

**WILL Y2K AND CHEMICALS BE A VOLATILE MIX?**

---

---

**FIELD HEARING**  
BEFORE THE  
**SPECIAL COMMITTEE ON THE  
YEAR 2000 TECHNOLOGY PROBLEM**  
**UNITED STATES SENATE**  
ONE HUNDRED SIXTH CONGRESS  
FIRST SESSION  
ON  
Y2K PROBLEMS AS THEY IMPACT THE CHEMICAL INDUSTRY

—————  
MAY 10, 1999

TRENTON, NJ  
—————

Printed for the use of the Committee



Available via the World Wide Web: <http://www.access.gpo.gov/congress/senate>

U.S. GOVERNMENT PRINTING OFFICE

56-950 CC

WASHINGTON : 1999

SPECIAL COMMITTEE ON THE  
YEAR 2000 TECHNOLOGY PROBLEM

[Created by S. Res. 208, 105th Cong., 2d Sess. (1998)]

ROBERT F. BENNETT, Utah, *Chairman*

JON KYL, Arizona

GORDON SMITH, Oregon

SUSAN M. COLLINS, Maine

TED STEVENS, Alaska, *Ex Officio*

CHRISTOPHER J. DODD, Connecticut,

*Vice Chairman*

JOHN EDWARDS, North Carolina

DANIEL PATRICK MOYNIHAN, New York

ROBERT C. BYRD, West Virginia, *Ex Officio*

ROBERT CRESANTI, *Staff Director*

T.M. (WILKE) GREEN, *Minority Staff Director*

(II)

# CONTENTS

## STATEMENT BY COMMITTEE MEMBERS

Robert F. Bennett, a U.S. Senator from Utah, Chairman, Special Committee on the Year 2000 Technology Problem .....	1
--	---

## CHRONOLOGICAL ORDER OF WITNESSES

Gerald Poje, Board Member, Chemical Safety and Hazard Investigation Board .....	4
Francis J. Frodyma, Deputy Director, Policy Directorate, Occupational Safety and Health Administration .....	6
Paul Couvillion, Global Director, DuPont Year 2000 Project .....	9
Jamie Schleck, Executive Vice President, Jame Fine Chemical .....	11
Charlie B. Martin, Jr., Site Safety Director, Hickson Danchem Corporation ....	20
James L. Makris, Director, Chemical Emergency Preparedness and Prevention Office, Office of Solid Waste and Emergency Response, Environmental Protection Agency .....	22
Paula R. Littles, Legislative Director, Paper, Allied-Industrial, Chemical and Energy Workers International Union .....	25
Lt. Colonel Michael Fedorko, Acting Superintendent, New Jersey State Police .....	27
Jane Nogaki, Board Member, New Jersey Work Environment Council and Pesticide Program Coordinator, New Jersey Environmental Federation .....	28

## ALPHABETICAL LISTING AND MATERIAL SUBMITTED

Bennett, Hon. Robert F.:	
Opening statement .....	1
Prepared statement .....	35
Couvillion, Paul:	
Statement .....	9
Prepared statement .....	36
Fedorko, Lt. Col. Michael A.:	
Statement .....	27
Responses to questions submitted by Chairman Bennett .....	38
Frodyma, Francis J.:	
Statement .....	6
Responses to questions submitted by Chairman Bennett .....	76
Littles, Paula R.:	
Statement .....	25
Prepared statement .....	78
Responses to questions submitted by Chairman Bennett .....	79
Makris, James L.:	
Statement .....	22
Prepared statement .....	80

IV

	Page
Makris, James L.—Continued	
Responses to questions submitted by Chairman Bennett .....	85
Martin Jr., Charlie B.:	
Statement .....	20
Prepared statement .....	88
Responses to questions submitted by Chairman Bennett .....	90
Nogaki, Jane:	
Statement .....	28
Prepared statement .....	92
Responses to questions submitted by Chairman Bennett .....	94
Poje, Gerald V.:	
Statement .....	4
Prepared statement .....	96
Responses to questions submitted by Chairman Bennett .....	111
Schleck, Jamie:	
Statement .....	11
Prepared statement .....	116

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

The American Crop Protection Association .....	120
Prepared Statement of the Chemical Manufacturers Association .....	127
Prepared Statement of the Chlorine Institute, Inc. ....	131
Prepared Statement of Audrey R. Gotsch, DrPH .....	134
Overview of Responsible Care® .....	135
Prepared Statement of Geary W. Sikich .....	138

## **WILL Y2K AND CHEMICALS BE A VOLATILE MIX?**

**MONDAY, MAY 10, 1999**

U.S. SENATE,  
SPECIAL COMMITTEE ON THE YEAR 2000  
TECHNOLOGY PROBLEM,  
*Trenton, NJ.*

The committee met, pursuant to notice, at 12 noon, in Committee room 11, Fourth floor, Statehouse Annex, 125 West State Street, Trenton, New Jersey, Hon. Robert F. Bennett (chairman of the committee), presiding.

Present: Senator Bennett.

### **OPENING STATEMENT OF HON. ROBERT F. BENNETT, A U.S. SENATOR FROM UTAH, CHAIRMAN, SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM**

Chairman BENNETT. Good afternoon. The committee will come to order.

My name is Robert Bennett. I am the chairman of the Special Senate Committee on the Year 2000 Technology Problem, and I am grateful to the State of New Jersey for making these facilities available to us, to allow us to hold this field hearing on Y2K problems as they impact the chemical industry.

I apologize for our late start from our earlier advertised time. Even though Y2K has not struck yet, the planes were still late coming out of Washington, and delayed the schedule on that basis.

Also, we had invited, and expected, Senator Lautenberg to come. He is not a member of the committee, but he had expressed an interest in being here, and we are always delighted to have him join us. We are told that there is a funeral that he has to attend, a death of someone close to him that has changed his schedule, and we extend our condolences to him and of course excuse him from being here. That means you are going to have to put up with me alone for the balance of the afternoon, along with of course the witnesses.

We are pleased to hold the hearing in New Jersey, not only because of the importance of the industry to New Jersey but because it is nice to get out of Washington every once in a while and hear from people who are in the real world instead of who are in the somewhat hothouse atmosphere inside the beltway.

Now I have just come from a tour of Sybron Chemicals in Birmingham, and I was impressed with what I found there. They have taken the Y2K problem very seriously in terms of effort and money. The two of course always go together. And I hope that most of the

chemical plants in America are as far along as they are. They gave me some insights into some of the challenges that they had, and that is again one of the reasons we hold these hearings outside of Washington when we can, because we can always tie them to a visit to actual facilities, instead of just having people describe them to us.

Today we have an excellent group of witnesses who have taken time out from their busy schedules to help shed light on the Y2K problem. We will have two panels, and I am grateful to all of the witnesses.

Before we begin with the witnesses, let me talk briefly about the importance of the chemical industry to America and of its place with respect to this problem. Chemicals, almost like computers, seem to be everywhere. The crude oil refining industry keeps America's transportation running, and it is dependent on chemicals. Our health, sometimes our lives, are dependent on pharmaceuticals that go back to the chemical industry.

The manufacturer of virtually every consumer product in one way or another is dependent on chemical ingredients, and we put up this chart in the form of a home that demonstrates that. Chemical products are present in the chart from everything from shampoo to floor polish and almost everything in between.

Now, on the economic side, the \$392 billion chemical industry is the largest industry in the manufacturing sector. Manufacturing has been overtaken by the service sector, but still in the manufacturing sector of our economy the chemical industry is the largest one. It employs over a million workers. It is our largest exporter, accounting for \$69.5 billion or 10 percent of the exports in 1997, which easily outdistances the second largest industry in exporting, which is agriculture. It generates a trade surplus on the average of more than \$16 billion annually over the last 10 years. So it is not only everywhere in our lives, it is a very significant part of our economic structure as well.

The chemical industry has set very high standards for safety. We take it for granted with respect to this industry. They handle highly toxic and dangerous materials every day and have turned safety into a routine experience rather than the exception. This is an industry that is already accustomed to dealing with risks, and that is the good news with respect to the Y2K problem because it is a problem that raises the possibility of risks.

But the reason we focus on it is because if there is an accident in this industry, it can have potentially devastating effects. Even though it happened over 15 years ago, and fortunately for us, in another country, most of us remember the Bhopal accident that killed several thousand people and injured tens of thousands of others.

We have never seen a chemical release of that size in the United States, we hope we never will, but the potential is always there. Something like Y2K that could trigger a failure in a plant is a logical reason for us to step back and take a look at it. An estimated 85 million Americans, which is roughly 30 percent of the population, live within five miles of one of the 66,000 sites that handle hazardous chemicals, so that is another reason why we need to look at this very closely.

In addition to safe onsite operations, chemical processing plants must prepare to deal with external services which might be Y2K vulnerable. Let me give you an example. On November 24, 1998, a power outage caused the shutdown of a plant in Washington, a refinery in Washington. As the refinery was returned to operation after a cool-down period, an accident occurred that took the lives of six workers.

Now, the power outage may not have directly caused the accident, but it caused the condition that put the workers into a harmful situation. It created the circumstances that put six men into danger and ultimately cost them their lives. This, in a way, is reminiscent of what happened at Chernobyl. People always raise the Chernobyl example as one of their fears with Y2K.

It is interesting to note that the release of nuclear material into the atmosphere at Chernobyl was not caused directly by the shutdown or failure of the plant. It was human error that occurred as they were trying to deal with the failure of the plant. And that is, again, a paradigm of what might happen here. If we have a shutdown because of Y2K, the difficulty of bringing the plant back might then trigger an accident which the shutdown itself did not.

I am told, I didn't know this before, that the two most dangerous times and accident prone-times in a chemical plant are when it is shutting down and starting up; sort of like an airplane, the two most dangerous times are when it is taking off and landing.

So the industry must prepare itself for some unexpected Y2K shutdowns and be very careful about the safety connected, also, with starting up. An industry with many harmful and toxic substances gives us one where there is very little room for error.

Now, as we do in these hearings, because the committee has no ability to pass a law stating that there will be no problems, or pass a law stating that the arrival of the Year 2000 will be delayed for 6 months while we get ready for it, one of the things we have done historically in the committee is to focus on the regulators who have access in the industry and have some degree of influence.

I knew that we were getting somewhere when my son-in-law, who works for a bank, came to me and said, "I don't know what has happened, but the bank examiners from the Federal Reserve Board now have only one thing on their minds, and that is Y2K. They have turned it into the top priority in the bank." And since we had had the Federal Reserve Board before our committee and talked to them about Y2K, I quietly took a little credit for that and said maybe, for one of the few times in government, something that we are doing is having an impact.

And that is one of the things we will be doing here today, also, not only finding out about where the industry is but talking to the regulators, and both stimulating them to help solve the problem and giving them an opportunity to inform the public as to what they have been doing and where we are. That kind of information is very important.

You can get on the Internet and find web sites that will tell you Y2K is going to lead to TEOTWAWKI. "TEOTWAWKI" for those who have not been on the Internet, is maybe the world's longest acronym, and it stands for "the end of the world as we know it." I don't think it will be TEOTWAWKI, but it is still something we

need to focus on, and we can prevent panic by getting out accurate information. This hearing will give us the opportunity to do that.

So with those preliminary remarks, we will now introduce the members of our first panel, some of whom have already testified before the committee and are familiar with what we do. We will hear from the Honorable Dr. Jerry Poje, who is a member of the U.S. Chemical Safety and Hazards Investigation Board. He is principal author of the March 1999 report on this subject, which first got this committee stimulated to pay attention to chemicals.

He will be followed by Mr. Francis Frodyma, the acting director of Policy at the Occupational Safety and Health Administration. Then we will hear from Mr. Paul Couvillon, who is global director for DuPont's Year 2000 Project, and Mr. Jamie Schleck, executive vice president of Jame Fine Chemicals, a specialty chemical manufacturer here in New Jersey. I see one more at the table, and I am not sure exactly who you are, sir.

Mr. COHN. My name is Don Cohn. I am legal counsel for DuPont.

Chairman BENNETT. OK, so you are here to make sure that Mr. Couvillon doesn't say something that will cause him to go to jail, or DuPont to be sued.

Mr. COHN. Yes.

Chairman BENNETT. To go back to another hearing, you are not a potted plant. Very good.

Dr. Poje, again, we thank you for your leadership in this area, and appreciate your help and appreciate your testimony. Let me give you one word on logistics here.

We have asked each of the witnesses to limit his testimony to 5 minutes. We have received much more extensive statements from them in writing, which will be part of the record of the hearing.

And we have this device to tell us when the 5 minutes are up. Unlike the one we use in the Senate, that has an amber light that can tell you when 4 minutes are up, this one is either red or green. No nonsense here in New Jersey, you are either up or you are down. But what we will do, we will turn the red light on after 4 minutes, as if it were the amber light, so you do get some kind of a warning and you don't have to cutoff in mid-sentence.

We don't usually do that in the Senate. That is left up to the Supreme Court, where a lawyer once asked the Chief Justice, "May I finish my sentence?" and he said, "If it's a short one." We won't be quite that dramatic, but we would appreciate your paying attention to the time limits so that will give us time for more interaction within the panel and more questions and other comments.

So with those ground rules, Dr. Poje, again we are grateful for your being here and look forward to your testimony.

**STATEMENT OF GERALD POJE, BOARD MEMBER, CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD**

Mr. POJE. Good afternoon, Mr. Chairman. I am Gerald V. Poje, member of the U.S. Chemical Safety and Hazard Investigation Board, a position nominated by the President and confirmed by the Senate.

I oversee the Board's efforts on reducing risk of accidents associated with the Year 2000 computer problems. The Board and its



members thank you for inviting us to testify regarding this critical issue.

The Chemical Safety Board is an independent Federal agency with the mission of ensuring the safety of workers and the public by preventing or minimizing the effects of industrial and commercial chemical incidents. The CSB is a scientific investigatory organization responsible for finding ways to prevent or minimize the effects of chemical accidents at commercial or industrial facilities. The Board is not an enforcement or regulatory agency.

Our Board views the Y2K issue within the larger evolutionary trend of expanding automation and information technologies in the chemical handling sectors. New technology will continue to penetrate the work place, affecting management, workers, equipment, and interrelationships with suppliers, customers, regulators, and the surrounding community.

Chairman BENNETT. His mike is on, so OK, go ahead.

Mr. POJE. How our Nation and businesses manage the Y2K problem will provide important lessons for other new technology issues. If Y2K failures become sufficiently apparent in 1999 to 2000, policymakers will likely need to consider three major issues:

First, the absence of adequate data regarding Y2K compliance, despite widespread recognition of the problems, deadlines for compliance, and consequences; second, inadequate application of established principles for managing process safety in facilities, particularly as it relates to automation and information technologies; and, third, gaps in process safety training, technical assistance, and research, particularly as it applies to small and mid-size facilities and those in low-income and minority communities.

The problem before this committee is urgent and significant. As you already pointed out, there are some projections of risk to the U.S. population. Even this projection from EPA may underestimate the full risk to the U.S. population.

Late last year your committee asked the Chemical Safety Board to investigate the issues of chemical safety and the Year 2000 computer technology problem, requesting that we evaluate the extent of the Y2K problem as it pertains to automation systems and embedded systems; the awareness of large, medium and small companies within the industry; their progress to date in addressing the Year 2000 problem; the impact of the Year 2000 problem on EPA's risk management plans; and Federal agency roles in preventing disasters due to the Year 2000 problem.

In December 1998 our Board convened an expert workshop on Y2K and chemical safety, involving leaders from industries, equipment vendors, insurance companies, regulatory agencies, research agencies, universities, labor organizations, environmental organizations, trade associations, professional engineering associations, and health and safety organizations. As a result, the Board considers the Y2K problem to be a significant problem in the chemical manufacturing and handling sector.

Enterprises with sufficient awareness, leadership, planning, lead time, financial and human resources, are unlikely to experience catastrophic failures and business continuity problems unless their current progress is interrupted or there are massive failures of utilities. Many larger corporate entities fit this profile. The overall sit-

uation with small and mid-size enterprises is less determinate, but efforts on the Y2K problem appear to be less than appropriate, based upon inputs from many experts.

While the impact of RMP should be positive, there are no special emphases or specific mention of Y2K technology hazards in either EPA or OSHA regulations. Compliance activities reported to the Safety Board to date have not found a single failure which, by itself, could cause catastrophic chemical accidents. However, it is unclear what the outcome might be from multiple failures, multiple control system failures, multiple utility failures, or a combination of both.

Surveillance of the industrial sector that handles hazardous chemicals is insufficient to draw detailed conclusions regarding the totality of the sector's Y2K compliance efforts.

Special workshop attendees reached consensus on the importance of four issues related to Y2K problems: First, small and medium-size enterprises' risks and needs are greater than those of larger corporate entities; second, existing risk management programs provide the most substantial framework for addressing this issue; third, the discontinuity of utilities threatens all chemical handling entities; and, fourth, management of Y2K problems will require responsive communication among the stakeholders.

Limited research indicates that large multinational companies are, in general, following well thought out and well managed paths toward Y2K compliance. These have, in addition to their Y2K compliance efforts, made extensive contingency plans, including in some cases plans to shut down batch operations for limited periods at the turn of the century.

