contingency plan are:

12/20/98 - Roll back system date 28 years on backup plant computer system.

12/31/99 - Perform RCS leak rate calculations manually per operating procedure XXXX.

12/31/99 - Augment swing shift staff with computer engineer/technician to monitor PMS computer performance during Y2K rollover.

01/01/00 - Verify CLCS operability post rollover date. Switch to backup computer system if CLCS is inoperable and cannot be restored on the PMS. Verify operability of trend display function, leak rate calculation, and smooth power display.

**Verification** - All of the activities are to be conducted as per procedure. Resource needs have been identified and will be available on key rollover dates.

NEI/NUSMG 98-07  
August 1998

NEI/NUSMG 98-07		<b>Year 2000 Contingency Plan</b>	
<b>Plan No.:</b> EX-03	<b>Item/Component/System:</b> Plant Monitoring System Computer System		<b>Priority:</b> HIGH
<p><b>Risk Description:</b> CLCS unavailability would result in a forced power reduction. The CLCS system incorporates complex real time interaction of multiple software applications that provides potential for a Y2K-induced event.</p>			
<p><b>Risk Analysis Summary:</b> Any possible Y2K computer failure would be expected to occur within minutes of Y2K rollover. Possible problems include the following:</p> <ul style="list-style-type: none"> <li>• Computer halt - Indication of a PMS computer failure or halt would be the PMS watchdog timer alarm on main control room annunciator panel.</li> <li>• Application stall or abort - Application modules such as TRENDS and CLCS may not complete execution within allocated task schedule. The task manager may abort individual tasks that do not respond to scheduled interrupts. Indication of application stall could be lack of response to user request to display trend data or failure of display information to update. Display of module status on system console would show tasks as INACTIVE.</li> <li>• Invalid calculation results - CS leak rate calculations may indicate extreme or illogical leak rates. Smooth reactor power averages may show a step change in value due to ring buffer errors.</li> <li>• Loss of trend display continuity - Trend displays of plant data may appear inappropriate due to ring buffer errors.</li> </ul>			
<p><b>Risk Mitigation Strategy:</b> Contingency plans to address potential Y2K problems are as follows:</p> <ul style="list-style-type: none"> <li>• Unexpected PMS computer halt - Switch CLCS display to backup computer system. System date for the back-up computer system is to be set 28 years back from current date as a diverse remediation strategy.</li> <li>• Application stall or halt - PMS computer system engineer or computer technician shall monitor the task scheduler for proper program execution. Reset or restart stalled applications manually. For unresolved CLCS stall, follow same procedure for PMS computer halt.</li> </ul>			



NEI/NUSMG 98-07  
August 1998

#### **Example 4: Contingency Plan for Work Control System Computer**

**Risk Identification** - The work control system (WCS) is used to initiate, plan, coordinate and implement maintenance activities at the plant. Maintenance order preparation, review and approval is computerized. Hardcopy printout of the maintenance order is generated when the job is ready to be worked in the field. The WCS is classified as a "quality affecting" computer application. The WCS is a client/server application with a graphical user interface front end that provides access to a relational database over a wide area network. The system has several Y2K vulnerabilities including its complex integration of various computer platforms, network interface, and commercial and custom software programs with date/time stamp dependencies. Remediation has consisted of implementing vendor firmware and operating system upgrades and code inspection of custom software developed in house. Successful integrated testing was conducted using a mock up of the system off line. Failure of the WCS could result in significant delays in planning and implementing emergent repairs, some of which may be directly related to Y2K events.

**Event Analysis** - Any Y2K-induced failure of the WCS is expected to be discovered only after Y2K rollover during the first attempt to use or access the system. Failure modes could include inability to launch the application (network or server failure), inability to access or update the database, or incorrect calculation of future routine maintenance or surveillance dates based on faulty date arithmetic.

**Risk Management** - Prepare special procedure to allow the maintenance order process to be initiated, planned, approved and implemented manually for emergent work if the WCS is not available. Train maintenance planner and equipment control personnel expected to be on shift during Y2K rollover on WCS contingency plan. Minimize challenges to the WCS during Y2K rollover by deferring routine report generation and maintenance schedule preparation to next business day (if possible) or until proper system operation has been verified by IT. Perform full system backup prior to Y2K rollover. Implementation dates for contingency plan are:

- 7/1/99 - Approve special procedure for manual work planning in event of WCS Y2K-induced failure.
- 12/1/99 - Train maintenance planners and equipment control personnel on contingency plan for WCS failure and special procedure on manual work processing.
- 12/31/99 - Perform full system backup of WCS.
- 01/01/00 - IT staff confirms proper operation of WCS.
- 02/29/00 - IT staff confirms proper operation of WCS.

**Verification** -The Training department will work with Maintenance and Operations to perform a walk-through of new WCS procedure and processes. The Training department will then develop and implement training for the identified personnel. These trained personnel will then perform the manual procedure in parallel with the computerized system to verify performance and end product.

NEI/NUSMG 98-07		<i>Year 2000 Contingency Plan</i>	
<b>Plan No.:</b> EX-04	<b>Item/Component/System:</b> Work Control System (WCS) Computer System	<b>Priority:</b> MEDIUM	
<p><b>Risk Description:</b> The system has Y2K vulnerability because of its complex integration of various computer platforms, network interface, and commercial and custom software programs with date/time stamp dependencies. Remediation has consisted of implementing vendor firmware and operating system upgrades and code inspection of custom software developed in-house. Integrated testing was simulated using a mock-up of the system off line. Failure of the WCS could result in significant delays in planning and implementing emergent repairs, some of which may be directly related to Y2K events.</p>			
<p><b>Risk Analysis Summary:</b> Any unexpected failure of the WCS is expected to be discovered after Y2K rollover following the first attempt to use or access the system. Failure modes can be inability to launch the application (network or server failure), inability to access or update the database, or incorrect calculation of future routine maintenance or surveillance dates based on faulty date arithmetic.</p>			
<p><b>Risk Mitigation Strategy:</b> Prepare special procedure to allow the maintenance order process to be initiated, planned, approved and implemented manually for emergent work if the WCS is not available. Train maintenance planner and equipment control personnel expected to be on shift during Y2K rollover on WCS contingency plan. Minimize challenges to the WCS during Y2K rollover by deferring routine report generation and maintenance schedule preparation to next business day (if possible) or until proper system operation has been verified by IT. Perform full system backup prior to Y2K rollover.</p> <p><b>Trigger dates for contingency plan implementation:</b></p> <p>7/1/99 - Approve special procedure for manual work planning in event of unexpected WCS Y2K failure.</p> <p>12/1/99 - Train maintenance planners and equipment control personnel on contingency plan for WCS failure and special procedure on manual work processing.</p>			



**Example 5: Contingency Plan For Loss of Station Emergency Plan Services (This Is the Emergency Plan Specific Portion of the Plant Process Computer Contingency Plan)**

**Risk Identification** - The facility emergency response plan (EPlan) implements the requirements of NUREG 0654 and Regulatory Guide 1.23. One of the digital components used to implement the EPlan is the use of the plant process computer (PPC) to obtain and distribute information required by and produced by EPlan requirements.

**Event Analysis** - A review of the joint NRC-FEMA report on the "Effect of Hurricane Andrew on the Turkey Point Nuclear Generating Station" illustrated the need to anticipate multiple failures, common mode failures and interdependent failures. Furthermore, it documented the competition for restoration resources that sometimes occurs subsequent to events. The EPlan was modified significantly to implement improvements that mitigate such concerns. Y2K events may challenge the EPlan, but it is an EPlan that has already been tested and verified.

The PPC provides a common facility to gather information from the facility in general and EPlan equipment in particular. It maintains the integrity of the data, provides it in a useful format, and maintains it as a historical record. The information is continuously passed through the offsite information system (OFIS) to the Emergency Response Data System (ERDS). Both systems are used to distribute data to decision makers onsite, locally and nationally. Although the PPC has redundant processors, they provide no diverse means for assuring the performance of their intended function.

The EPlan features are technical specifications requirements. They are commitments of the licensing basis supporting the current operating license. The PPC is one of the identified components.

The PPC has undergone an exhaustive Y2K review. Detailed assessments were cross-compared with independent vendor results and those of other utilities. The assessments included all analog-to-digital converters (ADCs), data-gathering equipment cabinets, interconnected processors, intelligent instruments and traditional software. The detailed assessment included testing measures for all critical date conditions that pertain to the PPC. All identified failure modes were remediated fully and confirmed by validation testing.

All applicable reviews were performed. The commitments of the facility software quality assurance program were maintained, and the design basis documentation for the PPC was revised. No changes to the licensing basis were made. There were no changes made that required prior regulatory review.

However, the PPC remains a critical component to smooth operation of the facility in general and the EPlan in particular. Since the PPC is a very complex digital system of



NEI/NUSMG 98-07  
August 1998

interconnected components that receives information from other similarly complex components, the Y2K team elected to develop a contingency plan.

**Risk Management** - The risk identified is an *internal risk*. It poses a challenge to the performance of EPlan activities. The mitigation strategy selected to offset this risk is manual data collection and requires no augmentation of existing procedures.

Subsequent to the Hurricane Andrew report, several improvements were made to the EPlan. Among these improvements was the ability to perform required activities manually for an indefinite period of time. Regular EPlan drills are conducted to demonstrate the operability of the plan. During drills, additional personnel are stationed in the control room and the emergency operations facility. Their job is to gather information from analog indicators and communicate it via diverse means (telephone and VHF radio) to EPlan command personnel.

**Verification** - This contingency plan will be evaluated as a Y2K induced failure of the PPC during the next EPlan drill scheduled 4<sup>th</sup> quarter 1998. Conditions appropriate to Y2K will be simulated. Multiple and interdependent failures will be tested.

NEI/NUSMG 98-07		<i>Year 2000 Contingency Plan</i>	
Plan No.: EX-05	Item/Component/System: Station Emergency Plan Services - Plant Process Computer	Priority: LOW	
<p><b>Risk Description:</b> The facility emergency response plan (EPlan) implements the requirements of NUREG 0654 and Regulatory Guide 1.23. One of the digital components used to implement the EPlan is the use of the plant process computer (PPC) to obtain and distribute information required by and produced by EPlan features.</p> <p>The PPC provides a common facility to gather information from the facility in general and EPlan equipment in particular. It maintains the integrity of the data, provides it in a useful format, and maintains it as a historical record. The information is continuously passed through the offsite information system (OFIS) to the Emergency Response Data System (ERDS). Both systems are used to distribute data to decision makers onsite, locally and nationally. Although the PPC has redundant processors, they provide no diverse means for assuring the performance of their intended function.</p>			
<p><b>Risk Analysis Summary:</b> The PPC has undergone an exhaustive Y2K review. All failure modes were remediated fully and confirmed by validation testing. However, the PPC remains a critical component to smooth operation of the facility in general and the EPlan in particular. Since the PPC is a very complex system of interconnected components that receives information from other similarly complex components, it is prudent to postulate that some degradation from Y2K events may occur.</p> <p>As a result of the Hurricane Andrew report, the ability to perform required EPlan activities manually for an indefinite period of time was retained. Regular EPlan drills are performed that demonstrate the acceptable use of both. During drills, additional personnel are stationed in the control room and the Emergency Operations Facility (EOF) whose job is to gather information from analog indicators and communicate it via diverse means (telephone and VHF radio) to EPlan command personnel.</p>			

<b>Plan No.:</b> EX-05	<b>Item/Component/System:</b> Station Emergency Plan Services - Plant Process Computer	<b>Page</b> 2
<p><b>Risk Mitigation Strategy:</b> The mitigation strategy selected to offset this risk is manual data collection.</p> <p>If the emergency plan is activated, station additional personnel in the control room and the emergency operations facility (EOF) to gather information from analog indicators and communicate it via diverse means (telephone and VHF radio) to EPlan command personnel.</p>		
<p><b>Implementation:</b></p> <p><b>Periods of Vulnerability:</b> <u>12/31/1999 – 01/01/2000, 02/28/2000 – 02/29/2000</u></p> <p><b>Implementation Timing:</b> <u>12/01/1999 – Designate and train additional EPlan personnel</u></p> <p><b>Resource Requirements:</b> <u>Two station engineers</u></p> <p><b>Subject Matter Expert:</b> <u>J. Pederson</u></p> <p><b>Training Required:</b> <u>EPlan Personnel</u>                      <b>Completed:</b> _____</p> <p><b>Exit strategy:</b> <u>Discontinue manual methods once service is restored and surveillances are completed.</u></p>		
<p><b>Verification &amp; Approval:</b> This contingency plan will be evaluated as a Y2K-induced failure of the PPC during the next EPlan drill scheduled 4<sup>th</sup> quarter 1998. Conditions appropriate to Y2K will be simulated. Multiple and interdependent failures will be tested.</p> <p><b>Verified By:</b> _____ <b>Date:</b> _____</p> <p><b>Approved By:</b> _____ <b>Date:</b> _____</p>		

**Example 6: Contingency Plan for Rod Position Information System**

**Risk Identification** - The rod position information system (RPIS) performs two major functions:

- It provides rod position information to the plant monitoring information system (PMIS) for control room graphical displays and calculation of core thermal values.
- It provides for the rod worth minimizer function by operating on pre-stored rod movement sequences.