The CSB conclusions vis-a-vis large and multinational companies should not be construed to mean that there is no potential for Y2K-related catastrophic events at these facilities. Some Y2K impacted components may not achieve 100 percent completion. Multiple failures may not have been considered and may result in accidents, and in addition, the erosion of commodity pricing, merger and acquisition activities, loss of critical Y2K staff for 1999, may create unique threats to the successful completion of the Y2K project.

In summary, I would like to say that given the time constraints, altering this situation requires a massive effort. Much work has been done to date. The Board has concluded that these efforts should focus on, one, providing easy-to-use tools; two, promoting accessible resources; and, three, providing attractive incentives for Y2K compliance.

I would be happy to answer your questions at an appropriate time.

[The prepared statement of Mr. Poje can be found in the appendix.]

Chairman BENNETT. Thank you very much.

Mr. Frodyma.

**STATEMENT OF FRANCIS J. FRODYMA, DEPUTY DIRECTOR,  
POLICY DIRECTORATE, OCCUPATIONAL SAFETY AND  
HEALTH ADMINISTRATION**

Mr. FRODYMA. Thank you, Mr. Chairman, and thank you for this opportunity to appear today to describe the Occupational Safety

and Health Administration's efforts to protect workers in the chemical industry. Before I discuss what we are doing with the Y2K issue, though, I would like to just spend a minute to talk about OSHA and who we are.

OSHA's core mission is to provide a safe and healthy workplace for every working man and woman in Nation. The language in our statute is very broad. It requires the agency to set standards and conduct inspections at over 6 million workplaces employing more than 100 million Americans.

This statutory responsibility covers all industrial sectors, including manufacturing; construction; longshoring; yes, chemicals; health care; retail trade; and many service sectors. The Act also allows States to operate their own OSHA-approved safety and health programs, and 25 States and Territories have elected to do so.

With regard to OSHA and the chemical industry, OSHA has been particularly concerned about the chemical industry since the mid-'80's, since the Bhopal, India catastrophe. And yet despite this impression created by a catastrophic accident and releases and other high publicity events, that this is a dangerous industry, from an occupational safety and health perspective, the overall injury/illness rate for the chemical production sector is substantially below the national average. Therefore, the chemical industry has not been to date targeted for OSHA programmed inspections.

However, OSHA does recognize that there is a continuing need to address the risk of catastrophic accidents in this industry, including those that might be caused by unsafe operation and/or equipment failure due to the Y2K problem. And, indeed, OSHA enforces numerous safety and health standards applicable to the chemical processing industry. The most important one to the Y2K issue is our Process Safety Management standard, or as we call it, PSM.

PSM requires employers who possess a threshold quantity of any substances on a list of highly hazardous chemicals to assess the risks posed to workers and to develop a plan for mitigating those risks. The employer must, as part of a hazard analysis, assure process safety by conducting an evaluation and controlling the associated hazards created by the technology (e.g., Y2K) of the process itself. Therefore, under this rule, employers now have a responsibility to assure that the effects of the Y2K problem on any such equipment or controls are appropriately managed.

However, for OSHA to rely solely on enforcement of regulations through PSM inspections to assure Y2K readiness is not practical, in part for the following reasons:

First, coverage. Whether a facility is covered by a PSM standard depends on the quantities and types of highly hazardous chemicals on their site. Coverage is not always determined by an industry or an SIC code. Thus, there are many facilities outside the chemical industry which are covered by process safety management, and some facilities within the chemical industry that are not covered. So many chemical facilities potentially facing Y2K compliance issues are, strictly speaking, not covered by the rule; and many covered facilities that do not engage in the type of processing activities considered at most risk of Y2K complications are covered.

The second reason is that for OSHA, process safety management inspections are complex and time-consuming. A quality process safety management inspection by OSHA takes over 4 weeks. In addition, OSHA just has a few inspectors with the necessary training and experience to conduct PSM inspections.

Therefore, OSHA must target—moreover, OSHA's inspection force of 2,000 compliance officers is responsible for, as I said, the 6 million establishments. Therefore, our agency must target its resources at the most dangerous workplaces, as indicated partly by the higher than average injury and illness rates. As I mentioned earlier, the chemical industry has a substantially lower than average injury/illness rate, and OSHA could not conduct a program of Y2K inspections at PSM-covered workplaces without diverting limited enforcement resources from industries where workers face a much higher probability of death or injury.

Therefore, OSHA has concluded that the existing regulatory framework will not effectively deal with the Y2K problem. Instead, we feel that it can be most effective in addressing this problem through a compliance assistance approach that involves outreach and dissemination of education materials. This is the approach that was also suggested by the Chemical Safety Board in its March 1999 report to your Committee.

As part of our efforts, I would like to mention quickly a few of the steps we have taken. In September, 1998 we published a fact sheet entitled "How the Millennium Bug Can Affect Worker Safety and Health." The sheet lists possible failure conditions and identifies specific hardware and electronic devices that should be evaluated for possible errors, and that fact sheet has been available through OSHA's web site since December 1998.

We have also begun dissemination of information to high hazard employers, and last month OSHA mailed letters to 12,500 employers with the highest injury/illness rates in the Nation, alerting them they need to take action to improve their safety record. We included the Y2K fact sheet in that mailing, which was also sent to 1,200 companies who use chemicals in high volume, such as those in the chemical, printing, rubber and paper industries.

We also conduct about 32,000 inspections annually, and in each of those inspections our compliance officers now distribute Y2K fact sheets to all employers after every inspection, regardless of the industry inspected. Also, those fact sheets have been made available to State inspectors, who conduct an additional 60,000 inspections.

And then, finally, our OSHA consultation programs, which operate in all 50 States, have also been distributing the Y2K fact sheet, and these consultants visit more than 20,000 workplaces annually.

Mr. Chairman, in conclusion I would like to say that OSHA thinks that we can most effectively address the Y2K problem through aggressive outreach and education efforts, and we will continue to distribute information and additionally seek new ways to spread the word about the need for every employer to seriously and thoroughly consider how Y2K affects the health and safety of their employees.

Mr. Chairman, I would be happy to answer any questions, at your convenience.

Chairman BENNETT. Thank you.

Mr. Couvillion.

**STATEMENT OF PAUL COUVILLION, GLOBAL DIRECTOR,  
DuPONT YEAR 2000 PROJECT**

Mr. COUVILLION. Good afternoon, Senator Bennett. My name is Paul Couvillion, the Global Director—

Chairman BENNETT. Couvillion, I apologize. I apologize for mispronouncing your name.

Mr. COUVILLION. That is quite all right, sir.

I am the global director for DuPont's Year 2000 Project. Thanks for inviting me this afternoon to discuss this very important issue.

DuPont has made some formal disclosures through the SEC, and today's statement will not be covering those again. The data that I have, contained in the statement that was sent to you, are up-to-date data as of the end of May, and I want to ask that you use this statement in conjunction with those earlier disclosures.

I have worked for DuPont for 35 years and was appointed to lead this global effort almost 2 years ago. I was selected to lead this work because of my experiences in leading people and in managing manufacturing processes in a number of DuPont's businesses.

The remediation of Year 2000 issues in our plant process control systems, computer hardware, applications software, embedded chip equipment, and in our suppliers' and customers' systems, is very important to DuPont. Based on our current plan, we should have more than 98 percent of our critical and significant computer systems Year 2000 capable by the end of June, with the remainder completed by year-end.

DuPont has been in business for almost 200 years. We are a world leader in science and technology with a range of disciplines and products, including high performance materials, specialty chemicals, pharmaceuticals, and biotechnology. DuPont's 93,000 employees are dedicated to bringing science to the marketplace in ways that benefit people and generate value for our stockholders.

This project is one of the top corporate initiatives identified by DuPont's president and CEO, Chad Holliday. We have proactively addressed Year 2000 issues since 1995. We have established two key goals for the project. The first, consistent with our commitment to continuously improve our safety performance, is to prevent safety, health or environmental incidents that could occur as a result of the Year 2000 problem. Second, we want to maintain the continuity of our businesses and service to our customers, employees, stockholders and communities.

This task has required mobilizing employees around the globe. The DuPont Year 2000 project consists of more than 40 teams and about 2,000 people from businesses, regions and functions that comprise the company worldwide. These teams work together with our information technology partners, Computer Sciences Corporation and Anderson Consulting, who operate the majority of DuPont's global information and technology systems infrastructure.

The Company's approach to the Year 2000 challenge, as shown in the written statement, involves the use of a multiphase process being used by many companies worldwide. This process is being applied through a large and diverse range and number of systems

that are connected in complex and extensive networks across businesses and regions.

Our Year 2000 project is managed centrally with a small, diverse team of experienced people. The work is executed locally within each business unit, function and region. Corporate direction is provided by our Operating Group, who receive updated biweekly. My team reports to an Executive Steering Committee every month, and the role of my team has been to develop and provide common technology and processes for the project, to monitor business unit progress against those goals, collect metrics, hold periodic reviews, and provide support to unit projects.

We estimate total expenditures to become internally capable to be in the range of \$350 to \$400 million, and through March 1999 we have expended \$225 million or about two-thirds of our 4-year estimated expenditures.

DuPont has more than 80,000 suppliers and 20,000 customers, with 150 joint ventures around the globe. A business partner work stream was established to develop an informed view of the readiness of more than 5,000 critical suppliers, 2,000 key customers, and all of our joint ventures.

About three-fourths of the suppliers that we surveyed responded. Of those assessed, 15 percent have potentially—will potentially create interruptions to the continuity of supplies or services to our value chain. Key reasons for our concerns are “no response,” “no program in place,” “late completion,” or “no supplier assessment in place.” We have initiated and have almost completed four special emphasis surveys aimed at key infrastructure operations, shown in the written statement. The initial conclusions indicate that we are likely to experience a low probability of failure among these groups of infrastructure providers. However, we found in some specific areas around the globe where we could have services interruptions and contingency plans may be required.

About half our customers surveyed responded. Of those responding, we have assessed 33 percent as potentially creating interruptions to our business processes.

In regard to the assessment of critical suppliers and customers, we rely heavily on and trust what we are told about their Year 2000 readiness. As a result, we cannot guarantee the readiness of any of our companies external to DuPont’s operations. At best, we have been able to create informed judgments.

In summary, this project is critical to DuPont’s success. We have committed the necessary resources to get this work done on time. From this work we have learned and gained much from this large global project. We intend to meet our goal of safe, continuous operation through the millennium.

At midnight on December 31, 1999, the world—companies, governments, and institutions—will be given a test. I don’t know about you or others in this Year 2000 class, but each time I take the test, I get a little nervous and anxious. We have done our homework, have taken reasonable approaches, and I believe we have prepared ourselves well for this final exam. There are no guarantees that we will succeed, but because of the extensive work we have committed and done for Year 2000, we expect to get an A for both our effort and our results.

Thanks for the opportunity to appear this afternoon.

[The prepared statement of Mr. Couvillion can be found in the appendix.]

Chairman BENNETT. Thank you very much.

Mr. Schleck.

**STATEMENT OF JAMIE SCHLECK, EXECUTIVE VICE  
PRESIDENT, JAME FINE CHEMICALS**

Mr. SCHLECK. Chairman Bennett and members of the committee, I would like to thank you for this opportunity to come and speak before you about this very important topic. My name is Jamie Schleck. I am executive vice president of Jame Fine Chemicals, a specialty chemical manufacturer, family owned. We have approximately 44 employees. We manufacture products for the pharmaceutical, cosmetic, dietary supplement, chemiluminescent, and disinfectant industries.

I myself am a software engineer, and I have spent 6 years in general management of this company. As such, I feel I have a unique perspective on this issue, as well as the industry dynamics of companies in the same roles that Jame Fine Chemicals is in.

I would like to talk to you first about these industry dynamics. I will then talk to you about the specific Y2K compliance efforts that Jame Fine Chemicals has undertaken. I will then talk to you about the exposure that I have identified within my company, which I think may be indicative of other companies also in the same roles as Jame Fine Chemicals. And finally, I will talk about industry initiatives which we have—which have been brought to bear on companies such as my own, and the impact that they have had in terms of Y2K compliance.

First, the industry dynamics: What I have found in reading some of the reports involved in—concerning the chemical industry, there seems to be a lack of understanding of batch processing versus continuous process. Batch processing involves the intermittent use of raw materials in the production of chemicals, as opposed to continuous processing which has a continuous input and a continuous output of manufacturing of chemicals.

As you stated earlier, one of the major dangers that could be identified from Y2K is the startup and shutdown of processes. At Jame Fine Chemicals we startup and shut down processes every day as a matter of normal business. Batch processing provides for flexibility and low-cost manufacturing of these products.

If I could draw an analogy between the types of specialty chemicals that my company manufactures and commodity chemicals, specialty chemicals could be considered like diamonds, whereas commodity chemicals would be compared to coal. As such, automation usually is not cost-effective for companies such as my own.

The reduction of labor costs and cycle times clearly has a second order effect when compared to yield management and the importance of maintaining tender loving control over the process. We have highly skilled operators, many of whom are paid more than \$30 an hour to operate our processes.

I would next like to talk about Jame Fine Chemicals' specific Y2K compliance initiatives. We began examining the Y2K compliance problem in 1997. Our process involved assessment,

prioritizing those processes which could be affected by Y2K, remediation, and finally, implementation of our compliance initiatives.

What we did was, we identified every process that could be remotely affected by embedded chips, by software-related intrusions into the process, as well as anything that would be affected by any kinds of Y2K compliance issues. We then began prioritizing those specific problems that we saw, and then we began implementing a program to eliminate Y2K compliance problems.

We expect that by June 30th of this year we will have completely ruled out any problems of Y2K compliance. As of today, we have two issues which are not Y2K compliant. One is a process controller on a freeze drying operation. The second is our phone system.

Next I would like to talk to you about some of the exposure that we have identified throughout our Y2K compliance issues. As many chemical companies have already identified, we are of course very dependent upon utilities—electricity, gas and water. It will be important for us, at the coming of December 31st, 1999, to ensure that we are not engaged in any processes which are dependent upon these utilities.

Additionally, we feel that there could be some exposure in terms of raw material availability. Again, on December 31st we will not be manufacturing any processes for which we do not already have raw materials in store.

Again, I mentioned that our phone system was something which was not Y2K compliant, but we do not consider this to be a critical business function, as we could just go back to using a normal phone system or roll our clocks back so that voice mail will again be usable.

There have been several industry initiatives that also have brought this important topic to light for companies such as my own. "Responsible Care" by SOCMA; software validation, which is brought forth through cGMP compliance, and also insurance compliance. It was important for us this year, when we did our annual insurance review, that the Y2K statements were up-to-date and were identifying all possible risk to our insurance company.

In conclusion, I would like to say that I feel that companies in the industry that I am in and in the role that I am in have limited exposure to Y2K problems because of the dynamics of the industry.

I will be happy to take your questions. Thank you.

[The prepared statement of Mr. Schleck can be found in the appendix.]

Chairman BENNETT. Thank you all very much. I at some point would like to get Mr. Schleck and Mr. Couvillion into a conversation about the large and the small and some of the contrasts and complementary activities that you get involved in chemical manufacturing.

Let me start with you, Dr. Poje. Throughout your statement you focused again and again on the small and medium-sized enterprises as the area where you either have the least information or where the most remediation needs to be done, and this of course is a concern that the committee has.

In general terms, we find on the committee that the people who are willing to come testify to us, regardless of what the situation is, are the people who are in good shape, and very often then there



is a tendency to extrapolate into the unknown area the good results that you have out of the known area. I think you have appropriately said we can't do that.

We can't at the same time extrapolate bad assumptions into the unknown area, but I think we would be terribly naive if we assumed that everybody who didn't report was in the same shape as those who did report.

So do you have any thoughts—or any of the rest of you, chime in on this, even though I am focusing it with Dr. Poje—as to what we could do to increase our information for the small and medium-sized enterprises that have not reported, either through their trade association or their regulator or to your inquiries, as to where they are?

Mr. POJE. Senator, thank you for that question. We are very concerned about the small, mid-size enterprises because we want them to succeed in this area as we do in other areas. The Board has to confront, unfortunately, terrible tragedies that have occurred in the last year or so involving such entities.

In March of this year we had to begin an investigation into a small company in Allentown, Pennsylvania that was manufacturing a material called hydroxylamine. In preparing a more purified solution of this chemical, something went awry in the process. The situation resulted in a catastrophic explosion. Four workers were killed inside the plant. One worker was killed in a business nearby. Eleven buildings were damaged in the area, and the explosion was felt 15 miles away, throughout Allentown.

It is unlikely that such a small, mom-and-pop operation would be part of an association. So, yes, we have worked with associations, we will continue to try to work with associations to build models of performance that could be useful for all such entities. I think the characterization by Mr. Schleck of the difference in scales are very important issues that need to be addressed by all such entities.

We would welcome other associations, in addition to the Chemical Manufacturers Association, to provide such examples of how to deal with specific Y2K related problems that are likely to be had in common across such small entities. Smaller businesses lack the large corporate communication structure which allows for learning to be disseminated from one facility to another, such as might happen in a very coordinated program described by Mr. Couvillion.

The Board would like to see is an acceleration of surveillance efforts so that we would have a better picture on the membership and how they are complying. However, we also would like to see additional models developed within each of those associations that could be used as examples to others within or outside the association, identifying how facilities can address contingency planning and compliance efforts that are effective throughout the rest of this year.

Chairman BENNETT. Mr. Schleck, you are the closest thing on the panel to a mom-and-pop operation, only you have grown to sisters and cousins and aunts, and far beyond just mom-and-pop, but do you have any comment at all as to how we might reach some of these small operations that Dr. Poje is talking about?

Mr. SCHLECK. Well, I would first of all characterize us possibly as a mom-and-pop operation, certainly a pop-and-son. My father is still active with the business.

Chairman BENNETT. Well, OK. Is it named after you?

Mr. SCHLECK. You know, people always ask me that, and his name is James, and it was started at the time that I was a young child, so possibly. It is commonly confused, though. I think that—

Chairman BENNETT. Be like the politicians. Take credit for it anyway.

Mr. SCHLECK. I shall. One thing that I think is critical for anyone involved in industry such as the chemical industry is to have adequate operating procedures which would rule out any kind of catastrophic events as we saw in Allentown. One thing that we have is a hazard operations procedure which runs down all the selected "what if" scenarios, which include the failure of utilities, the interruption of gas or water supply.

As I recall from reading about that incident, that was a company that had really just started, and they probably did not have the types of operating procedures that were—that are necessary to operate in this business. That being said, I think that it is important for industry trade associations to identify, through initiatives like "Responsible Care" and cGMP, which is actually an agency compliance issue with the Food and Drug Administration, to ensure that companies such as the one in Allentown, such as Jame Fine Chemicals or other companies, are in fact implementing and following those important operating procedures.

Chairman BENNETT. Mr. Frodyma?

Mr. FRODYMA. Yes, Mr. Chairman.

Chairman BENNETT. You spoke about the dissemination and distribution of your fact sheet. I have a fact sheet, single page. Is this what we're talking about?

Mr. FRODYMA. Yes, Mr. Chairman.

Chairman BENNETT. Well, I don't mean to make your afternoon uncomfortable, but this is woefully inadequate. There is nothing here that you couldn't pick up from the Sunday supplement in terms of information.

EPA has a four-pager which incidentally has in one small box what you take half a page to cover, and they just tuck it up there, with more information, web sites, addresses, a lot of alerts and so on.

Mr. FRODYMA. Well, we have also distributed other web site material to our—the groups that I mentioned in my testimony. The President's Y2K web site, which discusses the chemical industry, we have mentioned. We have also distributed to the small and medium-size—we are targeting the small and medium-size establishments. The SBA's web page, which has a lot more information on it which is more detailed.

But in addition to just the fact sheet, we have also had discussions with our managers about not just the information on the fact sheet but what they can talk to the employers about when they do visits. So we haven't—although the fact sheet, the document, we have also had discussions with the managers about how to use the fact sheet.

Chairman BENNETT. Well, again, there are very few facts on the fact sheet. If I might, if it doesn't offend your sensibilities to use another agency's information, here is the EPA "Prevent Year 2000 Chemical Emergencies." It describes the problem in greater detail than yours does, then goes on to: your software, your process control equipment, your service providers, hazard awareness and reductions. There is a box on some dates to watch. A lot of people don't realize that the first of January is not the only date that is affected, and there are a series of dates here, leap year and so on. Steps to address the problem, remedy, test, develop, so on.

Then here is the box with the items that are on your fax sheet included, and then a full page of information resources, Y2K freeware and shareware, national bulletin board for Year 2000, National Fire Data Center. I am just reading a few of them. Here is the President's Council on Year 2000 conversion product, compliance information, Chemical Manufacturers Association survey, and so on.

Again, I realize that Federal agencies (and I have worked in one before I came to the Senate, I served in the executive branch) get very jealous about turf, but I would suggest that simply reprinting this from EPA and putting it in your distribution channel would be very, very helpful.

I have seen the material put out by the Small Business Administration. It is not tailored to the chemical industry, and simply would help somebody deal with his billing or payroll kinds of problems. But I think something more than what we have seen under the banner of OSHA should be distributed through the OSHA network, because you have the largest network of anybody at the table.

Mr. FRODYMA. Well, we certainly can use the EPA's fact sheet. In fact, we have—our people have worked with EPA on development of their fact sheet and we can easily see that the EPA's material is also made available through all of our sources. It is a very good suggestion.

Chairman BENNETT. Thank you. I will look forward to see what goes on.

OSHA has perhaps the highest visibility in manufacturing of any Federal agency. I remember walking into a company that had a little sign on the window that said, "If you think OSHA is a small town in Wisconsin, you are in real trouble." So everybody is aware of you, and you can be of great help in getting more detailed information. And not to beat up on you personally, but the single page fact sheet that we have a copy of is, in our opinion, inadequate.

Dr. Poje, you want to get in?

Mr. POJE. Senator, if I could just chime in here, one of the recommendations from our Board's report was to have a high level Federal meeting coordinated through the President's Council on Y2K. I think this would be a way in which such information could be shared very expeditiously between agencies, and could maximize the impact of such common information. OSHA's reach is quite impressive. EPA has a similar reach but maybe in a different angle. There are other research entities, such as the National Institute for Occupational Safety and Health, which are working on Y2K.

That recommendation, which has yet to be acted upon, that the President's Council coordinate such a meeting. We could invite the associations, who also have a very important perspective on how to reach their members, and work expeditiously, in coordinated fashion, to make the message heard.

The Health and Safety Executive in the United Kingdom has produced a number of informational resources specific to health, safety and environmental protection. I think that these provide strong models for us to examine and adapt for an approach that is useful here in the United States.

Chairman BENNETT. Thank you. John Koskinen, who chairs that effort on behalf of the President, he and I talk every week, and I will mention that to him this week. I always tell him what comes out of these hearings, and he tells me what he is doing, and this is one that I can pass on to him as a very specific suggestion.

Yes, sir, Mr. Couvillion?

Mr. COUVILLION. Thank you, Senator. I had four thoughts, the first one of which, even though my name is French, I did not invent the company, though I do believe I made a contribution to it over my years of time. So just a little bit of an aside here.

I guess the four thoughts I had were, No. 1 is that we have 135 plant locations or site locations around the world. Among those sites, we have some 320 operations, a significant number of operations. We found that the only way to manage such a large operation is to leverage it on a global basis and to communicate daily, if not weekly, on the successes, the learnings, and the findings.

And so the idea would be, for example, a small plant might have 40 people in it, a large plant of ours might have 3,000 people. So the idea of leveraging among multiple site locations within a given industry, be it a small company industry, would have a high value I believe for those companies sharing information about their findings, their learnings, and their application to Year 2000, all the way into the contingency planning processes. So if you can model what we do at our plant sites around the globe, it would be a very, very critical piece of success.

The second area deals with process safety management. I think clearly process safety management forces you to think about Year 2000 not as a device that might fail, but within what system does it fit, and are we doing the necessary testing and integration work that is necessary to create success? And a sound process safety management process, built upon for Year 2000, is another way of assuring success in the business. So I think to me a recommendation would be to have very strong views of process safety management, as Dr. Poje has already spoken about, I think are really key to that whole process.

I think the third area of value for us has been a learning that with the Chemical Industry Technology Alliance, a group consisting of about 60 large Fortune 500 companies, we participate on a quarterly basis in reviews. We will get groups of suppliers to come in and share what they are doing to the whole industry. We will get the power providers to come in and share what they are doing as a key learning. So if there is some way to create an alliance of small businesses to get together to listen to large providers, telecommunications, power industry providers and so forth, would be

another key value. I don't know if such an industry, small industry forum, exists today.

I think the last one would be to create an open sharing of information, so the fear of litigation, the fear of legal barriers doesn't stand in people's way to get this work done. Maybe an extension to the current disclosure act might be a valued thing, and the CMA work we have done in creating a supply chain pledge, where people sign a mutual pledge in this process, to commit the effort and energy to get this work done, might be a way to sort of cap it off and put the icing on the cake.

So those are four suggestions at least that I think about in the learnings we have had in this project.

Chairman BENNETT. We appreciate that. We have tried to facilitate the exchange of information with the legislation that Senator Dodd and I passed, or convinced the Congress to pass, last year. Unfortunately, we have not seen as much exchange of information as we had hoped. Not to slam your companion there, but the legal departments of many companies have said, "Well, the law notwithstanding, don't tell anybody anything. That's the safest way to go."

Mr. COUVILLION. I join you in that.

Chairman BENNETT. Yes. Let me ask you a tough question, but you mentioned it in your opening statement and I think you might want to elaborate it a little more. You say you are over 90 percent there?

Mr. COUVILLION. Ninety-eight percent.

Chairman BENNETT. Ninety-eight percent there, but you have spent only two-thirds of the money.

Mr. COUVILLION. We are finding—

Chairman BENNETT. Does that mean that you have left the really tough part still to do, or that you got it done much, much cheaper than you anticipated? If it is the latter, then you are the only company that I know of in that situation.

Mr. COUVILLION. We are finding that we are in the labor-intensive part of this work today. Our spend rate is pretty high right now through the summer months. And I think, second, that we are in fact seeing ourselves spending less money than we originally estimated in this project.

Now, those are the two fundamental reasons for this. We are going to spend it out. I had \$225 million. We have come a long way and done a lot of work. Particularly we found ourselves spending less capital than we originally anticipated to get work done.

Chairman BENNETT. That is surprising. Just about everybody else that appears before the committee ends up spending substantially more than they originally had thought, very much including the Federal Government. The initial estimates for the Federal Government were that we would spend \$2.5 billion. We are probably going to go over \$10 billion, and there are still parts of the government that are saying, "Gee, we could use a little more." Of course, they say that all the time.

Let me ask you one other question, Mr. Couvillion. Dr. Ed Yardeni, whom everyone who is connected with Y2K knows very well, looked at your disclosure, I don't mean to pick on you, but you're the only one available—and he said that 65 percent of your key suppliers were at a high risk of not being Y2K ready. You are

saying now that 15 percent of your suppliers are at high risk. Do you want to reconcile those two numbers, for anybody who may be watching?

Mr. COUVILLION. Sure. The data—we are constantly reviewing and looking at our status in this information—the data shown in the statement reflects current information, last week's state of the business in terms of our supplier relations process. The earlier data probably comes from the third or the fourth quarter report, I don't know which offhand.

What we have done is——

Chairman BENNETT. Is there any difference between critical suppliers and key suppliers?

Mr. COUVILLION. No, they are the same, one and the same.

Chairman BENNETT. OK.

Mr. COUVILLION. We have found that calling supplier forums, we have called entire groups, supplier groups together, to come to DuPont, to share with them what they are doing, and we have found a significantly greater openness in the last three to 4 months.

We have initiated face-to-face contacts with everyone in the infrastructure processes—transportation, shipping, telecommunications, the power industry, and the natural gas industry. We have called on each one of those on a face-to-face basis, and frankly we have found that that has paid off tremendous dividends just to go talk to people face-to-face, rather than depending on the earlier processes where we used a significant amount of written survey data and asked people to fill the blanks in and send data back to us.

So starting with telecommunications, open forums for both customers and suppliers, as well as getting these face-to-face discussions, has made a tremendous difference in the process for us.

Chairman BENNETT. Well, I think that is a significant contribution, because when we are dependent on surveys by trade associations, we miss a whole lot of folks. Mr. Schleck, do you have any thoughts as to where such a forum could be put together, that we could do the kinds of things that Mr. Couvillion is talking about.

Mr. SCHLECK. Well, I would like to just supplement his comments in saying that, as is the case, we supply as a specialty chemical manufacturer many large pharmaceutical companies such as DuPont, specialty chemical companies such as DuPont or Cytec or——

Chairman BENNETT. Are you going to ask him for an order, as long as you are here?

Mr. SCHLECK. No, but my point is that actually it is, as a business priority it is important for us to be Y2K compliant and show that to our customers, because this is obviously a competitive advantage and an important business function that we can play for our customers. So as DuPont has called in their key suppliers, we have also been questioned by some of our major customers about our Y2K compliance strategy and what our plans were.

Chairman BENNETT. One last question. As we look at this overall from the Senate point of view, we think the United States is probably going to be in fairly good shape. I don't have the same confidence at all overseas.

And both you, Mr. Schleck, and Mr. Couvillion, do you have foreign suppliers, raw materials or finished goods, that you are concerned about, that you have looked at as part of this? And do you share our concern that there is greater risk overseas, or do you think this is going to be all right? Mr. Schleck, we will start with you.

Mr. SCHLECK. As I mentioned before, we found that it is important for us to have an increase of our raw materials supplies come year-end. We are fairly dependent upon raw materials from other countries. We have audited those suppliers. We visit them usually on a yearly basis. This past year it has been somewhat more frequently.

And what I have found from many of these suppliers, again, there is a different industry dynamic from what is commonly associated with the chemical industry. There is much less automation, higher value products, so therefore certainly justifying the need for specialized labor and less automation.

The exposure that I see is in regard to shipping, customs clearance, those types of issues, and those may really have a nuisance value to us which can be mitigated by having the adequate raw materials supply at the end of the year.

Chairman BENNETT. So you are stockpiling?

Mr. SCHLECK. Yes. We are probably going to be increasing our base inventory by approximately 20 percent, which is about 1 month's supply.

Chairman BENNETT. OK. Mr. Couvillion?

Mr. COUVILLION. Yes. As I indicated earlier, we have about 5,000 critical suppliers, or key suppliers, if you want to call it that, of the roughly 80,000 we deal with. Now, that accounts for probably 90-plus percent of our purchases. Half of those suppliers are outside of the United States.

And so we have a process that is very similar to what we are doing here. We are going out, we are calling on people, we are talking to people in a very similar fashion. We have had very good success in our Asia Pacific region, very good success in our European region, and very good success in Mexico, for example, in getting data back from suppliers.

I think the aggressiveness and the energy which you put into it will determine the outcome of the process, and our view is that we have put a significant amount of energy because we view this as an absolutely critical part of our success.

We do have, as I indicated in the statement, some 15 percent who we are not comfortable with. We are going to go out and, in fact, have contingency plans. Our intent is not to build inventory. The belief on our part is that it is critical from a quality point of view to get the work done, not to put inventory in place. Although we don't discount it, we see some view of being able to get at that.

Now, we are looking at direct suppliers only in this particular case, not those further back in the stream. At least it gives us very strong comfort about where we are.

Chairman BENNETT. You are not stockpiling. Are you going to change any suppliers if you decide they are not going to be ready? Are you going to cut them off for future?

Mr. COUVILLION. We have that as one of our contingencies, and we have a group of suppliers we call mission critical, limited alternatives, that we look at. And in those cases we are going to find a way, if we can't get business, we will find alternatives to do that. We have not pulled the trigger on doing that yet, though.

Chairman BENNETT. OK, fine. Let me thank you all. This has been a very informative panel, and I have enjoyed the discussion as well as your opening statements.

We will now go to the second panel. We have Mr. James Makris, who is the director of the Chemical Emergency Preparedness and Prevention Office at EPA; Mr. Charlie Martin, he is the safety coordinator for Hickson DanChem Corporation in Danville, Virginia. We appreciate Mr. Martin's coming up here to emphasize that this is a problem we must be concerned about across the Nation.

We have Ms. Paula Littles, who is the citizenship and legislative director of the PACE International Union; Lt. Col. Michael Fedorko, the state director of the New Jersey Office of Emergency Management; and Ms. Jane Nogaki, who represents the New Jersey Work Environment Council and the New Jersey Environmental Federation.

So we appreciate all of your being here. Let's see. I introduced Mr. Makris first, but Mr. Martin, you seem to be on the far end, so let's go down in the physical order in which you are seated and start with you, Mr. Martin.

**STATEMENT OF CHARLIE B. MARTIN, JR., SITE SAFETY  
DIRECTOR, HICKSON DANCHEM CORPORATION**

Mr. MARTIN. Yes, sir. Good afternoon, Chairman Bennett. My name is Charlie Martin, and I am the site safety coordinator at Hickson DanChem Corporation. I would like to take this opportunity, if I may, to introduce Mr. Jonathan Miels, to my left, who is our information systems manager at Hickson DanChem, and he has also been our prime leader in our Y2K compliance efforts.

I thank you for inviting me today to appear before you and this distinguished panel. Although our company is not physically located in New Jersey, the issue we are discussing here today does not vary across State lines. I am here today to present my industry's perspective on Y2K contingency planning from both inside and outside the company fence.

Hickson DanChem is engaged in custom manufacturing of organic and inorganic specialties for major chemical companies. It also produces a comprehensive line of textile chemical auxiliaries and specialty surfactants. In layman's terms, we make the chemicals that are used for fabric conditioning, paint additives, and personal care products. The company employs 132 persons at our plant in Danville, Virginia and uses batch manufacturing processes, which is inherently different from the continuous operations.

As the site safety coordinator, I serve on the Y2K compliance team. Since the last panel addressed Y2K initiatives generally, I will focus my comments on the last step of Y2K preparation, which is contingency planning. It should be noted that our company will be Y2K compliant on June 30, 1999.

In developing the final draft of our emergency contingency plan, Hickson DanChem tried to foresee every possible situation, how-



ever remote. Our plan covers safe process operations, emergency response planning, and community dialog.