While not a true safety system, RPIS is nevertheless an important system to plant operation. It is composed of a single PDP micro-11/23 processor.

**Event Analysis** - A failure of the RPIS would be obvious. The RPIS software has built-in error detection and reporting for most failures. Other failure modes would consist of the entire system going off-line, which would be immediately reported to the operators via PMIS. There is no hot standby for this system, but a warm standby is available. Less than one hour is required to bring the warm standby online. This standby provides redundancy, but not diversity, as it is identical architecture to the online system. The preferred remediation method is to obtain an upgrade to the current operating system version that is fully Y2K compliant.

**Risk Management** - The following strategy is proposed for minimizing the effects of an RPIS outage:

- Obtain rod positions from control room panels. These indications can be manually fed into PMIS so that core thermal calculations can continue. The capability to manually substitute values in PMIS already exists.
- Use existing procedures to perform rod sequence movements, if necessary, without the automation provided by RPIS. This includes additional verification steps by control room personnel to ensure that proper sequences were being followed.
- Prepare a procedure to change the date back 28 years. Since PMIS assigns all times to control rod information, the RPIS date/time is only cosmetically important.

Implementation dates for contingency plan are:

- |           |  |
|-----------|--|
| 12/1/1998 | Determine, by observation and documentation, whether rod position movements during startup could be successfully and |
|-----------|--|

NEI/NUSMG 98-07  
August 1998

- safely achieved without RPIS online. This will be following the next refueling outage.
- 7/1/1999 Approve contingency plan for loss of RPIS during/after critical Y2K dates.
- 12/1/1999 Train operations and reactor engineering personnel on RPIS contingency plan.
- 12/30/1999 Obtain a full image backup of the RPIS system. Check operability of backup system.
- 01/01/2000 Nuclear Information Services assesses operational condition of RPIS.
- 02/29/2000 Nuclear Information Services assesses operational condition of RPIS.

**Verification** - Determine, by observation and documentation, whether rod position movements during startup, could be successfully and safely achieved without RPIS online. This test will be conducted following the next refueling outage.

NEI/NUSMG 98-07		<i>Year 2000 Contingency Plan</i>	
Plan No.: EX-06	Item/Component/System: Rod Position Information System	Priority: HIGH	
<p><b>Risk Description:</b> The rod position information system (RPIS) performs two major functions:</p> <ul style="list-style-type: none"> <li>• It provides rod position information to the plant monitoring information system (PMIS) for control room graphical displays and calculation of core thermal values.</li> <li>• It provides for the rod worth minimizer function by operating on pre-stored rod movement sequences.</li> </ul> <p>While not a true safety system, RPIS is nevertheless an important system to plant operation. It is hosted on a single PDP Micro-11/23 processor.</p>			
<p><b>Event Analysis:</b> A failure of the RPIS would probably be obvious. The RPIS software has built-in error detection and reporting for most failures. Other failure modes would probably consist of the entire system going off-line, which would be immediately reported to the operators via PMIS. There is no hot standby for this system, but a warm standby is available. Less than one hour is required to bring the warm standby online. This standby provides redundancy, but <u>not</u> diversity, as it is identical architecture to the online system. The intent is to obtain an upgrade to the current operating system version that is fully Y2K compliant.</p>			
<p><b>Risk Mitigation Strategy:</b> The following strategy is proposed for minimizing the effects of an RPIS outage:</p> <ul style="list-style-type: none"> <li>• Obtain rod positions from the control room panels. These indications can be manually fed into PMIS so that core thermal calculations could continue. The capability to manually substitute values in PMIS already exists.</li> <li>• Use existing procedures to perform rod sequence movements, if necessary, without the automation provided by RPIS. This includes additional verification steps by control room personnel to ensure that proper sequences were being followed.</li> <li>• Prepare a procedure change to set the date back 28 years, at least until the operating system can be upgraded. Since PMIS assigns all times to control rod information, the RPIS date/time is only cosmetically important.</li> </ul> <p>Trigger dates for contingency plan implementation:</p>			
12/1/1998	Determine, by observation and documentation, whether rod position movements during startup, could be successfully and safely achieved without RPIS online. This will be following the next refueling outage.		
7/1/1999	Approve contingency plan for loss of RPIS during/after critical Y2K dates.		
12/1/1999	Train operations and reactor engineering personnel on RPIS contingency plan		

NEI/NUSMG 98-07  
August 1998

<b>Plan No.:</b> EX-06	<b>Item/Component/System:</b> Rod Position Information System	<b>Page</b> 2
12/30/1999 Obtain a full image backup of the RPIS system. Check operability of backup system.  01/01/2000 Nuclear Information Services assesses operational condition of RPIS.  02/29/2000 Nuclear Information Services assesses operational condition of RPIS.		
<b>Implementation:</b> Periods of Vulnerability: <u>12/31/1999 – 01/01/2000, 02/28/2000 – 02/29/2000</u>  Implementation Timing: <u>See trigger dates in Risk Mitigation section.</u>  Resource Requirements: <u>One NIS engineer.</u>  Subject Matter Expert: <u>T. I. Simple</u>  Training Required: <u>Operations Reactor Engineering Completed: _____</u>  Exit Strategy: <u>Discontinue manual methods once RPIS is restored and surveilled.</u>		
<b>Verification &amp; Approval:</b> Determine, by observation and documentation, whether rod position movements during startup, could be successfully and safely achieved without RPIS online. This test will be conducted following the next refueling outage.  Verified By: _____ Date: _____  Approved By: _____ Date: _____		

**APPENDIX D****Examples of External Contingency Plans**

As discussed in Section 7, external Y2K events are outside the direct control of the facility. Some external events are important enough to the safety of the facility that they were anticipated in design basis accident analyses. They have also been addressed exhaustively in existing contingency plans, probabilistic risk assessments (PRA), failure modes and events analysis (FMEA) and integrated plant evaluations (IPE). External events that the facility may elect to plan as part of their Y2K contingency planning process include:

- loss of offsite power
- grid instabilities
- interruption of consumable supplies such as bottled gases, domestic water, diesel fuel and telephones.
- loss of emergency plan equipment and services such as sirens, meteorology and communications equipment.