As Hickson DanChem conducted its Y2K assessment, employees played a critical role. In fact, employee involvement is not unique to Y2K safety activities. Recognizing that their contribution is paramount to a successful employee health and safety program, we have always included our employees in developing safety plans and procedures.

This involvement enhances our compliance with Federal regulations such as the Occupational Safety and Health Administrations Process Safety Management or PSM rule and the "Responsible Care" code guidelines. Coupled with regulatory requirements, these guidelines address many of the potential results of Y2K technology problems.

Some specific activities at Hickson DanChem that our employees play a dynamic role in are our formal Site Safety and Health Committee, which is comprised of eight task groups. These groups participate in various areas of our safety program. They also perform hazard assessment audits. We hold monthly shift training sessions on related OSHA and regulatory topics; departmental safety meetings, which are also held monthly; and 5-minute supervisor safety talks that are performed daily.

Hazard/Operability or HAZOP studies are performed on new and existing processes, and include recommendations for corrective actions that will preclude potential failures. HAZOP action items result in decisions such as installing emergency shutdown devices in conjunction with process control systems.

Regarding specific impacts of Y2K, our onsite Y2K assessment team performed evaluations on business information systems, process control systems fire and security systems, field control units, and QC lab equipment. During the roll over period of December 31, 1999 through January 1, 2000, provisions were considered for a phased startup of utilities, system checkouts, and status verifications with the emergency response agencies before manufacturing processes are resumed.

Another important aspect of an effective safety program is involvement with local emergency response teams and participation with local emergency planning committees, better known as LEPC's. Hickson DanChem participates in the Pittsylvania County LEPC by providing technical expertise in the planning process, assisting with training of local responders, and hosting regular plant tours and emergency response drills for local responders.

In fact, we had a major emergency response drill on March 11, 1998, in which Y2K related issues were addressed. The drill was noted as being the first of its magnitude in our area. Since that time, lessons learned have enabled us to identify potential challenges and make continuous improvements in our system.

Because of strong involvement in the county LEPC, we were chosen to serve on the city of Danville Emergency Planning Committee, as well.

As you can tell, handling chemicals has led the industry to develop extensive plans to address potential incidents covering both onsite and offsite consequences. However, Y2K presents a unique set of potential consequences, such as potential multiple system

failures. As such, our emergency response plans designate actions to be accomplished should these type situations arise.

Communicating Y2K compliance with your local community establishes public confidence and provides opportunities for open dialog between the community and the plant. Several of our customers, suppliers and business support agencies have requested and been provided information on our Y2K progress.

Our information systems manager participated in a Y2K drill with our regional medical center. The drill proved beneficial for both Danville Regional Medical Center and Hickson DanChem. Participation in the Pittsylvania County Safety Roundtable provides vital information to small industries on topics such as risk management plan or RMP preparations. A seminar hosted by the Danville LEPC was held on April 29, 1999, to further explain RMP requirements. Hickson DanChem also sponsors programs such as Educators in the Workplace, which provides awareness information to local teachers and guidance counselors.

In conclusion, Hickson DanChem is committed to having an effective emergency response plan that avoids the potential Y2K technology concerns. Many of the contingency planning activities for Y2K readiness in the chemical industry are already being addressed through procedures and practices. However, Hickson DanChem has added additional measures to ensure the safety of our employees, neighbors, environment and equipment come December 31, 1999 and January 1, 2000. The involvement of our employees and local emergency responders has led us to develop an effective and open community dialog and on and offsite contingency plans.

Mr. Chairman, we appreciate the opportunity to appear before you today. The Y2K issue warrants the collaborative efforts of all stakeholders before you today. We welcome your leadership and look forward to a transition to a safe and prosperous new millennium. Thank you very much.

[The prepared statement of Mr. Martin can be found in the appendix.]

Chairman BENNETT. Thank you.  
Mr. Makris.

**STATEMENT OF JAMES L. MAKRIS, DIRECTOR, CHEMICAL EMERGENCY PREPAREDNESS AND PREVENTION OFFICE, OFFICE OF SOLID WASTE AND EMERGENCY RESPONSE, U.S. ENVIRONMENTAL PROTECTION AGENCY**

Mr. MAKRIS. Thank you, Mr. Chairman. My name is Jim Makris, and I am at the Environmental Protection Agency. It is really a pleasure, a terrific opportunity, to be here, share some of these views with you.

I also would like to make a comment to Paul Hunter, who has been a terrific aide to I think all of the Federal agencies as we have worked through some of these processes. He has just been a terrific ally and a supporter.

Within EPA—

Chairman BENNETT. On his behalf, I will thank you.  
Mr. MAKRIS. Pardon me?

Chairman BENNETT. On his behalf, I will thank you for your kind comments.

Mr. MAKRIS. Well, I know he wouldn't say that himself, but within the agency my responsibilities are to be the emergency coordinator of EPA, which covers a wide variety of difficult and technical tasks. I am also responsible for managing the Chemical Emergency Preparedness Program and right-to-know programs as they relate to chemical accidents. I am accompanied by Oscar Morales, the associate director of the Information Management Division in TSCA, who has the Toxic Release Inventory responsibilities, and Don Flatery, who is EPA's sector outreach coordinator for 2000.

Within our agency, as in most agencies, we have three basic tasks. One is to be sure that the agency's business will go on uninterrupted. It is a fundamental issue. The President said, "Do it." You wanted it done. So what we are doing is making sure that EPA's systems are in good order, and I think we have gotten an A from some of the committees that have rated us and from OMB. We didn't start there, but we are there now.

The second responsibility that we have is to deal with sectors that have been assigned to us, one of which is the chemical industry sector which we are talking about today.

And then of course the third obligation we have as an agency is, if things go wrong, if there are accidents involving chemical releases or other releases, is EPA ready to meet its emergency response responsibilities which, in conjunction with the Coast Guard and the other Federal agencies, we have carried out for so many years dealing with hazardous materials and oil spills.

But we are the agency with the responsibility for ensuring that the environment and the public are protected from the unreasonable risk of toxic chemicals. We identify hazards in the environment, regulate their use, assess the risks of release to public health, and indeed deal with prevention programs.

Following the world's largest chemical accident in Bhopal, India, which has been mentioned by several people including the Chairman, Congress passed a law which required EPA to work closely with industries to participate in emergency planning, to notify their communities of the existence of releases, and to allow local communities to enhance emergency preparedness and accident prevention.

I think it is very important to note that that law moved things in a different way than a lot of previous regulation around industry that EPA was managing. It changed the paradigm from complete command and control to a recognition that communications was critical.

Senator Lautenberg, I wish he had been here today. He was a key part of passing this original Community Right-to-Know Act in 1986. But it is fundamentally against Thomas Jefferson's statement, where he said people are inherently capable of making proper judgments when they are properly informed. And I think that, you know, that is in all EPA's little brochures, but I think fundamentally it says that if you get information to the public and you create an environment and a forum in which they can communicate, the risk-taker with the risk-maker, progress will be made.

And I think that the Act created the Act of 1986 created a whole lot of dialog between the public and private sector, leading to reductions in risk on a voluntary basis by the chemical industry accompanied by exposure and disclosure and discussions at the local level. We also have, obviously, the Superfund law, and most all EPA environmental laws provide some emergency provisions to be able to move forward.

Based on our legislative authorities, EPA was asked by the Council to take responsibility for the chemical sector, and we felt that it could be well achieved within the legislative framework that the agency already had, and we stepped forward in that manner. We have taken a broad array of outreach activities in consultation with the chemical industry trade associations. The Administrator has asked that all EPA speakers talk about Y2K in any kind of issues with which they deal.

I thank you very much for the compliment on the fact sheet that we put out. It was an innovation to try in plain English to reach out and get as many words as we could to the private sector over what might go wrong. I also have to say that OSHA helped us to that, as did CMA and some others, so that we were clear, to put out a message that was understandable and that was in plain English.

I think EPA has—we have put a lot of tools in our toolbox that are useful to small and medium-size enterprise, and specifically with the case of the fact sheet, have distributed it broadly to LEPC's throughout the country, to State emergency response commissions. We submitted it to SBA, who are redistributing it to some of their constituents. And so we feel that that brochure, together with some of the other information that we have created, will be very useful indeed.

We work with CMA on the "Responsible Care" program—I am going to turn pages rapidly now. I think that in the matter of surveys, we are working hard to try to get the best input we can from the field. We keep being told by industry they are being surveyed to death, so we think that it is important to do some pointed surveys rather than any more of the broad surveys. We are getting to the—we are getting to a point now where we need specific information, not broad "How are you doing it?" But at the moment, the surveys seem to be showing that most people are doing a really terrific job.

Going to the end, I think that we are ready to deal with an emergency if it happens. We were part of the FEMA visit to 10 regional offices; EPA was on that podium. I personally was in both Philadelphia and Newark, New York, and also Atlanta. I understand that just today there was a meeting of 300 people here in New Jersey dealing with the Y2K issue, specifically around emergency management, but leading to the chemical industry.

I was reminded this morning of the importance, and Mr. Martin mentioned it again, of using the local emergency planning committees that were created by the Congress in 1980 and 1986 as an outreach mechanism directly to the community and directly to the industry, and to provide the LEPC's with questions that they can pose to the industry in their local communities about Y2K, just as we ask them to do that regarding chemical safety generally.

I guess in conclusion I would like to make it real clear that I am also the chairman of the National Response Team. We have a monthly meeting. The meeting always includes a Y2K discussion. We had full briefings by agencies. We have had DOE and HHS. We will have the other agencies presenting to us where they are in the emergency planning process during subsequent National Response Team meetings.

We, as you may or may not know, Senator Bennett, some companies were concerned with testing, that in order to test they might have a release. EPA found a way to allow a testing—"amnesty" is a peculiar word, but at least a testing flexibility, to allow moderate releases under certain preestablished conditions that would allow a company to take the risks of testing without having a Federal sanction.

And the last thing I would like to comment on is, the risk management planning process that we have under Section 112(R) of the Clean Air Act requires that companies meet their general responsibilities and general duties. The essence of our publication is to say, "Industry, you have a general duty to operate safely, and that includes Y2K." Thank you, Mr. Chairman.

[The prepared statement of Mr. Makris can be found in the appendix.]

Chairman BENNETT. Thank you.

Ms. Littles.

**STATEMENT OF PAULA R. LITTLES, LEGISLATIVE DIRECTOR,  
PAPER, ALLIED-INDUSTRIAL, CHEMICAL, AND ENERGY  
WORKERS INTERNATIONAL UNION**

Ms. LITTLES. Thank you, Mr. Chairman. Good afternoon. My name is Paula Littles, and I am the legislative director of PACE International Union. Our union represents workers employed nationwide in paper, allied-industrial, chemical or refining, and nuclear industries. Workers at these facilities are responsible for critical plant operations. They implement the contingency measures used during emergencies, from inclement weather to system failures to fires and/or explosions.

The Chemical Safety Board report released in March 1999 explained that "The Year 2000 technology problem is significant in the chemical manufacturing and handling sector, posing unique risks in business continuity and worker and public health and safety." We firmly believe that chemical workers, emergency responders, and local government agencies that focus on environmental and emergency response should be provided with training and tools to adequately address Y2K issues. Currently workers are provided training on contingency plans for single device failures, for example, loss of a boiler or loss of electricity or some other similar utility.

However, multiple device failure possibilities are not normally considered in the current process hazard analysis. It is unclear what the outcome might be due to such failures—possible multiple control system failures, multiple utility failures, or a combination of both.

Contingency planning for Y2K-related emergencies has to be designed and implemented with worker involvement—workers pro-

vide the day-to-day operations of these facilities, and they have the day-to-day operating knowledge—and should also be designed to include safe operations, safe shutdown, and emergency response. Any such planning must also take into account human factors such as appropriate staffing, hours of continuous work, rest intervals, and worker stress levels.

We have discussed this issue with the companies that employ our members at their facilities, and it is felt in our organization that a number of the larger companies are taking the Y2K problem seriously and are expending large amounts of resources to correct the problem. A number of these facilities have shared their concern regarding the reliability of their utility suppliers.

Petrochemical facilities have a great dependency on purchased utilities for their day-to-day operations. We strongly urge and encourage greater communications between utility providers and the facilities they serve, to ensure that each entity is doing their part in addressing this issue.

We are also very concerned with the small and mid-size facilities where we represent workers, and also where we don't represent workers. Unfortunately, we do not believe these facilities have the capability to expend the necessary resources to test the design and Y2K contingency measures for all of their systems and provide the necessary training for their employees.

We would encourage the companies that are ahead of the curve on their Y2K efforts to provide assistance to those that are not proportionately comparable. In the short period of time remaining before Y2K, we feel that this is one viable option to assist these employers that have been unable to adequately address this issue.

No matter what size the company, the Y2K issue could threaten worker and public health and safety. We would encourage companies to follow the proposed emergency response planning as specified in the Chemical Safety Board report through Y2K contingency planning on three levels.

Level one should address continued safe operations that include preplanning of actions that will allow the facility to continue to run in a safe and environmentally sound manner. Level two should address safe shutdown. This level of planning assures the availability of personnel, equipment, utility services, and other resources needed to ensure a safe shutdown of a facility. Level three is activated when contingency level one fails to ensure continued safe operations; and contingency level two fails to ensure safe shutdown. This will likely initiate a process safety incident.

PACE strongly believes that both employers and government agencies should designate worker representatives and include them in discussions regarding Y2K contingency planning, because ultimately workers will be the ones responsible for implementing these plans.

In conclusion, I would like to say that because of the lack of adequate planning for reaching Y2K compliance, contingency planning and worker training should be initiated immediately to build an emergency response infrastructure to respond to environmental disruptions, chemical releases, and worker public health and safety. Thank you, Mr. Chairman, for allowing me to speak to you today.

[The prepared statement of Ms. Littles can be found in the appendix.]

Chairman BENNETT. Thank you for being with us.  
Colonel Fedorko.

**STATEMENT OF LT. COLONEL MICHAEL FEDORKO, ACTING  
SUPERINTENDENT, NEW JERSEY STATE POLICE**

Mr. FEDORKO. Good afternoon, Senator. I am Lt. Colonel Mike Fedorko. I serve as the acting superintendent of the New Jersey State Police, and as State director of the New Jersey State Police Office of Emergency Management. Thank you for the opportunity to testify before the Senate Subcommittee on the Year 2000 Technology Problem.

In New Jersey, Y2K readiness is coordinated by Governor Christine Todd Whitman's office, resulting in a comprehensive, coordinated effort by all State agencies. The role of the State Police Office of Emergency Management in this process is to oversee and guide the activity of local emergency planning committees. LEPC members interface directly with representatives of chemical facilities in their communities on issues related to hazardous materials, emergency planning and emergency response.

Our State is home to nearly 1,000 chemical facilities that are regulated under the Superfund Amendments Reauthorization Act or the U.S. Environmental Protection Agency risk management rule. New Jersey's unique emergency management legislation mandates the establishment of a local emergency planning committee and the development of a State-approved emergency operations plan in every one of our 21 counties and 566 municipalities.

Our Y2K recommendations to the county and local emergency management personnel are that they assess potential risks, determine how those risks will impact on the local emergency operations plan. We are urging local emergency management personnel to examine, assess and build on the disaster readiness capabilities they already have.

This office is supporting those recommendations through training sessions and outreach programs aimed at the emergency response community. In cooperation with the Office of the Governor, the Department of Law and Public Safety, the Department of Community Affairs, we have developed an outreach program concerning Y2K issues to address our elected officials and the emergency response community.

We have scheduled three regional conferences and invited the elected officials, business administrators, emergency response personnel, and emergency management personnel from all of our 21 counties and 566 municipalities. The timing of this hearing is notable, as we held one of our Y2K training sessions in Morris County this morning. To date, we have reached 14 counties and over 235 municipalities.

Plan appropriately, prepare responsibly: This is New Jersey's Y2K message to local governments and community members. Local governments have an opportunity to set an example and to set the tone for citizens by addressing Y2K issues in a proactive, deliberate, and consistent manner.

“Proactive” means start addressing Y2K immediately. “Deliberate” means that we should integrate Y2K planning into the existing framework for disaster preparedness, training and response. “Consistent” means that we should test all emergency response systems, verify and test again.

To the members of the chemical industry who are represented here today, we recommend that you continue working with the local emergency planning committees, as you are already required to do under existing Federal laws such as Superfund Amendments and Reauthorization Act and the U.S. Environmental Protection Agency risk management rule. The Y2K readiness status of your company should be on the agenda during regularly scheduled planning meetings held with the emergency response community.

In conclusion, our position—plan appropriately, prepare responsibly—is consistent with our planning strategy for all emergency disasters. We look forward to the continued cooperation and support from the Federal Emergency Management Agency and other Federal agencies. We are committed to working in conjunction with all State agencies and private sector organizations to enhance Y2K readiness for all New Jersey citizens.

Thank you for your time and attention, sir.

Chairman BENNETT. Thank you very much.

Let's end with Ms. Jane Nogaki.

**STATEMENT OF JANE NOGAKI, BOARD MEMBER, NEW JERSEY WORK ENVIRONMENT COUNCIL, AND PESTICIDE PROGRAM COORDINATOR, NEW JERSEY ENVIRONMENTAL FEDERATION**

Ms. NOGAKI. Chairman Bennett, thank you for having this hearing today in New Jersey, and thank you for extending to the New Jersey Work Environment Council and the New Jersey Environmental Federation the opportunity to testify today on concerns that the citizens and workers of this State have regarding potential Y2K problems in facilities using hazardous chemicals.