Three examples of individual contingency plans for external events are included.



NEI/NUSMG 98-07  
August 1998

Year: 2000 Contingency Plan		Plan Number: 2000-01
<b>Item/Component/System:</b> Station Consumables		<b>Priority:</b> Medium
<b>Risk Analysis:</b> Consumable providers may not be able to provide a steady supply of consumables to the station as a result of Y2K-related interruptions		
<b>Risk Mitigation Strategy and Actions</b>		
<p>1. Materials Management will review status of Y2K readiness for all consumable vendors and identify any vendors and their associated consumables that may be at risk on key rollover dates. Initiate a contract with an alternate, Y2K ready vendor for any critical plant consumable that is identified to be at risk from a primary vendor.</p> <p>2. Maintain the following plant consumables at the 90% level or greater during the implementation timing periods below. At the end of these periods, return to nominal consumable stocking levels:</p> <ul style="list-style-type: none"> <li>• Main generator hydrogen storage farm</li> <li>• Containment atmosphere dilution (CAD) nitrogen tank level</li> <li>• Containment atmosphere control (CAC) nitrogen tank level</li> <li>• Reactor water chemistry chemical reagents</li> <li>• Auxiliary boiler fuel oil storage tank</li> <li>• Site vehicle gasoline storage tank</li> <li>• Emergency diesel fuel oil storage tanks</li> <li>• Emergency diesel fuel oil day storage tanks</li> <li>• Emergency diesel generator CARDOX CO2 storage tank</li> <li>• Lubricating oils and greases (operations storage area)</li> <li>• Turbine building CARDOX CO2 storage tank level</li> <li>• Sodium Hypochlorite tank for chlorine injection system</li> <li>• Pure water storage tank levels</li> <li>• Portable nitrogen bottles for plant use</li> <li>• Bottled gas bottles for welding and other maintenance</li> </ul>		
<b>Implementation</b>		
<b>Period of Vulnerability:</b>	December 31, 1999 to January 1, 2000 February 28, 2000 to February 29, 2000	
<b>Implementation Timing:</b>	08:00h December 20, 1999 to 08:00h January 7, 2000 08:00 February 17, 2000 to 08:00 March 6, 2000	
<b>Resource Requirements:</b>	None	
<b>Subject Matter Expert:</b>	John Smith x1234	
<b>Training Required:</b>	None	
<b>Extra Strategy:</b>	N/A	
<b>Verification:</b> Review facility procedures for consumable vulnerabilities and compare against the list above.		
<b>Verified by:</b>	_____	<b>Date:</b> _____
<b>Approved by:</b>	_____	<b>Date:</b> _____

Year 2000 Contingency Plan		Plan Number: 2000-02
<b>Item/Component/System:</b> Loss of external 500-kV grid system		<b>Priority:</b> High
<b>Risk Analysis:</b> There is a small potential for loss of the external 500-kV grid system due to a Y2K-induced failure at other sites connected to the grid system.		
<b>Risk Mitigation Strategy and Actions</b>		
<ol style="list-style-type: none"> <li>1. Station an augmented operations crew on shift from 18:00 on December 31, 1999, until 18:00 January 1, 2000, and from 18:00 on February 28, 2000, until 18:00 on February 29, 2000. Additional personnel are listed on the attached modified shift lineup sheet.</li> <li>2. Coordinate with the load dispatcher to reduce plant power on both units to 95% power from 23:00 on December 31, 1999, to 04:00 on January 1, 2000, and from 23:00 on February 28, 2000, to 04:00 on February 29, 2000, to provide additional operating margin in case of grid voltage fluctuations.</li> <li>3. Station an additional plant reactor operator at the chief operator's station to monitor grid voltage and generator parameters.</li> <li>4. In case of loss of grid, the station will execute the loss-of-grid casualty procedure using the additional operators to assist with dual-unit scram actions.</li> </ol>		
<b>Implementation</b>		
<b>Period of Vulnerability:</b>	December 31, 1999 to January 1, 2000 February 28, 2000 to February 29, 2000	
<b>Implementation Timing:</b>	18:00 December 30, 1999 to 18:00h January 1, 2000 18:00 February 27, 2000 to 18:00h February 29, 2000	
<b>Resource Requirements:</b>	None	
<b>Subject Matter Expert:</b>	John Smith x1234	
<b>Training Required:</b>	Each operations crew will review the loss of offsite power procedure during the November-December 1999 training cycle. Principal crews scheduled to be on shift during the vulnerability period also will conduct a crew simulator session involving loss of offsite power in the week before the vulnerability period.	
<b>Exit Strategy:</b>	Follow guidance contained in approved facility procedures.	
<b>Verification:</b> N/A covered by facility procedure approval process.		
<b>Verified by:</b>	_____	<b>Date:</b> _____
<b>Approved by:</b>	_____	<b>Date:</b> _____

NEI/NUSMG 98-07  
August 1998

### Contingency Plan 2000-3

#### **Item/Component/System: Telecommunications**

##### **Risk Identification**

Facility emergency plans and disaster recovery plans depend on the availability of telecommunications.

##### **Event Analysis**

Since the Y2K readiness of telecommunications companies does not assure continuity of service and many Y2K experts indicate that questions still exist concerning Y2K-related failures within the integrated telecommunications network, there is some risk of the plant experiencing some period of telecommunications service disruption.

The telephone company supplying services has been contacted and has indicated that they will be Y2K ready by the first quarter of 1999; but because of the complexity of the service, they cannot preclude possible service disruptions. The Y2K team has thus determined that a contingency plan is appropriate.

##### **Risk Management**

Each department will evaluate any operational impact from the loss of telecommunications. Departments will provide a list of license-based and business-critical activities that would be impacted by a loss of telecommunications and indicate the time required before the impact would be exhibited.

Each department will prioritize their impacted business processes and assess the need for a mitigation strategy. Examples include:

##### **Emergency Preparedness**

Callout of emergency plan personnel is dependent on telephones. Therefore, emergency facilities will be pre-staffed at a pre-determined level for the millennium turnover and leap year transition.

Communications with off-site city, county, state and federal agencies also depend on telephones. Portable radios will be issued to all agencies within radio range and text beepers will be issued to the remaining agencies. Alternate mitigation strategies can include Y2K-compliant direct link satellite mobile phones or relocation of personnel within radio range (This presumes you have found a supplier that is already Y2K ready).

**Contingency Plan 2000-3 (Continued)**

**Operations**

Fire department communications will be assured by providing the local fire station with a portable radio.

Law enforcement communications will be assured by providing the sheriff's department with a portable radio.

Medical emergency communication will be assured by providing the local hospital with a portable radio.

**Implementation**

Period of Vulnerability: December 31, 1999 to January 1, 2000  
February 28, 2000 to February 29, 2000

Implementation Timing: January 1, 1999 for equipment purchase  
December 31, 1999 to January 1, 2000  
February 28, 2000 to February 29, 2000

Resource Requirements: Designated EP staff and designated departmental staff resources

Subject Matter Expert: John Smith at x1234

Training Required: None

Exit Strategy: Resumption of normal service will be accompanied by announcements over approved facility communications equipment that primary service has been restored.

Verification: Station procedures will be reviewed to ensure that no other related vulnerabilities exist.

Verified By: \_\_\_\_\_ Date: \_\_\_\_\_

Approved By: \_\_\_\_\_ Date: \_\_\_\_\_

**APPENDIX E****Integrated Contingency Plan Matrix**

This is an example of an integrated Y2K contingency plan matrix that is developed and used as part of the integrated contingency plan. This matrix is compiled as the remediation, internal risks and external risk individual contingency plans are submitted to the Y2K project manager. This matrix should be a controlled document that is frequently reviewed and updated for implementation timing and resources actions. The Y2K project manager should use this matrix to provide input to the project management scheduling program. Relationships and dependencies associated with the individual contingency plans should be identified and resolved based on the review of this matrix.

NE/NUSMG 98-07  
August 1998

Plan No.	Item, System, Component	Risk Description	Mitigation Strategy	Vulnerable Period	Implementation Timing	Resources	Subject Matter Expert	PRL
001	FULL FLOW CONDENSATE POLISHER (FFCP)	Risk may cause transients in S/G water level with possible safety system activation if S/G level control is lost. Extended loss will result in degraded S/G water quality.	Operate FFCP in passive cleanup mode during Y2K key rollover dates.	Key rollover dates between 12/31/99 to 01/01/00	12/25/99 perform OP XX. 12/29/99 regen. Per OP XX. 12/30/99 acid neut. Per OP XX. 12/31/99 station additional operator	Post one additional operator at FFCP control station	O. N. Engineer	High
002	WORK CONTROL SYSTEM COMPUTER (WCS)	Risk of inability to run application and access data base, and loss of ability to schedule and track surveillance	Prepare special procedure to manually perform work order process to be used for emergent work if WCS is not available. Perform full backup prior to key rollover dates.	12/3/99 to 01/01/00 02/28/00 to 03/01/00	07/1/99 Approve special procedure, 12/01/99 train maint. planners on procedure, 12/31/99 Full system backup of WCS 01/01/00 IT staff verify operation of WCS.	Procedure prep 40 man hours. System backup IT 8 hours, Training 48 man hours.	W. F. Olsen	Medium
003	CONSUMABLE WATER TREATMENT CHEMICALS	Depletion of chemicals required for resin regeneration and water treatment. Risk is deterioration of water quality over time.	Stock-pile supplies by topping off chemical tanks and having 60 day supply of bulk chemicals in the warehouse.	January 2000	12/20/99 Order sufficient chemicals to top off tanks. 12/20/99 Verify warehouse has 60-day supply of identified bulk chemicals. 01/03/00 Contact chemical suppliers and verify continuing supply chain.	Work performed as routine, 4 hours.	D. M. Johnson	Low

Figure E-1 Example Integrated Contingency Plan Matrix

**APPENDIX F**

**Boundary Analysis and Supply Chain Readiness**

**Boundary Analysis**—Consideration of external events may be facilitated by the use of boundary analysis. Figure F-1 provides a graphic view to help visualize this process, along with items that may be considered. This is not meant to be a comprehensive list, nor is it required that each item indicated be addressed.

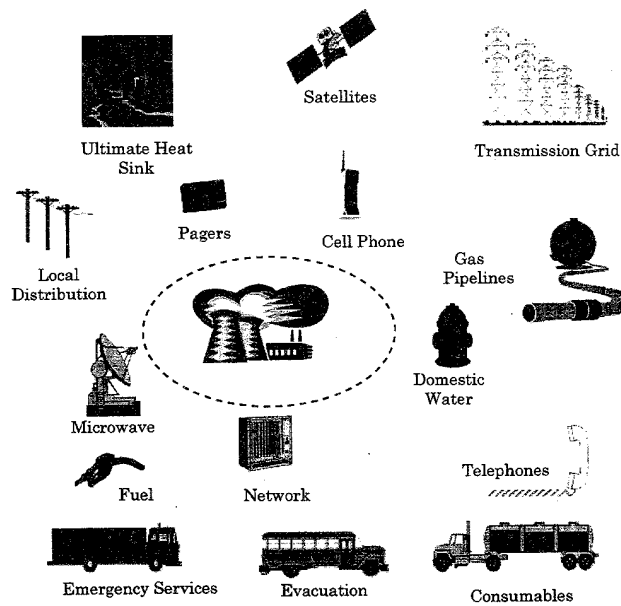


Figure F-1 External Event Boundary Analysis

NEI/NUSMG 98-07  
August 1998

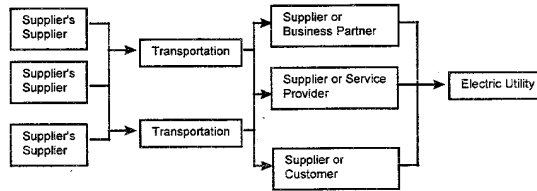
An example that illustrates the use of the technique is: the ultimate heat sink for the facility is the level of water in the river. The water level is maintained by control of gates operated by another utility as part of its hydro-electric power generation division. There are technical specification requirements for river water level and temperature. Plant instrumentation indicating this information is transmitted to the hydro facility control room. The facility can also communicate with the hydro facility by phone.