My name is Jane Nogaki, and I have been involved in community and environmental right-to-know issues for 20 years. I am a board member of the New Jersey Work Environment Council, a State-wide alliance of labor and environmental activists, and I am the pesticide program coordinator for the New Jersey Environmental Federation, a nonprofit coalition composed of 80 organizations and 90,000 members. I am also a resident of Marlton, New Jersey and a public member of the Burlington County Local Emergency Planning Committee, the county where you were this morning when you were looking at Sybron Chemical.

The New Jersey Work Environment Council and the New Jersey Environmental Federation are concerned about potential public and occupational health risk posed by chemical releases resulting from the Year 2000 computer problems. It is our contention that, despite corporate and government efforts to identify and remedy Y2K problems, the situation in New Jersey remains perilous for workers and residents alike.

At the same time, if policies are properly designed and implemented to address this potential health risk, New Jersey's workers



and residents may be able to seize opportunities to increase awareness about toxics in our neighborhoods and workplaces.

We can be proud of the effectiveness of New Jersey's Toxic Catastrophe Prevention Act [TCPA], which covers 91 facilities using extremely hazardous substances. We also look forward to expansion of the program under the U.S. Environmental Protection Agency's Clean Air Act Section 112(R), which will extend to approximately 70 additional facilities. Together, these laws authorize the State DEP to collect voluminous risk information data about roughly 160 facilities using high-risk toxics, and they are considered model laws for chemical accident prevention.

Yet, State government efforts to address potential Y2K problems in the chemical and related industries appear inadequate. Last fall, for example, the DEP conducted an informal survey of 20 New Jersey chemical facilities and concluded that these manufacturers had few date-dependent processing units. DEP simply accepted management's verbal assertions and did not request independent verification and validation data.

Thus, it appears that the New Jersey DEP, the agency charged with preventing toxic disasters, has put its head in the sand when faced with challenges posed by the millennium bug. Moreover, it is also apparent that no other agency in New Jersey is independently verifying even the most basic assertions from chemical facilities.

Therefore, we have some proposals to remedy this situation. To safeguard against preventable Y2K-related chemical releases, and to assure New Jersey citizens that both the DEP and facilities in the State that use hazardous substances are taking adequate precautions, we propose the following:

That the New Jersey Department of Environmental Protection should distribute a Y2K preparedness survey to the roughly 160 facilities covered by the Toxic Catastrophe Prevention Act and the EPA Clean Air Act, Section 112. This survey should request information about Y2K efforts, including their preparedness and planning, to help the DEP determine whether each company is Y2K-compliant. The survey should also include questions about equipment suppliers and other contractors.

A reasonable deadline should be set to allow companies to complete the survey, and copies of the survey and a list of the companies receiving it and an introductory letter about the importance of Y2K preparedness should be sent to the appropriate mayors and local emergency planning committees in municipalities throughout the State.

Second, for those companies that do not respond to the survey by the deadline, the DEP should conduct follow-up enforcement activities. They should conduct independent validation and verification audits of a limited number of facilities, and then they should generate a report detailing the results of their findings, and make this information available to the public.

And then we believe that the DEP should initiate a series of local hearings on Y2K preparedness, in which a survey of questions that people could ask in their own community, such as, are chemicals being stockpiled onsite in anticipation of the Year 2000? Have independent verifications taken place? Have risk management programs been shared with the community? This kind of survey and

public outreach could go a long way toward making sure that the outcome of this preparedness is to prevent accidents.

We see this as a tremendous opportunity, but only if there are some more teeth in a program, a State survey and prevention program that heightens the awareness about this potential problem. We don't think that there should be panic about the situation, but I think we concur with your feelings and the feelings of the Chemical Safety Board that the prevention awareness has to be heightened at this point and not left to chance.

So thank you very much for the chance to testify here.

[The prepared statement of Ms. Nogaki can be found in the appendix.]

Chairman BENNETT. Thank you.

Who wants to respond to Ms. Nogaki? Let me ask you. You run an operation. How would you respond to a questionnaire of that kind? You have the advantage of not being from New Jersey, so that you can give us maybe, Mr. Martin, a reaction. How would you respond if the State were to do the kinds of things she has just described?

Mr. MARTIN. I think the forums, the forums as I understand she is speaking of, would be quite great, and I am trying to relate that to what we are already doing, and I think it has made us a lot of money, and increased our understanding and increased our awareness level within the community and within our plant site.

Whereas to the specifics of all the things she is requesting, maybe not knowing the logistics of everything that goes on as far as New Jersey is concerned, it would be hard to maybe address them specifically. Like I said, for our particular area, we have had a great relationship with our LEPC's, we have had a great relationship with the communities. I don't know. We dispel, I guess, any type of outlandish fears, if you will, of anything that could happen, because of that relationship and that we work so closely together.

Chairman BENNETT. Thank you.

Mr. Makris, you have a sort of a national view of these kinds of things. Could you give us a reaction?

Mr. MAKRIS. Several. First, I am glad that Jane is saying they are going to do it in New Jersey, rather than saying it is something that EPA Washington should do, because I think it is consistent with the general view of the program as best run closer to the people.

So my view would be that we would provide, I would provide, my office would provide any support that we could to this kind of an effort with DEP, and I suspect that it would be like something that would catch on throughout the country and other States might follow some of these models.

Along those lines, you know, several people mentioned the importance, especially you, Senator Bennett, the importance of trying to penetrate what is really going on out there. You know, our folks in the Toxic Release Inventory Program have put out a major letter to their constituents talking about enforcement and reminding them of their obligations.

Similarly, we are planning an enforcement test in EPA Region Six, which I guess we will regard as a pilot. And last, I would like to mention that Dana Minerva, our deputy assistant administrator

for water, testified before you in Anaheim, and one of the things that she has done is, she is initiating a National Test Day for water systems.

So, you know, I think we are going to have several examples and really do some testing and observe some specific instances. So I think anything that gets that profile raised and that provides an opportunity with a rifle instead of a shotgun to see what goes on is helpful, and we will provide whatever help Jane needs. Probably can't send money.

Chairman BENNETT. OK. Mr. Fedorko, I have gone to two other places first to give you a chance to collect your thoughts. Do you have a response to—

Mr. FEDORKO. Senator, we work with the local emergency planning committees, and it is their responsibility to go out and talk to the chemical industry, and we actually rely on them to do that.

Chairman BENNETT. The issue raised by several of you is the issue of self-reporting, and that gives us some concern at the Federal level. The only information we have is self-reported.

Ms. Nogaki, what agency would you think should go out and do the audit? As far as Mr. Makris is concerned, he gets audited by the General Accounting Office. When he says that all of EPA's computers are going to work, we say, "Thank you very much," and then we turn to the General Accounting Office to have them tell us whether he is right on or not, and sometimes the GAO disagrees with some of the folks who self-report.

Colonel Fedorko or Ms. Nogaki, who should do some of the independent auditing of people who self-report in New Jersey?

Ms. NOGAKI. Well, we are suggesting—and understand, you know, I do not represent the Department of Environmental Protection, I represent—

Chairman BENNETT. I understand. Sure.

Ms. NOGAKI [continuing]. I believe that the Department of Environmental Protection should be an enforcing and verifying agency, that we shouldn't leave this to self-reporting.

And so who should do that auditing? I think the DEP is probably able in a limited number of cases to verify and audit, and I think that companies are sometimes hiring their own auditors, third person auditors and verifiers, to do that audit. And I think either one would be a method, but I think that it is government's responsibility here to provide some verification that this effort is going on.

The self-reporting, in the case of many companies, you know, it is in their own interest to do this right, and many of them will do it right, but I think that there is a public need and a worker need for some kind of verifiable audit going on. Even if it is in a limited number of facilities, I think it should happen, and I think that the State branch of the Environmental Protection Agency, which is in most places called DEP or DNR, should be that agency.

Local emergency planning and local emergency responders, they are the people that are left to pick up the pieces when things go wrong. You know, God bless them, they are always willing and ready to be there, and they have a communication status, but they don't have any enforcement powers and they are not enforcers of environmental laws, they are responders.

It is the Department of Environmental Protection's job to enforce this law, and they are clearly—they have statutory authority under the TCPA and the Clean Air Act, to inspect facilities to ensure that they are operating safely.

Chairman BENNETT. Yes, sir?

Mr. MAKRIS. Senator, we did not include in the original requirements for the risk management planning, Y2K. We put that rule out in 1996, and it was before some of this flurry took place and some of this great concern.

But what we have done is reminded, through that alert, that it is their general duty, which is a very important part of the 112(R) program, risk management planning program. And in addition, when people file electronically, one of the first reminders is, "Don't forget to include Y2K and include it in your executive summary of your operation." Now, that is not mandated by law but it is an encouragement that we have done to the 69,000 facilities we expect to submit risk management planning.

Chairman BENNETT. Yes. I am interested, Ms. Nogaki, that you are very complimentary of New Jersey's initiative, just talking about the State government as a whole here, New Jersey's initiative in the Toxic Catastrophe Prevention Act. I don't know of any other State where they have done that with State legislation. Do you, Mr. Makris, know of any?

Mr. MAKRIS. Clearly New Jersey led the way.

Chairman BENNETT. Yes.

Mr. MAKRIS. New Jersey led the way. Louisiana, California, several other States have very active programs. Georgia is developing an active program. But I think it was the State of New Jersey and Senator Lautenberg's powerful influence, and at that time Congressman Florio's influence, that helped to drive some of the programs in the first place. And the first thing we do at EPA is ask New Jersey to come on in and give us some advice.

Chairman BENNETT. Well, coming from outside the State, then, I come in for this hearing and I hear high praise for the State's initiative in one area, and criticism for the State's initiative in another area or the State's enforcement in another area. I find a little bit of a disconnect, that a State can lead out in the one regard and then is derelict in another regard. Can any of you help me?

Ms. NOGAKI. I would just like to respond. I don't understand myself the dereliction of duty here. As I said, DEP didn't even attend a national briefing on this issue, but we think that by our raising this issue and bringing it to the department or to the Governor of the State, to ask if some enforcement mechanism can be instituted, that perhaps that can be corrected.

Now I am going to say that while New Jersey was first in writing a toxic catastrophe prevention law, it was Bhopal, the disaster at Bhopal that triggered it. I mean, we do have the third highest chemical production in the country. We have a high volume of chemicals transported in the State and manufactured here, and a very dense population. So our awareness of toxic chemicals is probably higher than any other State in the country.

And despite the institution of that law and the pollution prevention that has occurred as a result of it, we still have had more than 8,000 releases since 1986 that have been responded to by emer-

gency responders—transportation spills, chemical accidents, very serious accidents.

Four years ago at NAPP Chemical, four workers were killed. It is a batch operation plant. Just last year in Patterson, New Jersey, Heterene Chemical released a chemical called creosol, and two blocks away an elementary school had to be evacuated and many people were sickened by it.

We continue to have accidents, and we will continue to have them, but to the extent that we can prevent them, we need to do that. And we think that enforcement, particularly in this kind of scenario, should be stepped up.

Chairman BENNETT. The witness from OSHA who appeared on the first panel indicated that one of the reasons OSHA has not spent more time than it has on Y2K is that the overall record of the chemical industry has been very good, and that OSHA spends its time with people who have records that are bad. Are you challenging that comment on his part?

Ms. NOGAKI. I can't really explain that. I think that in New Jersey, that we have a high risk of chemical accidents because of the joint nature of our high population density and the proximity to—

Chairman BENNETT. That is one of the reasons I am holding the hearing in New Jersey, is because you have that juxtaposition here that you don't have in a lot of other States.

Ms. NOGAKI. Right, so that the consequences of chemical releases and accidents are felt immediately, because they often happen right in the neighborhood. The plant that you visited today, Sybron, is in a relatively rural area, but most—

Chairman BENNETT. Yes. Not relatively. It is rural.

Ms. NOGAKI. Well, yes, it is in a rural area, but many of the manufacturing and chemical facilities in New Jersey are in neighborhoods, you know, like a block away from here. They are in residential neighborhoods, they are in light industrial areas facing highways where there is heavy exposure, and we have the New Jersey Turnpike, the route between Philadelphia and New York where there is a high volume of transport going on. So we are at higher risk than other places.

Chairman BENNETT. Ms. Littles, we haven't heard from you since your opening statement. Do you have a comment on some of the issues we are discussing here?

Ms. LITTLES. Well, actually I think that Jane's suggestion is a very good one, and I believe it could be beneficial in more than just New Jersey, in other States also. There has got to be some mechanism in place, I think, for the government to be able to track what companies are or are not doing around this issue, to enable to ensure that they can come up to a level that would be acceptable for the end of this year.

Chairman BENNETT. I agree with Mr. Makris, I am delighted to have the suggestion made at a State level rather than a Federal level, because we couldn't get the space rented and the pencils bought for an agency in time to do this at any kind of a Federal level.

Ms. LITTLES. Oh, I am certain, but there are other States that are, as New Jersey is, that actually could also benefit from having some system such as the one she suggested in place.

Chairman BENNETT. Mr. Martin, just to go back to you for a minute, where is Virginia on this? Just to get another view, do you have the kind of State monitoring that is being asked for here in New Jersey?

Mr. MARTIN. Well, as far as the different reports that need to go to State agencies, those reports are quite naturally submitted on time and by their request. Again, you know, through the regular regulatory reporting systems, I think all of our information is sent and everything is checked out and verified. No other normal reporting that I think—that I know of in Virginia that is required would have any kind of bearing or any kind of impact, other than the ones we are already submitting, the 112, the other reports, et cetera, that are mandated by EPA.

Chairman BENNETT. Thank you. Well, Governor Whitman's office has been very cooperative with us in helping us set up the hearing. We have a sense of very good communication, and we will communicate to the Governor's office the suggestions and comments that have been made here.

Anyone have any final comment you wish to make?

Mr. FEDORKO. Senator, we can make that recommendation to Commission Shenn with DEP, through the Office of Emergency Management.

Chairman BENNETT. I think that would help short-circuit the communications loop, and I thank you for your willingness to do that.

We thank you all. We thank the members of the first panel and those who have attended. The hearing is adjourned.

[Whereupon, at 2 p.m., the hearing was adjourned.]

## APPENDIX

### ALPHABETICAL LISTING AND MATERIAL SUBMITTED

---

#### PREPARED STATEMENT OF CHAIRMAN ROBERT F. BENNETT

Good Morning and welcome to our hearing on the impact of the Year 2000 technology problem on the chemical industry. I am pleased to be holding this hearing here in New Jersey, not only because of the importance of this industry to your state, but also because it is nice to go outside of Washington DC to meet the people on the front lines of the battle against the Y2K computer problem.

I have just come from a tour of Sybron Chemicals in Birmingham and was impressed with the level of automation in this plant, which I understand is typical of other plants in the industry. While this automation enables safe and efficient operation of the plant, it also increased susceptibility to Y2K anomalies. I can only hope that the other tens of thousands of chemical producers and users in America are doing as well as Sybron in addressing this insidious problem.

We have an excellent group of witnesses here today who have taken time out of their busy schedules to help us shed light on the Y2K problem in the chemical industry. Before we begin let me talk about the importance of the chemical industry.

The crude oil refining industry keeps American transportation running. Our health—and sometimes our lives—are dependent on pharmaceuticals produced by the chemical industries. And, the manufacture of virtually every consumer product is in some way dependent on vital chemical ingredients. As you can see on this chart, (shaped like a house) chemical products are present in everything from shampoo to floor polish.

On the economic side, the \$392 billion chemical industry is the largest in the manufacturing sector and employs over one million workers. It is also our largest exporter accounting for \$69.5 billion or 10% of the total exports in 1997, easily outdistancing the second leading industry—agriculture—and generating a trade surplus on average of more than \$16 billion annually over the last ten years.

The chemical industry has set high standards for safety, and has a very proactive program to preserve this record and to continuously improve on health, safety, and environmental performance. This industry is one that is already accustomed to dealing with risks, and I am hopeful that we won't see any Y2K-related problems. Nevertheless, the chemical industry warrants our attention because accidents can have such devastating effects. Even though it happened over 15 years ago in another country, most of us remember the Bhopal accident that killed several thousand people and injured tens of thousands of others. We have never seen a chemical release of that size in the United States, but the potential for harm is great. An estimated 85 million Americans—more than 30 percent of the U.S. population—live within 5 miles of one of the 66,000 sites that handle hazardous chemicals. That's why any potential Y2K problems at chemical facilities cannot be taken lightly.

In addition to safe "on-site" operations, chemical processing plants must prepare to deal with external services which may be Y2K vulnerable. Let me give you an example. On November 24, 1998, a power outage caused the shutdown of an Anacortes, Washington refinery. As the refinery was returning to operation after a cool-down period, an accident occurred that took the lives of six workers. The power outage may not have directly caused the accident, but it brought about the circumstances that put six men in danger, and ultimately cost them their lives. Accidents are more likely to occur at a chemical plant during startups and shutdown—just as airlines face an increased risk of accidents during takeoff and landing. This industry must be ready for any sudden Y2K-induced shutdowns.

In this industry, with the many harmful and toxic substances that are involved in chemical processes, there is very often little room for error, and the potential for a Y2K impact must be determined and planned for. Our Committee has been very

concerned about the Y2K impact on numerous government agencies and private sector organizations. However, in few other areas have we have perceived a similar possible public health risk associated with Y2K. That's why we're here today to address the question, "Will Y2K and chemicals be a volatile mix?"

\* \* \* \* \*

**Panel 1 Introduction:** The witnesses for our first panel today are:

- The Honorable Dr. Jerry Poje (POE-GEE), member of the US Chemical Safety and Hazards Investigation Board and principal author of the March 1999 report on this topic.

- Mr. Francis Frodyma (FROE-DEE-MA), the Acting Director of Policy at the Occupation Safety and Health Administration,

- Mr. Paul Couvillion (COE-VEE-ON), Global Director for DuPont's Year 2000 Project, and

- Mr. Jamie Schleck, Executive Vice President of Jame Fine Chemicals, a specialty chemical manufacturer here in New Jersey.

**Panel 2 Introduction:** We'll now start our second panel. Our witnesses are:

- Mr. James Makris, director of the Chemical Emergency Preparedness and Prevention Office at the EPA,

- Mr. Charlie Martin, Site Safety Coordinator for Hickson Danchem Corporation in Danville, VA. We appreciate Mr. Martin's being here to emphasize that this is a problem we must be concerned about across the nation,

- Ms. Paula Littles, Citizenship & Legislative Director of the PACE International Union,

- Lt. Col. Michael Fedorko, the State Director of the New Jersey Office of Emergency Management, and

- Mrs. Jane Nagoki (NAH-GAWK-EE), representing the New Jersey Work Environment Council and New Jersey Environmental Federation.

We appreciate the efforts of all of our witnesses today, and we extend our gratitude for their preparation and contributions. As I said when we began, this industry is very important to our standard of living, our health, and our economy. We must all work together to prevent the Y2K-problem from damaging any of these areas.

---

#### PREPARED STATEMENT OF PAUL COUVILLION

##### Introduction

Good afternoon, Mr. Chairman and members of the Senate special committee. My name is Paul Couvillion, Global Director for DuPont's Year 2000 Project. Thank you for inviting me to appear before you today to discuss this very important issue.

DuPont has made formal disclosure statements to the U.S. Securities and Exchange Commission regarding our Year 2000 Project. I'm not here to restate those disclosures and disclaimers, but to give you a brief update on our project and to answer any questions you may have when I complete my statement.

I have worked for DuPont for 35 years and was appointed to lead this global effort almost two years ago. I was selected to lead this work because of my experiences in leading people and in managing manufacturing processes in a number of DuPont businesses.

The remediation of Year 2000 issues in our plant process control systems, computer hardware, applications software, embedded chip equipment and our suppliers and customers are very important to DuPont. Our goal is to achieve safe, continuous business operation through the Millennium. Based on our current plan, we should have more than 98% of our critical and significant computer systems Year 2000-capable by the end of June 1999, with the remainder completed by year-end.

I am excited about what our teams have accomplished and am confident we will be internally ready for the Year 2000. We are developing contingency plans where we have assessed potential interruptions in supplies or product flow to customers.

##### Who Are We?

DuPont has been in business for almost 200 years. We are a world leader in science and technology with a range of disciplines and products including high performance materials, specialty chemicals, pharmaceuticals and biotechnology. Our portfolio of 2,000 trademarks and brands includes Lycra(R) elastane, Teflon(R) fluoroproducts, Stainmaster(R) residential carpeting, Kevlar(R) aramid fiber and Corian(R) solid surface materials. We operate in 65 countries worldwide and have



a long-established presence in North America and Europe and strong and growing market positions in South America and Asia Pacific. DuPont's 93,000 employees are dedicated to bringing science to the marketplace in ways that benefit people and generate value for our stockholders.

#### **DuPont and Y2K**

The goal of our global Year 2000 team is to be certain that critical and significant information technology is capable. This project is one of the top corporate initiatives identified by DuPont President and Chief Executive Officer Chad Holliday.

DuPont has proactively addressed the Year 2000 issue on a global basis since 1995. We established two key goals for the project. The first, consistent with our commitment to continuously improve our safety performance, is to prevent safety, health or environmental incidents that could occur as a result of the Year 2000 Problem. Secondly, we want to maintain the continuity of our businesses in service to customers, employees, stockholders and communities.

This task has required mobilizing employees around the globe. The DuPont Year 2000 Project consists of more than 40 teams and about 2,000 people from businesses, regions and functions that comprise the company worldwide. These teams work together with our Information Technology (IT) Alliance Partners—Computer Sciences Corporation (CSC) and Anderson Consulting—who operate the majority of DuPont's global information systems and technology infrastructure.

The company's approach to the Year 2000 challenge involves the use of a multi-phase process being used by many companies worldwide:

- Assign qualified people to the project,
- Find and Inventory systems, hardware, and software (objects),
- Assess object capability (Capable, not capable, unknown),
- Define safety or business criticality of objects (Mission critical, significant, negligible),
- Strategies to remediate/test non-capable objects (remediate, replace, retire, validate),
- Create plans to define the work, the schedule and resources needed,
- Prepare and Remediate objects,
- Test objects/systems individually or as an integrated system,
- Redeploy into production, and
- Contingency planning and Event management.

This process is applied to a diverse range and number of systems connected in complex and extensive networks across businesses and regions.

- 6 regions—US, Mexico, Canada, Asia Pacific, Europe (includes Middle East, Africa), South America,
- 3 global data centers in 2 countries,
- 2,000 medium range computer platforms, each with—100 software applications,
- 12,000 telecommunications, wide area and local area network devices, switches or servers,
- 60,000 personal computers and applications,
- 500 globally shared, centrally managed, applications used to manage our global businesses,
- 8,500 business specific applications among 17 global business units and 10 functions,
- 200,000 objects or embedded chips at 320 production units at 135 sites around the globe, and
- 2,000 non-manufacturing sites, warehouses, sales offices, with bar code readers, faxes, etc.

Our Year 2000 Project is managed centrally with a small, diverse team of experienced people. The work is executed locally within each business unit, function and region. Corporate direction is provided by our Operating Group who receive project updates biweekly. My team reports to an Executive Steering Committee every month. This steering group is made up of senior corporate officers, including the CIO, CFO, and the V.P.'s of Sourcing, Engineering and two global businesses. The role of my team has been to develop and provide common technology and processes for the Year 2000 project, monitor business unit progress versus plans, collect metrics, hold periodic reviews and provide support to unit projects.

#### **Costs**

We estimate total expenditures to become internally Year 2000 capable to be in the range of \$350 to \$400 million. Through March 1999, we have expended \$225 million or about two-thirds of our 4-year estimated expenditures.

#### Readiness of Parties Upstream and Downstream from DuPont

DuPont has more than 80,000 suppliers, 20,000 customers and 150 joint ventures around the globe. A Business Partner workstream was established to develop an informed view of the readiness of more than 5,000 critical suppliers, 2,000 key customers and the joint ventures.

About three-fourths of the suppliers surveyed responded; of those we have assessed 15% as potentially creating interruptions to the continuity of supplies or services. Key reasons for our concerns are "no response," "no program in place," "late completion," or "non supplier assessment in place." We initiated and have almost completed four special emphasis surveys among these key supplier groups to become better informed about potential disruptions to our operations:

- Global telecommunications,
- Logistics suppliers (air, truck, rail, ocean and freight forwarders),
- Electrical utilities generation and distribution, and
- Natural gas providers.

Initial conclusions indicate we will likely experience a "low" probability of failure among these groups of infrastructure suppliers. However, we have found some specific regional or area exceptions where these services could be interrupted and where contingency plans will be required.

About half of the customers we surveyed responded; of those responding we have assessed 33% as potentially creating interruptions to our business processes. Key concerns include the late remediation of order placement systems, receipt of product by customers and accounts payable systems.

#### Contingency Plans, Crisis Management and Event Management

Each of the company's business units has formulated contingency plans to address potential disruptions to their business operations from both internal and external sources. DuPont is reviewing a number of options including sourcing raw materials from alternate vendors or arranging for back-up or alternate transportation carriers. We have completed summary plans and expect to complete detailed contingency plans by June 1999. We will continue to update these plans during the remainder of the year. They will be executed in time to assure continued operations.

Information about DuPont's Year 2000 project including a completed CMA survey and our most recent SEC disclosure statement are available on our internet home page at [www.dupont.com](http://www.dupont.com).

#### Summary

This project is critical to DuPont's success and we have committed the necessary resources to get the work done on time. From this work we have learned and gained much about how to do a large global project including:

- Using teams and networks globally,
- Leveraging knowledge and solutions globally across businesses and regions,
- Partnering with our IT Alliance for maximum business benefit,
- Better insights and understanding about how our IT systems work,
- Helping us to create a new, future IT strategy, and
- Closer working relationship and understanding of our value chain.

We intend to meet our goal of safe, continuous operation through the Millennium.

At midnight on December 31, 1999, the world—companies, governments, institutions—will be given a test. I don't know about you, but each time I take a test I get a little anxious and nervous. We have done our homework and I believe we have prepared ourselves well for this final exam and expect to get an "A" for both effort and results.

Thank you for the opportunity to appear before the committee this afternoon. I will be happy to answer any questions you may have.

RESPONSES OF LT. COLONEL MICHAEL A. FEDORKO TO QUESTIONS SUBMITTED BY  
CHAIRMAN BENNETT

*Question 1.* Do you have specific concerns regarding the Y2K-vulnerability of the chemical industry, and has the Office of Emergency Management responded to those concerns?

Answer. From the perspective of an organization concerned primarily with consequence management, let me assure you that we take this issue seriously. While regulatory authority for this segment of industry resides with the NJDEP, the NJSPOEM is responsible for coordinating emergency management by assuring that States agencies, counties and municipalities maintain current and viable all-hazard

emergency operations plans to deal with a full range of emergency situations. With the onset of the Y2K issue, we recognized the unique challenges inherent with Y2K and felt it prudent to hold three regional public officials conferences to provide local planners and responders with information and advice on addressing Y2K concerns in their jurisdictions. These workshops were extremely well received. In conjunction with the State's Chief Information Officer and the 18 respective State Department Y2K coordinators, we continue to monitor progress toward achieving Y2K readiness.

The NJDEP does not have specific concerns because of the significant outreach effort by the USEPA and the various chemical industry trade association. Assessments indicate that the larger facilities are aware of the problem, have allocated appropriate resources and should be ready. Additional effort is being made by the USEPA and these trade associations to target the small and medium sized enterprises to facilitate their rate of progress to that of the larger facilities. The NJDEP's general concerns (i.e., how do we handle problems that occur in spite of the foregoing) are being addressed by the Local Emergency Planning Committee activities described in response to question 3.

*Question 2.* What is being done to plan for response to multiple system failures within a single plant, or simultaneous failures in neighboring facilities?

Answer. Community Emergency Managers have been trained using the Guide for State and Local Emergency Managers. This Contingency and Consequence Management Planning for Year 2000 Conversion manual developed by FEMA is being used to prepare plans that address these worst case scenarios. Consequence management plans will then be developed, coordinated and tested. These actions will occur in the time line shown in the response to question 3, below.

In addition, risk management plans, as required under both TCPA and Section 112(r) of the Clean Air Act do require worst case scenario development and the corresponding emergency procedures. Training programs conducted by the NJSPOEM, NJDEP and USEPA have always included consequence management and multiple system failures as part of their classroom and hands-on curricula. This is a standard practice under hazard and risk assessment for emergency response teams.

*Question 3.* Can you describe specific initiatives undertaken by the Local Emergency Planning Committees (LEPCs), and what impact have they had on Y2K readiness in the chemical industry?

Answer. LEPCs have been advised to convene a special session to occur not later than September 30, 1999 to address potential impact of Y2K. Please refer to the enclosed letter, which was sent on May 27, 1999 to all 566 municipal and 21 county emergency management coordinators. They are to insure active participation of local government officials, private industry, businesses and community organizations in the analysis and problem-solving process of confronting potential Y2K challenges. Municipal emergency management coordinators are to schedule the meetings no later than June 30, 1999. NJSPOEM regional staff will work closely with the county coordinators to assist in the planning and conduct of these meetings, placing emphasis on municipalities hosting TCPA and/or SARA chemical handling facilities.

An annex by annex review of their respective emergency operations plans and worst case analyses will be the basis for coordinated plan development, testing and implementation. These activities are designed to minimize the adverse impact to human health and the environment if releases occur in spite of the best Y2K readiness preparations by the chemical facilities.

*Question 4.* Would you describe the training and outreach programs your office has developed to support the Local Emergency Planning Committees?

Answer. The NJSPOEM's Training and Program Support Bureau offers a variety of interrelated courses designed specifically to improve the professional, managerial and technical skills of LEPCs. The curriculum includes over 50 offerings which cover emergency management, planning, community disaster education, leadership, hazardous materials planning and emergency response, incident command and other emergency management programs designed for targeted audiences, such as school administrators and persons with disabilities.

During the past year, the NJSPOEM has also been able to focus on specific projects related to the implementation of the USEPA Risk Management (RMP) Rule. Activities include the development and delivery of the NJSPOEM Risk Management and Communication Course, over 15 RMP outreach presentations, development and distribution of RMP print materials aimed at LEPCs, and three pass-through grants which were awarded to county LEPCs for demonstration projects related to the USEPA Rule. During this time, The New Jersey Chapters of the American Institute of Chemical Engineers and the Academy of Certified Hazardous Materials Managers also approached the NJSPOEM regarding the development of an RMP volunteer match program, where trained volunteer chemical engineers from either association would be matched with county and municipal LEPCs to assist them

in interpreting industry RMPs, and integrating RMP data into their community's emergency operations plan. To date, three county LEPC matches have been made.

Finally, the New Jersey Department of Community Affairs, Division of Local Government Services distributes a quarterly publication entitled "Y2K? OK!" to all municipalities and counties in the State. This publication was targeted specifically at local government officials by providing them with current technology and advice on addressing Y2K concerns in their communities, and encouraging public education and awareness. A copy of Volume 2 of this publication is enclosed for your review. In addition, the State Y2K Coordinator and his staff have been conducting a vigorous outreach campaign to the public and private sectors to deliver the Y2K compliance message and reinforce the need for emergency planning.

*Question 5.* What are the Department's [NJSPOEM] plans to provide an increased response capability (to address problems which might occur in the time period immediately before and after the date change)? Will there be any increase in emergency response capability to deal specifically with chemical plant incidents?

Answer. Emergency response capability probably will not be altered significantly from normal procedures. Y2K preparation has enhanced the quality of contingency plans by encouraging local planners and responders to consider direct and secondary impacts of this hazard. It is hoped that each of New Jersey's 566 municipalities will have developed a Y2K appendix to their EOP before the end of this year.

*Question 6.* What has been the level of involvement of your Department [NJSPOEM] with the New Jersey Department of Environmental Protection in addressing the allegation that the NJDEP is not sufficiently aware of status of Y2K readiness in the chemical industry?

Answer. These criticisms were communicated in a letter from the witness (co-signed by others) to Governor Whitman on May 7, 1999. The response by Robert C. Shinn, NJDEP Commissioner, dated May 26, 1999, (also enclosed) outlined actions that the NJDEP considers necessary and sufficient for effective accomplishment of its mission. The NJSPOEM has no direct role in these issues, however, as discussed earlier in this letter, we do have significant interaction in coordination, development and implementation of emergency response planning. At the three public officials conferences, LEPCs were encouraged to place special emphasis in encouraging participation from their chemical industry in addressing Y2K issues in their community and reporting their progress to the public through local media and community group meetings. In addition, the State's Y2K Coordinator holds monthly Y2K coordinating meetings with all 18 State Department Information Officers to share information and monitor progress towards Y2K compliance.

Again, thank you for the opportunity to respond to your concerns. The NJSPOEM and NJDEP are making every effort to take a pro-active stance on the Y2K issue. We believe that we have the mechanisms in place to expediently address the known and potential challenges of Y2K. Should your office or members of the Special Committee on the Year 2000 Problem have additional concerns, please do not hesitate to contact this office.



State of New Jersey

CHRISTINE TODD WHITMAN  
Governor

DEPARTMENT OF LAW AND PUBLIC SAFETY  
DIVISION OF STATE POLICE  
POST OFFICE BOX 7068  
WEST TRENTON NJ 08628-0068

Attorney General

DATE: May 27, 1999

TO: County and Municipal Emergency Management Coordinators

SUBJECT: Local Emergency Planning Committee (LEPC) Involvement in Year 2000 (Y2K) Contingency and Consequence Management Planning

I commend you for your enthusiastic response to the recently concluded series of regional public officials conferences on the Y2K challenge. All 21 counties and over 325 of our municipalities took part in this informative dialogue with State agencies, utility providers and the private sector. Mayors, managers, first responders and public works professionals came together to scrutinize the many facets of the Millennium and its potential to complicate the process of government. Thank you for your candid sharing of concerns and for highlighting areas which demand additional focus.