Concerns regarding indication and communication have surfaced as part of the Y2K project detailed assessment. The external interface has been identified as a risk to the safe operation of the facility. To mitigate the risk, the facility has invested in suitable portable radios to provide a diverse means of communication.

Affected procedures have been revised at both facilities. Simulators have been upgraded to allow revised operator training. The radio system has been added to the appropriate surveillance procedures.

**Supply Chain Readiness**—The supply chain warrants special attention for critical consumables. A critical element of external event analysis is to understand the complete supply chain for critical systems and suppliers. Figure F-2 illustrates a process for assessing the Y2K risks that result from dependence on suppliers and their partners. The supply chain is only as strong as its weakest link. The weak links should be identified and analyzed. An appropriate mitigation strategy should be selected. The facility may place some reliance on the remediation program of the supplier.

Where are the critical weak links???



Supply Chain Readiness Management Process

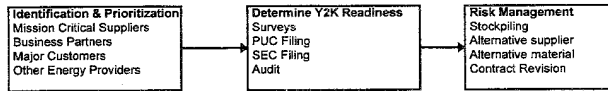


Figure F-2: Supply Chain Readiness Management



Mr. HORN. Also in the record will be the letter of February 25, 1999, to Chairman Jackson, and the response that was the response from there and our letter from December 17, 1998 earlier when it was mentioned in the record. Without objection, it will be there.

[The information referred to follows:]

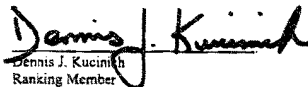


We stand ready to provide assistance with regards to this matter as you may need it. Your prompt action and response to this letter, as well as your continued efforts to ensure that the Year 2000 problem does not present a risk to public health and safety, are very much appreciated.

Respectfully yours,



Stephen Horn  
Chairman  
Subcommittee on Government Management,  
Information, and Technology  
Committee on Government Reform  
and Oversight



Dennis J. Kucinich  
Ranking Member  
Subcommittee on Government Management,  
Information, and Technology  
Committee on Government Reform  
and Oversight



Donald A. Manzullo  
Vice-Chairman  
Subcommittee on Government Programs  
and Oversight  
Committee on Small Business

### Timeline of NRC Staff Nuclear Power Plant Y2K Readiness Oversight Efforts

May 1998	Issued GL 98-01, "Year 2000 Readiness of Computer Systems at Nuclear Power Plants."
August 1998	Received first licensee responses to GL 98-01 confirming implementation of NEI/NUSMG 97-07, "Nuclear Utility Year 2000 Readiness."
September 1998	Began NRC staff sample audits of 12 licensee Y2K readiness programs.
January 1999	Completed sample audits of Y2K readiness programs; Issued GL 98-01 Supplement 1.
March 1999	Issue Information Notice summarizing Y2K readiness audit observations and lessons learned.
April 1999	Begin review of 6 licensee contingency planning efforts.
May 1999	Begin resident inspector review of Y2K program at each site.
June 1999	Complete licensee contingency planning reviews.
July 1999	Review second licensee responses to GL 98-01 or GL 98-01 Supplement 1 confirming Y2K readiness and address any that may raise concerns. Complete resident inspector reviews of Y2K programs.
September 1999	NRC staff decision on need to order plant specific Y2K action (e.g., shutdown).

Enclosure



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

February 25, 1999

The Honorable Stephen Horn, Chairman  
Subcommittee on Government Management,  
Information, and Technology  
Committee on Government Reform  
United States House of Representatives  
Washington, D.C. 20515-6143

Dear Congressman Horn:

Thank you for your letter to me dated December 17, 1998. The Commission shares your concern that the Year 2000 (Y2K) problem not pose an adverse impact on public health and safety and that nuclear power plants continue to operate safely throughout 1999 and 2000 and beyond. From your oversight of the Nuclear Regulatory Commission (NRC) staff efforts to address the Y2K problem, you will note that we continue to be proactive with licensees in order to achieve Y2K readiness of all nuclear power plants.

Your letter focuses on one of a number of initiatives undertaken by the NRC staff to address the Y2K problem, namely the 12 sample audits of licensee Y2K readiness programs. A sample audit approach was determined by the NRC staff to be an appropriate means of oversight of licensee Y2K readiness efforts based on the fact that all licensees had committed to the nuclear power industry Y2K readiness guidance (NEI/NUSMG 97-07) in their first response to NRC Generic Letter (GL) 98-01 and the NRC staff had not identified any Y2K problems in safety-related actuation systems. The 12 licensee sample includes large utilities such as Commonwealth Edison and Tennessee Valley Authority (TVA) as well as small single unit licensees such as North Atlantic Energy (Seabrook) and Wolf Creek Nuclear Operating Corporation. Because licensee Y2K programs are corporate-wide, many of the NRC staff audits include more than a single nuclear power plant site since many utilities own more than one nuclear power plant. In all, a total of 42 of 103 operating nuclear power plant units were associated with the Y2K readiness program audits of 12 utilities. The NRC staff selected a variety of types of plants of different ages and locations in this sample in order to obtain the necessary assurance that nuclear power industry Y2K readiness programs are being effectively implemented and that licensees are on schedule to meet the readiness target date of July 1, 1999, established in GL 98-01. The second response to GL 98-01 requests confirmation of plant readiness by July 1, 1999, or a status and schedule for those actions necessary to achieve readiness. The results of the audits will be used to assess the overall Y2K readiness of commercial nuclear power plants, and to determine the need for any additional action, such as expansion of the audit sample, formal inspections, or other regulatory action.

In late January, we completed the 12 audits. Based on the results of these audits, we concluded that the audited licensees were effectively addressing the Y2K problem and were undertaking the actions necessary to achieve Y2K readiness per the GL 98-01 target date. We

did not identify any issues that would preclude these licensees from achieving readiness. These findings are consistent with those recently reported by the Department of Energy in the report prepared by the North American Electric Reliability Council on the status of Y2K readiness of the electric power grid. The NRC staff is not aware of any Y2K problems in nuclear power plant systems that directly impact actuation of safety functions. The majority of commercial nuclear power plants have protection systems that are analog rather than digital. Because Y2K concerns are associated with digital systems, analog reactor protection system functions are not impacted by the Y2K problem. Errors such as incorrect dates in print-outs, logs or displays have been identified by licensees in safety-related devices, but the errors do not affect the functions performed by the devices or systems. Most Y2K problems are in balance-of-plant and other systems such as security systems and plant monitoring systems which support day-to-day plant operation but have no direct functions necessary for reactor safety. These systems are being addressed in the licensee Y2K readiness programs consistent with the industry guidance and GL 98-01 schedule.