I believe it is essential for us to formalize the follow-up process for Y2K consequence management outlined during the conferences. This is especially critical for those communities hosting one or more chemical handling facilities subject to the U.S. Environmental Protection Agency Risk Management Rule, Title III of the Superfund Amendments and Reauthorization Act, the New Jersey Toxic Catastrophe Prevention Act, or the New Jersey Right-To-Know Act. The appropriate mechanism for our follow-up is the involvement of your Local Emergency Planning Committee (LEPC). Active participation by the LEPC will insure that every instrument of local government, both public and private, takes part in the analysis and problem solving process for confronting potential Y2K challenges.

Governor Whitman, Commissioner Robert C. Shinn of the New Jersey Department of Environmental Protection and Lieutenant Colonel Michael A. Fedorko, the State Director of Emergency Management, agree that the focus must begin at the local level. I strongly suggest, therefore, that you convene a special session of your LEPC between now and September 30, 1999, to deal exclusively with local Y2K issues. This meeting should be a matter of public record. An annex by annex review of your Emergency Operations Plan (EOP), with an eye toward isolating the most likely areas of Y2K concern, is an excellent start point for this endeavor.

I ask that you notify your county office of emergency management by June 30, 1999, of your intentions to conduct this meeting and of any assistance that you require. County coordinators are requested to consolidate and furnish this information to their NJOEM Regional Units by July 15, 1999.

LEPS  
ENCLOSURE 1

New Jersey Is An Equal Opportunity Employer • Printed on Recycled Paper and Recyclable



County and Municipal Coordinators

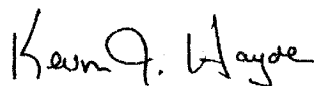
2

May 27, 1999

The State Office of Emergency Management is committed to a prepared and Y2K-compliant emergency management community. A review by your LEPC of plans and procedures, while there is still time to react, appears to be a prudent strategy for us to adopt.

Should you have any questions or require further assistance, please contact Mr. Joseph Painting of the Operational Planning Bureau at (609) 538-6012.

FOR LT. COLONEL MICHAEL A. FEDORKO  
ACTING SUPERINTENDENT  
STATE DIRECTOR



Kevin J. Hayden, Captain  
Assistant Section Supervisor  
Emergency Management Section

KJH/elg

c Commissioner Robert C. Shinn, DEP  
NJ Chief Information Officer, Wendy Rayner  
Phil Angarone, Governor's Office  
Jack Longworth, OIT  
Steve Long, OAG  
Carl Wyhopen, OAG  
Marc Pfeiffer, DCA  
James Giuliano, BPU  
Robert Van Fossen, DEP

**YEAR 2000 READINESS DISCLOSURE. THIS  
YEAR 2000 STATEMENT IS HEREBY  
DESIGNATED A YEAR 2000 READINESS  
DISCLOSURE.**

# Y2K? OK!

## Y2K Advice for New Jersey Local Government Officials

Prepared by the NJ Division of Local Government Services, Department of Community Affairs and the Office of the Chief Information Officer

March, 1999

Volume 2

- ▼ The **Y2K? OK!**  
Talk: Do's and Don'ts
  
- ▼ Emergency Services  
**Y2K** Update
  
- ▼ **Y2K** Readiness  
Status Report
  
- ▼ Updated Link List
  
- ▼ How to Check  
Embedded Systems
  
- ▼ **Y2K** News From  
The Federal  
Government



ENCLOSURE 2

**Y2K? OK!** Volume 2

page

## IN THIS ISSUE...

Editorial	1
The Y2K Talk: Do's and Don'ts	2
Emergency Services Y2K Update	3
Y2K Readiness Status Report - March 1999	4
Emergency Management Coordinators - What Should They Be Doing?	5-6
Y2K Embedded Systems — 10 Steps to Y2K Readiness	7-8
Link List	9
For Water and Wastewater Utility Operators	10
From the Association of Environmental Authorities...	11
Y2K News From the Federal Government...	12
The End - Y2K Humor	13
▼ Special Pull-Out Section	
<i>Your Little Box of Problems</i>	A1-A14
<i>Y2 Techie Quiz</i>	A-14
<i>Microsoft Y2K Update</i>	A-15
<i>Y2K Legal References</i>	A-16

**Y2K? OK! Mailing List**

If you've got e-mail, we've got a mailing list! You can use any internet e-mail service to subscribe to our new **Y2K? OK!** mailing list to receive questions and answers from your fellow local officials on Y2K issues.

Not familiar with mailing lists? Well, they are one of the great free internet resources. By subscribing to the list (see precise instructions below) you can send and receive mail from all other subscribers to share information, relate experiences, ask questions, and get answers to your Y2K questions.

Just send an e-mail to: [Y2Klist@listserv.state.nj.us](mailto:Y2Klist@listserv.state.nj.us), do not enter a subject, and include in the body of the e-mail, just the word "subscribe" (no quotes) and you'll be on the list. You'll receive an e-mail confirming your subscription and information on how to use the list.

**Y2K? OK! Year 2000 Readiness Disclosure Statement and Disclaimer**

The contents of **Y2K? OK!** and the Supplement, is a Year 2000 Statement from the State of New Jersey, and is designated a Year 2000 Readiness Disclosure. In addition, this document contains Year 2000 statements that have been republished from other sources. Interested persons should contact the person or entity identified as the source of the information to verify the accuracy of those Year 2000 statements. The references contained herein have been provided because the reader may find them of interest and should not be relied upon as legal advice. Neither the State nor the Department guarantees the accuracy or completeness of any of the information contained in these references. Local government units should consult with their legal counsel to discuss the many legal issues associated with Y2K, such as how to prepare and follow a due diligence plan; what contractual or other remedies may be available; potential exposure to legal claims; the obligations of issuers of securities; and, the protections available under the Federal Year 2000 Information and Readiness Disclosure Act.



**Y2K? OK!****Editorial**

We're making progress! With the help of the media, the message about Y2K is getting through to local officials and the public. Society is responding and all sectors are stepping up to assess and manage their Y2K risks. Slowly, but surely, people are understanding that the banking system, utility systems, and telecommunications systems, among others, are all responding to the challenge and fully expect to be operating on January 1, 2000, as well as on leap year, February 29, 2000!

What's important now is follow through and communication. Local government officials have the critical responsibility of not only ensuring that their own computer, telecommunications and utility infrastructures are Y2K ready, but they must ensure that their emergency plans are up to date. Most importantly, we must continue to inform the public that government is successfully responding to the challenge and that our contingency plans are a backup we never expect to use.

This issue of **Y2K? OK!** continues the State's effort to assist local government officials with meeting the Y2K challenge. This issue's "centerfold" includes an detailed article on check-

ing your PC's and networks for Y2K compliance. We know that's a tough thing for smaller governments, and we hope this article (Excerpted with permission from the PC Novice Guide to Y2K - Sandhills Publications, January 1999), will let officials finish this important part of Y2K readiness.

We also cover the legal exposures held by government officials. This is one more reason why it's critical that government carefully study their exposures and document their efforts to get **Y2K? OK!** The lawyers are warming up their briefs, and local government should not be providing them any ammunition. So, document, document, document!

With this issue we start our coverage of emergency planning for Y2K. In emergency management terms, Y2K is just another event to prepare for, it's important to be sure that our plans are up-to-date and resources have been checked. Local governments are the first line of response for infrastructure failures and must be ready to respond. We're working with the State Police Office of Emergency Management to produce a series of State-wide seminars this spring - please watch for them and be sure emergency management leaders attend.

We also can't stress enough the importance of public communication of your Y2K efforts. We provide some advice on how to handle public communication with some important Y2K do's and don'ts on Y2K matters. To help that process along, we encourage you to take our **Y2K? OK!** pledge (see last issue or our web site for it) and to start a local Y2K committee.

Also, watch your mail for a newsletter from the Joint Y2K Task Force, made up of DCA, the League of Municipalities, Association of Environmental Authorities, and New Jersey Association of Counties, all coordinated by the Municipal Excess Liability Fund. Between the Task Force and **Y2K? OK!**, we should be able to get you references to all the information you need to know.

How are you doing? Write or e-mail us with your experiences. Better yet, if you have e-mail, you can join our Y2K list - an internet based mailing list for local officials to share information about their Y2K experiences and concerns. See the back page for information on how to subscribe.

And finally, this entire edition of **Y2K? OK!** is designated a "Year 2000 Readiness Disclosure." Anything your organization prints describing its Y2K status, should include this same statement. It provides limited protection against litigation!

**Y2K? OK!****The Y2K Talk: Do's and Don'ts**

Are you being asked by your constituents and others about your Y2K status? Sam Byassee, a partner at the law firm of Smith Helms Mullis & Moore LLP, in Raleigh, N.C., offers some pointers for year 2000 communications:



- ▶ **DO be responsive.** Trying to stonewall or evade inquiries will raise a red flag and focus more attention on your company.
- ▶ **DO explain** that the information being provided may change based on changes in future circumstances.
- ▶ **DO include a notice** on written material that it's a "year 2000 readiness disclosure" pursuant to the federal Year 2000 Information and Readiness Disclosure Act of 1998. Statements with that label can't be used as evidence in any lawsuit.
- ▶ **DO be truthful and as accurate as possible.**
- ▶ **DO brief people** who may be asked year 2000 questions on what the company is doing and what the appropriate type of response is.
- ▶ **DO have those people add** that they aren't directly involved in the project and that for more detailed information, the questioner should contact the project office.
- ▶ **DON'T assume** that you must use the questionnaire form that an organization asks you to answer. **DO provide** information that you think will be useful and **DO offer** to work with the other party to address any concerns specific to your company. That helps to show due diligence without wasting your time on minutiae that doesn't apply.








- ▶ **DON'T sign** a questionnaire that says you're certifying anything, indemnifying the other company or providing a warranty. **DO provide** the appropriate information and send it back with a letter declining to accept the additional risk requested in the certification or warranty.
- ▶ **DON'T assume** that if you're ready internally for year 2000, you won't have any problems.
- ▶ **DON'T allow** any over-optimism or overconfidence to creep into your response.
- ▶ **DON'T give** firm projections even if your project is on schedule.
- ▶ **DON'T give an absolute deadline** for when you'll be ready. "It's the difference between 'We will be ready' and 'We now expect to be ready,'" Byassee notes.
- ▶ **DON'T provide more** information than requested, even if you're proud of the work you've accomplished. "If you say 10 things, you have 10 chances of something going wrong," Byassee says. "If you say 20 things, you have 20 chances."

**Y2K? OK!**

**Emergency Services Y2K Update**

DCA and the Joint Task Force have received many inquiries about the status of emergency management, infrastructure, and public safety equipment and Y2K readiness. Here's what we can tell you as of the end of March:

- 
  - As far as we can determine, after checking with manufacturers, police cars and other automobiles **do not** have inherent Y2K failure potential. If you have added custom equipment to them, that equipment must be checked to it ensure it is Y2K ready and it's failure will not affect anything it's connected to.
  - The Office of Emergency Management, OCA, and the State's Y2K office will be sponsoring a series of Y2K Emergency Management, Public Safety and Infrastructure regional seminars in the spring. They will include information we received from seminar FEMA held in February.
- 
  - The rumor that all fire apparatus built before 1985 will fail is an urban legend, and is not true. We've also checked with many apparatus manufacturers and they advise that their computer controlled systems are not date dependent. Where microprocessors are used, they may clock hours of use, but do not have a date setting for operational purposes.
  - The State's public utilities are well on their way to meeting June 30, 1999, goals for readiness. The Board of Public Utilities is meeting regularly with them and those efforts are being coordinated with the State's Y2K planning efforts. Local utility operations are acting independently to ensure their system are Y2K ready. We have already found that most water and sewer pumping systems are not Y2K risks, and as long as the computers that control them are Y2K ready, failures are not anticipated.
- 
  - The State's 9-1-1 system is already Y2K ready. The State's Office of Emergency Telecommunications Services has surveyed and notified all Public Safety Answering and Dispatching Points of the status of the 9-1-1 network. There are several Public Safety Answering Points that have terminal equipment Y2K issues to manage, but they have been identified, they know who they are, and are acting to upgrade their equipment.
  - After all is said and done, what kind of problems can we expect, even if everyone does their jobs? The most expert advice we now see on the potential for system failures stemming from Y2K is said to be similar to those posed by a hurricane. Hurricanes can result in spot power outages and telecommunications failures, and require temporary shelter and sanitary facilities. That's what we see as the planning scenario. There's another article on Emergency Management in this issue and we'll have more in the next issue of
- 
  - The State's Emergency Operations Center will be operational over the New Years holiday and will be coordinating communication and other matters with the National Guard and the military.
- 

**Y2K? OK!**

**Y2K? OK!****Y2K Readiness Status Report - March 1999**

The following information has been gathered from a variety of sources to answer some general questions about problems expected with particular types of equipment. *This information is intended for planning purposes and is not a guarantee of any reliability of any specific system mentioned.* Local emergency managers are responsible for confirming the reliability of these specific systems within their own communities.

**Traffic lights:** Little effect. Other than outages from electricity failures, the worst case scenario: intersections won't be in synch with each other. Tests in many jurisdictions (including New Jersey) indicate that a relatively small number of problems identified by the test may cause inefficient operations of traffic signals if left uncorrected.

**Elevators:** Not affected. Worst case (remote) scenario: elevators may return to the lobby and stay open. This may appear if building management systems to which they are connected fail. Most other building systems appear Y2K ready, though system operators should check with vendors to be sure!

**Automobiles:** Except for roughly 100,000 Cadillacs built in 1989, no American car should have any sort of Y2K problem. And the Caddy's just have an oil change light that may flick on.

**Medical Devices:** The FDA has sent Y2K surveys to almost 2,000 medical-device makers, and so far has heard back from over two-thirds of them. While many testing and diagnostic devices (including defibrillators) may have some problems unless they are updated, most of the problems will be small, like displaying an incorrect date. A **Y2K? OK!** spot check of



defibrillators at a biomedical site indicated all were compliant. FDA officials have noted that "while we are in the process of reviewing the issue, we do not currently believe that there will be any major impact on medical device safety." To be sure, local officials should use the embedded system guides and the health equipment device inventories on the web to check suspicious equipment. See our list of these sites in this issue's **Y2K? OK! Link List**.

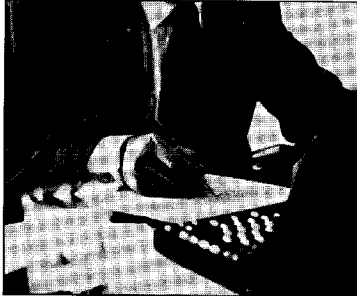
**Electric Power Generation:** The North American Electric Reliability Council has recently noted that "With proper contingency planning, sufficient generating capacity is anticipated to be available to meet demand during the critical Y2K transition periods." New Jersey's utilities have recently reported the same scenario - the worst case is spot outages, and prudent planning will ensure fuel reserves and emergency responses capability.

**Nuclear Power Plants:** The Council also noted that "Y2K issues...in nuclear facilities do not represent a public health or safety issue. No nuclear generating plant has found a Y2K problem in safety systems that would have prevented a safe plant shutdown at the turn of the century."

**Railroad switches and highway crossings:** Information from Union Pacific tells us that systems controlling switching are not date-dependent. In any case, switches can be operated manually if needed. Highway crossing warning systems are not date-dependent. Each system has battery back-up for a period of time in case of power outage. Most railroads "storm-test" their systems for power outages on a regular basis.

**Public safety communications systems:** A recent survey by 9-1-1 Magazine highlighted that many dispatch and radio systems are Y2K ready. (<http://www.9-1-1magazine.com/magazine/1998/0598/features/44y2kSBI.html>). However, each agency should verify with the manufacturer that their equipment is covered. See this issue's **Link List** for web sites of emergency communication equipment manufacturers.

*A publication of the Minnesota Division of Emergency Management was the starting point for this list.*

**Y2K? OK!****Emergency Management Coordinators-  
What Should They Be Doing?**

There are three key actions that all emergency management staff should be performing, starting now and continuing through the year.

**Get informed and inform others**

Nobody expects you to become a computer expert. As emergency managers, you're used to dealing with the consequences of a disaster without having to become disaster experts. After all, you don't have to be a meteorologist to effectively manage a hurricane. In the emergency management profession, Y2K is essentially "just another potential event." So, your job is to get a detailed picture of the type of problems your community can reasonably expect on New Year's, 2000. You may be the only person in your community considering the big picture.

**Be proactive with information**

The public is becoming aware of Y2K and they want to know what they should do to prepare for it. We need to use this time of increased awareness to enhance our community preparedness. Help your citizens get organized. Advise them to make family protection plans - the kind they can use for other emergencies: floods, hurricanes, tornadoes, etc. (Family

preparedness checklists are available from the Red Cross - we'll publish them in the next issue!). There are plenty of sources of questionable, alarmist information available that advise people to take some drastic measures. If you don't give them good, reliable preparedness advice, they may get bad advice somewhere else.

**Get ready**

Your community should already have a disaster plan and procedures to deal with power outages, traffic problems, and other emergency situations. Use the information you gather in Step 1 to create Y2K-specific preparations that are incorporated into your existing all-hazard plans. For instance, your community should already have a plan for opening public shelters in the event of prolonged power outages during the winter. It doesn't matter whether an outage is caused by a severe ice storm or a Y2K problem. Just ensure that any Y2K-specific aspects are also included in your plans.