We have also made the General Accounting Office (GAO) Y2K guidance available to the industry on the NRC website and have referenced it in GL 98-01. We have noted from the completed audits that licensee Y2K contingency planning efforts have not progressed far enough for a complete NRC staff review, and, therefore, additional oversight of this area is planned for the Spring of 1999. The NRC staff currently plans to review the contingency planning efforts of six different licensees from those included in the initial 12 sample Y2K readiness audits, beginning in April 1999 and ending in June 1999. These reviews will focus on the licensees approach to addressing both internal and external Y2K risks to safe plant operations based on the guidance in NEI/NUSMG 98-07.

With regard to the assessment of Y2K programs at operating nuclear power plants, NRC resident inspectors will review plant-specific Y2K program implementation activities including contingency planning. The resident inspectors will be using guidance prepared by the NRC headquarters staff who conducted the 12 sample audits. Training in the use of the guidance will be provided. The experienced headquarters staff will be available to the resident inspectors for support and assistance during the review as necessary. The headquarters staff will also provide oversight of these reviews to ensure consistency among the Y2K program implementation activities. The results of the resident inspector plant-specific Y2K program reviews will be documented in publicly available documents which will be posted on the NRC Year 2000 website.

I note in your letter that you refer to the NRC audit of the Seabrook plant, which was conducted in September 1998, as an example of your concerns on Y2K readiness. Of the 12 items classified as "Safety Implication" items, only one, the Reactor Vessel Level Indication System, performs a post-accident monitoring and actuation function -- isolation of certain high energy lines upon indication of leakage in these lines. This safety-related system has been assessed by the licensee as not Y2K compliant. Only the monitoring function has been determined to potentially be affected by the Y2K noncompliance. The actuation function has not been determined to be affected by the Y2K noncompliance and, therefore, the system will continue to properly perform its intended safety function. The system is being remediated by the vendor, Westinghouse, as part of the Westinghouse Owners Group Y2K effort. The remediated system

is scheduled to be tested and installed at Seabrook prior to July 1, 1999. I would point out that this is an example of how Y2K problems are addressed in a well-implemented Y2K readiness program. Because all power reactor licensees have committed to follow a Y2K readiness program similar to the industry proposed, NRC-endorsed program, we have confidence that all licensee programs will similarly identify and correct such problems if they exist. You also express concern that the audit reports are not presented in a standard format that is understandable to the general public. We will make an effort to address this concern in the finalization of the remaining audit reports.

The NRC staff will continue its vigorous oversight of the Y2K problem in nuclear power plants through the remainder of 1999. In July 1999 a review of all licensee responses to GL 98-01 will be performed and the staff will address any that may raise concerns. By September 1999, we will determine the need for issuance of orders to address Y2K readiness issues including, if warranted, shutdown of a plant. At this time, we believe all licensees will be able to operate their plants safely during the transition from 1999 to 2000, and do not believe significant plant specific action directed by the NRC is likely to be needed. Enclosed in this letter is a timeline showing the milestones and schedule for the NRC staff's completed and remaining Y2K readiness oversight efforts for nuclear power plants.

I also note in your letter that you have indicated your readiness to provide assistance to the NRC in this matter if needed. Upon completion of our activity planning efforts we will evaluate the need for resource assistance as you have offered. I remain confident that the actions taken by the NRC staff and planned for the future and the resources committed are appropriate based on our understanding of the potential safety impact of the Y2K problem on nuclear power plants.

The Commission remains committed to ensuring that the NRC does what is necessary in its oversight of nuclear power plant licensee Y2K readiness efforts in order to achieve readiness of these facilities to safely operate throughout 1999, 2000 and beyond. Please call me if I can be of further assistance.

Sincerely,



Shirley Ann Jackson

Enclosure: Timeline

Mr. HORN. I now yield to the ex-ranking member, Mrs. Maloney, if she has any questions.

Mrs. MALONEY. No questions, Mr. Chairman.

Mr. HORN. OK. Do we have any from the vice chairman of the Government Management, Information, and Technology Subcommittee?

[No response.]

Mr. HORN. How about Dr. Bartlett.

Mr. BARTLETT. Thank you very much.

Since most embedded chips will not know what time zone they are in, if they were to fail, when should we expect them to fail?

Mr. MIRAGLIA. In terms of the guidance, sir, we recognized that some of them may be on Greenwich Mean Time, so, in terms of the contingency planning, it is to look for failures across that spectrum. And, in terms of the assessment and the remediation, that was recognized, as well. It depends on the embedded chip and the functions that it performs.

Mr. BARTLETT. Greenwich Mean Time midnight would be when here?

Mr. RHODES. 7 p.m. Eastern time.

Mr. BARTLETT. 7 p.m. So if embedded chips are going to cause problems, we could expect that to perhaps start happening about 7 p.m.?

Mr. MIRAGLIA. And, as I indicated, we are manning our response centers, sir, at 6 p.m.

Mr. BARTLETT. You are an hour ahead of the curve?

Mr. MIRAGLIA. Hopefully, sir.

Mr. BARTLETT. Hopefully. Let me ask, are there, to your knowledge, any countries with nuclear power plants who have not been cooperating so that we do not know the status of their readiness?

Mr. MIRAGLIA. In terms of what I understand the primary assessor of the international Y2K readiness is the International Atomic Energy Agency, and they have been conducting assessments at the various countries. I am not aware of any such issues, but that is the extent of my knowledge.

Mr. BARTLETT. As far as the panel knows, all countries with nuclear power generating facilities have been inspected and are cooperating?

Mr. RHODES. I cannot say that they have been inspected. I can say they are providing information. The information, however, is self-reported and some of the official positions that are given, as we were discussing earlier about the former Soviet Union, are not very encouraging.

Mr. MIRAGLIA. I would offer the same answer, sir. I know the IAEA has gone to a number of the countries to make assessments and suggestions and the like, and the President's Y2K Council has been very active through the U.N. and encouraged information sharing and providing information flow and that kind of thing, but as to whether each plant has been inspected or not, I can't answer that question, either.

Mr. BARTLETT. I thank you.

Thank you, Mr. Chairman.

Mr. HORN. On that question, a few weeks ago we had a hearing here that related to the International Civil Aviation Organization



that is a similar organization to the nuclear one in Europe, and there were about 35 countries that hadn't released the information.

Well, our hearing got them to release them, so that was Friday, and Monday morning we had them.

But the question would be to the Nuclear Commission, the U.S. version, which you represent: do you have access to the documents they would have filed with the international agency? And I think some of you were dubious if they have filed. Granted, it is self-reported, but so are what the executive branch here that we look at every quarter. That is all self-reported, and the only time we will know if those data were proper and reliable will be on January 1, 2000, wherever the time zone is.

Mr. MIRAGLIA. In terms of our agency and access, as I said, we have been cooperating and we do get reports via the IAEA.

We are an independent regulatory agency, and perhaps the Department of Energy would have even more direct access, but we do get reports on the assessments being done by IAEA and have a general knowledge and awareness of the kinds of discussions and findings that they have.

Mr. HORN. One of our worries is, with the power needs, we look at Japan. We are worried about that. We look at Italy. We are worried about that. We know there are some central European and eastern European countries that haven't really taken the energy and the focus that you have had in this country. That is what worries us.

Is that a correct worry?

Mr. MIRAGLIA. I think your representation reflects the degree of knowledge that we have, as well, sir, as the concerns overseas.

Mr. HORN. Well, let me ask you gentlemen if there are any questions you would make or any points you would make that we didn't get out of you in the question period.

Mr. Beedle.

Mr. BEEDLE. I'd like to make a comment concerning Mr. Bartlett's question, "Does this offer an opportunity to underscore the value of nuclear in this Nation's energy mix?"

This Y2K situation is rather interesting. About 2 years ago the focus was on, "Let's shut all these plants down because we are not sure they are going to be safe." Now the emphasis is, "Keep them running, because we need the energy."

So I would say to Mr. Bartlett we do have an opportunity to underscore the value that these nuclear plants provide to this Nation of ours. They do present 20 percent of the electric generation, it is clean, it is reliable, and I think we are well prepared to deal with Y2K.

Mr. HORN. OK. It looks like there are no more questions.

Mr. MIRAGLIA. Might I comment on the last comment, sir, in terms of the posture of the NRC with respect to that? The NRC was created back in 1975 from the perspective of being an independent regulator, and, as such, we are not a promoter of the use of nuclear energy, so to take an active role in the promotion, sir, that is not a particular statutory mandate we have. That rests more with the executive branch and the Department of Energy.

Notwithstanding that, our job is to assure that if nuclear power is used in this country, it is used safely, and that is our goal and our mission, and that we should also not be an impediment.

The former chairman and present commissioners have indicated that we should have the right kind of regulation for each of the activities that we regulate.

Our posture and goal is to make our regulatory process an efficient one, and, in terms of public outreach, we have an obligation in establishing public confidence in that we are doing our job of protecting and providing reasonable assurance for the public health and safety, and so in that sense we have that type of obligation, and we recognize it, sir.

Mr. HORN. Well, on that point, the two reactors you mentioned at the beginning of your testimony I take it will conform with your safety standards on this subject.

Mr. MIRAGLIA. In terms of the two remaining ones?

Mr. HORN. Right.

Mr. MIRAGLIA. Yes, sir. We will followup.

Mr. HORN. In other words, you are telling us you don't have to worry about 103, they are all going to be OK.

Mr. MIRAGLIA. That is a reasonable assurance of that expectation, sir.

Mr. HORN. OK. Good.

Mrs. MORELLA. Thank you.

Mr. Chairman, I just wanted to ask about, speaking of international, my understanding is that there is going to be a command center right in Washington, DC, that is going to be monitoring what happens in New Zealand. Are you all going to be connected to that? Maybe GAO would know the total structure of it.

Mr. WILLEMSSEN. I can comment on the Information Coordination Center from a more broad perspective.

FEMA will be a key part of the Information Coordination Center that, and through its regional offices will be gathering information on what is happening in States and localities, and that information will flow up to the ICC.

In addition, each of the major Federal agencies will have their own command/coordination center and report into the ICC.

I anticipate that NRC will have a similar mechanism. We have briefly looked at the NRC's day one plan and note that they have begun efforts to do that internally, and I have heard in the testimony today additional planned efforts from an oversight and an external perspective.

I look forward to the detail in their plans on how exactly that will be carried out.

Mr. MIRAGLIA. If I may add to that, Madam Chairwoman, in terms of our contingency plan, it does include an element of participation in the coordinating center.

In part of the contingency plan that we exercised on October 15th, we simulated our ICC cell. I, personally, will be at the ICC during the turn-over, with some additional staff, having communications to our central response center.

As Mr. Willemsen has indicated, it is to be a central flow of information.

In addition, the Y2K early warning system data is being provided to the ICC, as well, so we will have an involvement.

And, as Mr. Willemsen has said, the existing Federal response plan, overall response plan, is FEMA, and all of that is coordinated with many, many sister Federal agencies.

Mrs. MORELLA. Thank you.

Thank you, Mr. Chairman.

Mr. HORN. Well, thank all of you, because I think this has reassured a lot of us. We had been very worried when you hadn't been looking at all of the reactors, and now you have taken that view, and I'm very impressed with the testimony we have received today and I thank all four of you for giving us that information. That is most helpful.

Let me thank the majority and minority staff that prepared this hearing. J. Russell George is back there in the corner, staff director and chief counsel; to my immediate left, your right, Matt Ryan, senior policy director on Government Management, Information, and Technology, prepared the hearing; Bonnie Heald, our communications director and professional staff member against the wall there; Chip Ahlswede, our clerk; and P.J. Caceres, a faithful intern; and Deborah Oppenheim, the other faithful intern. And from the Technology Subcommittee of the House Committee on Science, Jeff Grove, staff director; and Ben Wu, professional staff member; Joe Sullivan, staff assistant. And from the minority staff, Trey Henderson, minority counsel, and Jean Gosa, staff assistant. And from the Technology Subcommittee, Michael Quear, professional staff member; and Mary Ralston, staff assistant. And our court reporter is Ruth Griffin.

So thank you all, and with that we are adjourned.

[Whereupon, at 1:59 p.m., the subcommittees were adjourned.]