**What else do I have to do?**

There are four other things all emergency managers or planners must do to prepare for potential Y2K problems:

- ◆ Assess your community's preparedness for Y2K: Talk to the utilities and major businesses in your community about their Y2K activities. What work have they done so far to prevent Y2K-related problems? What kind of problems do they reasonably expect to occur? What have your government agencies done to assure their conti-

nity past December 1999? Assemble a clear picture of what your community may expect in January 2000.

- ◆ Share your completed assessment with local officials, your county coordinator, and the public. Make your community aware of the dangers it may face (or not face)! The assessment you send to the county will be combined with those of other communities in the county and then used to form a statewide picture of Y2K preparedness. Based on this statewide assessment, we should be able to determine the amount of assistance you can count on locally if there is a serious problem.

- ◆ Adjust your emergency plans accordingly: Ensure that your community emergency plan and procedures are as thorough as possible. Are you prepared to shelter people in mid-winter? How many could you shelter on your own before you need to call the county or State for assistance? Remember, while the chances are remote, this may be a widespread problem. The situations you face locally could happen in many other locations around the state at the same time.

- ◆ Communications and Power: Finally, remember to check communications and backup power systems. As the cornerstone to emergency response, be sure your systems are checked and tested in time for December.

**Where do you begin?**

Work on Y2K issues should be very similar to your work in regard to other potential hazards:

**Step 1:** Identify the services and facilities in your community critical to the safety of public life and property.

**Y2K? OK!****Emergency Management Coordinators- What Should They Be Doing?** *continued*

**Step 2:** Confirm (as clearly as possible) which items in Step 1 may be affected by Y2K problems and which probably will not be affected

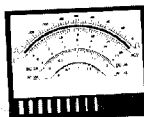
**Step 3:** Ensure that your existing emergency plan and procedures consider the loss of critical systems identified in Step 2 that may not be Y2K compliant.

FEMA has produced a model Y2K emergency planning document that incorporates all of these planning elements. A copy will be provided at the upcoming State emergency management seminars. You can get it in advance from the FEMA web site at: <http://www.fema.gov/y2k/ccmp.htm>.

Remember to document everything at all three steps, and build on the work of others. Check the web for examples of emergency response work. Subscribe to our mailing list and share information with your peers.

As with all other hazards, work with your local officials, and others from areas such as public works, utilities, business, citizen groups, etc., to complete the steps above. As always, you can contact your county Emergency Management Coordinator if you have any questions or need additional assistance. Also, the State will be sponsoring regional seminars targeted at emergency management and Y2K this spring. Be sure to attend!

**Y2K? OK!** thanks the Minnesota Division of Emergency Management for use of its material in this article.

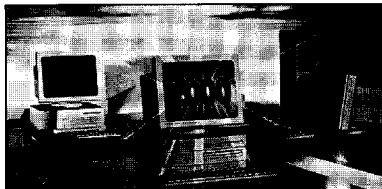
**Have You Tested Your Generators?**

Many government agencies have stand-by generators to keep critical government services operating in the event of a loss of electricity. Good planning practice requires the generators to be tested periodically to make sure they are in good working order. While many to test their backup power systems, many organizations do not test their generators under real life load circumstances and for periods for which they may be expected to operate.

The Y2K planning process is an excellent opportunity for this type of load and stress testing. Emergency managers should work with their local officials and conduct an appropriate test to determine if their emergency electric power will work under true emergency circumstances, and take appropriate action if the systems fails the test.



This Year 2000 Statement is designated a Year 2000 Readiness Disclosure



## Your Little Box of Problems

### The Y2K Dilemmas For Your PC

by Mark Edward Soper

©PC Novice Guide to Y2K - January 1999 - Sandhills Publications

Since the ancestors of today's PCs were introduced about 20 years ago, some farsighted users wondered aloud about the infant industry's retention of an old shortcut: two-digit years. They realized that someday, somebody would have to fix the myriad problems resulting from the inevitable day that 1/1/00 becomes later than 12/31/99. That "someday" has arrived. In less than a year, the world will know whether the computer industry's much-delayed attempts to fix the millennium bug have succeeded.

While most of the world's attention has been fixed on major mainframe systems the government, military, and banking interests use, many of us are overlooking the Y2K problem sitting on our own desks: our PCs. There aren't enough experts to go around, so it should now be painfully obvious that it is up to you to tackle Y2K.

#### The Two-Headed Monster

There are two major causes for the Y2K problem: hardware and software.

**Hardware.** Virtually all of today's PCs have real-time clocks (RTCs) onboard. The interaction between the RTC and the Basic Input/Output System (BIOS) chip causes hardware-based Y2K problems. Most RTCs on motherboards don't know how to switch from one century to another. The BIOS has the responsibility to change the century byte (the part of the RTC that displays centuries) from 19xx to 20xx. If the BIOS doesn't correct the RTC's century byte when the clock rolls over from (19)99 to (20)00, the RTC will still read (19)00, and it will be 100 years off.

**Software.** Software, like the BIOS, has tradition-

ally used two-digit date fields. Software also must be designed to handle the 99 to 00 transition; most software does, but it does so with varying (and incompatible) methods.

You must discover and cure both hardware and software problems to avoid the Y2K problem that otherwise will begin Jan. 1, 2000 (and even earlier, in the case of software that deals with future dates).

Is any PC safe? Hardly any category of Windows-based personal computers is immune to the Y2K problem at both the hardware and software levels. The cure should start with the BIOS chip on your computer's motherboard.

The BIOS chip is responsible for interfacing all of a PC's basic hardware with the CPU, operating system, and applications. Each BIOS chip contains a built-in table of devices for which the BIOS is responsible. These include recognizing and controlling the hard drive and disk drives and interfacing with the CPU and other motherboard components, including the RTC. A BIOS that cannot roll over automatically from 12/31/1999 to 1/1/2000, roll over automatically from 2/28/2000 to 2/29/2000 (yes, the year 2000 also is a leap year), or can't be set manually to 1/1/2000 or to 2/29/2000 as a workaround is a BIOS that helps cause the Y2K problem.

A new reason for upgrading the BIOS. BIOS-compatibility problems have occurred many times during the life span of the IBM-compatible PC family. Traditional reasons for a BIOS upgrade have included the inability to use large hard drives (larger than 504MB, 2.1GB, or 8.4GB), the inability to replace the existing CPU with a faster version, or lack of Plug-and-Play support for Windows 95 or Windows 98.

Now we have to add "inability to handle post-1999 dates" to the list of important reasons for a BIOS upgrade. Because many computers sold as recently as early 1997 have noncompliant BIOS chips, a BIOS upgrade is a real necessity for the vast majority of Intel-compatible PC users.

Because this problem affects most computers with onboard clocks, the only computer categories that lack a hardware Y2K

problem include the early IBM PC and XT machines and their compatibles (8088-based), which have never had a clock retrofitted to them. In virtually every case, most computer users retired these machines long ago, or they have been improved by installing add-on boards with real-time clocks on-board. Adding an RTC to a computer with a noncompliant BIOS is a popular recipe for Y2K problems.

**If I recently bought a PC am I OK?** Unfortunately, not really. While the first articles about Y2K problems started rolling out in early 1996, many vendors waited to fix Y2K problems until late 1997 or even 1998. There is no substitute for looking up your major-brand system on your vendor's Y2K compliance chart or testing your system to determine compliance.

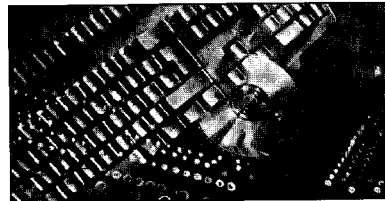
### Getting Started

**Will you need to replace your BIOS chip?** This question isn't as easy to answer as it would seem. The major BIOS vendors (American Megatrends Inc. [AMI], Award Software, and Phoenix Technologies) license their BIOS code to different motherboard/system vendors that may modify the product before using it in a specific system or motherboard. The best way to determine BIOS compatibility is by testing the BIOS. Here are some general guidelines.

AMI pre-1998 BIOS versions, as well as BIOSes previous to AMI version number 6.31.01, are not automatically Y2K compliant. To determine the BIOS version or date, watch the bootup screen for date/version information. Most AMI BIOSes can be manually set to 1/1/2000 or later as a workaround. For more information, navigate your Web browser to [http://www.ami.com/y2k/y2k\\_statement.html](http://www.ami.com/y2k/y2k_statement.html).

Award Software has three levels of Y2K compliance: manual reset of date to 2000 (BIOSes released before April 26, 1994), can't be reset to 2000 (those BIOSes released between April 26, 1994, and May 31, 1995), and compliant (all BIOSes released June 1, 1995, or later). Award BIOS code dated after Nov. 18, 1996, also passes NSTL 2000.exe testing. For help and fixes, go to: <http://www.award.com/tech/y2k.htm>. Award also warns that improper modification of BIOS code by a motherboard vendor can cause Y2K problems for BIOSes that were originally compliant.

Because the Phoenix Technologies BIOS is widely distributed and modified, its Y2K compliance also varies. According to Phoenix's Support Reference: The Year 2000 Web site (<http://www.pttd.com/support/y2k.html>), many, but not all, systems with Phoenix BIOS version 4.0 release 5 and newer should automatically roll over



to 1/1/2000 and beyond. System makers had this BIOS capability available to them from mid-1995, but not all of the system makers implemented the feature, or they may have rolled it out at varying times. Again, test to determine your system's compatibility.

**Finding your vendor.** Your first stop for a BIOS solution is your system vendor. All major system vendors have tested or are in the process of testing their systems for Y2K compliance. With most Pentium-based systems, and sometimes those with older processors (386, 486), the BIOS chip may be a "flash" chip, which is upgradeable with software that you can download from the vendor's Web site or bulletin board and install. Major system vendors normally list their Web sites in their product guides, or they can be easily searched for with any of the major Web search tools. For smaller motherboard and system vendors, finding information can be a lot harder. Try these sites:

- You can use Electronic Data Systems' extensive product database (<http://www.vendor2000.com>) for compliance information about all types of computer products. This database doesn't offer links to the vendors' Web sites.

For links to system and motherboard vendor sites, try one of the following:



A more extensive version of this list for both AMI and Award BIOS motherboards is available from Wim's BIOS page at <http://www.ping.be/bios>. The Award BIOS numbers are linked to the motherboard manufacturers, but relatively few of the AMI BIOS numbers are linked as of press time. This site has a link to Award's flash BIOS Web site for motherboard manufacturer-specific flash BIOS files (<http://www.award.com.tw/download>).

For information that is useful both for upgrading your present BIOS and buying a new motherboard, stop by <http://www.motherboards.org>. Wim's BIOS page suggests this site for links to the motherboard manufacturers it lists.

If you can't get a BIOS upgrade from your system or motherboard vendor, you'll need to upgrade the BIOS chip, get a Y2K BIOS upgrade card, or use software that patches your BIOS when you start the computer.

If you have a clone system, you may be worried. However, because the interaction of the BIOS chip with the RTC is the critical factor in Y2K hardware problems, you can check with your computer's BIOS chip vendor (normally displayed at startup, along with the version number and date) for compliance information. One difficulty you may have is that unlike with most major brands, you may need to pay for a BIOS upgrade.



### The Softer Side Of Y2K

Even if your brand-new Pentium II 450MHz screamer has a Y2K-compliant BIOS and correctly functioning RTC, you still face a host of other Y2K issues, including:

- software that is built into accessory hardware or that supports hardware (device drivers, utility programs), problems with application software, operating system software, utility software, and networking software, and

- date dependencies in the data you create with accounting, database, and spreadsheet programs.

**Firmware Y2K issues.** The notion that only computers have upgradeable firmware (BIOSes) is a big mistake. Many types of products on the market other than computers have firmware that not be Y2K-compliant. For example, Hewlett-Packard's Y2K Web site (<http://www.hp.com/year2000/allproducts.html>) shows the range of possibilities in some of its popular PC and networking peripherals:

- Some HP fax products will display incorrect dates after 1999

- Some OfficeJet printer/fax units have similar problems, with a software patch promised to be available in early 1999.

- HP's popular JetDirect network-printer management software may need updating for some users. One HP multifunction (copier/printer/fax) machine won't allow automatic online registration after 12/31/1999, but it will operate properly.

- Some HP network scanners and CD-ROM towers will require a firmware patch that is presently available.

- Battery backup units with software shutdown features pose another potential Y2K problem. Major manufacturers' present product lines are Y2K-compliant, but you should

check your battery backup's software against your vendor's compliance list and download or purchase new software, if necessary.

Any software can have a Y2K problem. It's important to realize every piece of software on your system, from the operating system to the humblest utility program, can be a source of Y2K problems.

Software vendors typically list their products' Y2K compliance at three levels:

**Noncompliance:** software just won't work with dates past 1999. In some cases, patches may be available from the software vendor; otherwise, you'll need to upgrade. This generally applies to older applications that were replaced by newer products.

**Date Windowing:** two-digit dates are placed in either the 20th or 21st centuries according to the vendor's rules. If every vendor used the same date-windowing method, this would be an acceptable work-around that would work until all such applications became outdated. Unfortunately, not only do different vendors use different date windows, but the same product may use different date windows in different versions. This poses a major problem for organizations or users who pass data between different applications or try to save files in a backward-compatible mode for use with an older software version. Many applications have used this method for several years, and many present software versions still rely upon it.

**Fully Compliant:** this level requires the use of four-digit year dates. Most new software versions achieve this level; however, the import of two-digit year data could cause problems.

You can find an easy-to-read color-coded list of major applications that rates their compliance and provides links to the manufacturers' Web sites at <http://www.blouberg.co.za/y2k/vendor.html>.

### Software Risks

Depending upon the software you use and how up to date it is, you may run into a variety of Y2K-related problems. Here are a few of the most common problems.

#### **Problem: Incorrect interpretation of two-digit year date fields.**

**Software affected:** Accounting, spreadsheet, database applications, custom programs.

**Why it's a problem:** Some older versions of these programs assume all two-digit dates are 20th century (19xx) and can't work with dates past 1999.

**Workaround:** Newer versions of these programs often use a technique called "date pivoting" or "date windowing" that assumes dates before a certain year are 21st century (20xx), while more recent dates are 20th century (19xx).

**What's wrong with workaround:** Different applications, and even different versions of the same application use different date windows.

For example, "24" is recognized as "1924" by Microsoft Excel 5.0/7.0, and Lotus 1-2-3. But, "24" is recognized as "2024" by Microsoft Excel 97 and Quattro Pro versions 7 & 8. Quattro Pro version 6 recognizes "24" as "1924" now, but as "2024" Jan. 1, 2000, and afterward (see chart at bottom of page).

Note that the inconsistency with how two-digit dates are treated can cause "contamination" of data

when spreadsheet files with two-digit dates are transferred from one program to another, or when an older spreadsheet version is updated to the latest release. Four-digit years fix the problem, but this can be a time-consuming change.

#### **Problem: Lack of Y2K information about previous versions of software.**

**Software affected:** Utility, application, and operating systems.

**Why it's a problem:** You're forced to upgrade your software to stay safe.

Utility software is tied so closely to the "state of the art" in operating systems and hardware that using an obsolete utility program can actually risk damage to data. For example, Symantec wisely refuses to test versions of Norton Utilities prior to its final MS-DOS/Windows 3.1 version (version 8) for Y2K compliance because the older versions can't safely support data compression, large hard drives, and other common features of recent computers.

This attitude is far less commendable with other types of software. For example, Symantec isn't testing any previous-version products, including recent releases of Windows 95/Windows products, such as pcANYWHERE32 7.5. Only current (as of end of 1997 or beyond) products are tested. This forces users to either perform their own Y2K-compliance testing or buy the latest version. Because many close-out firms still sell older application versions, check that bargain software's Y2K-compliance before you buy. Buying a noncompliant program at any price is no bargain with less than a year to go to 2000.

This problem also can take place with programs that have been transferred from one vendor to another. For example, IMSI Software ([\[imsisoft.com\]\(http://imsisoft.com\)\) now sells the former Quarterdeck Hijaak Pro graphics converter, which Quarterdeck also acquired by merger. IMSI has no information on Y2K compliance for older versions of this product, and Quarterdeck no longer provides support for Hijaak Pro in any version. If you check the last-known vendor of your software for Y2K compliance and find no mention of your product, it may have been sold or transferred.](http://</a></p>
</div>
<div data-bbox=)

#### **Problem: Recent noncompliant applications with no Y2K fix available.**

**Software affected:** Various applications.

**Why it's a problem:** You're forced to upgrade your software to stay safe.

The lack of software developers' serious attention to the looming specter of Y2K problems can hit you in the pocketbook. Just ask a user of Microsoft's popular FrontPage 97 Web-building software, for example. While many 1997-vintage applications are either fully compliant or require, at most, minor adjustments, FrontPage 97 is noncompliant, according to Microsoft's Y2K information site at <http://www.microsoft.com/technet/topics/year2k/product/product.htm>. Microsoft's answer is for you to upgrade to FrontPage 98. And if you use the server extensions, upgrade those, too. This looks suspiciously like a way to force users into the latest version of a program. FrontPage 98 has better features, but the lack of Y2K compliance in FrontPage 97 means upgrading is no longer a "good idea someday," but a must-do-now requirement.

**Problem: Backups made with non-Y2K compliant software may not be usable past 1999.**

**Software affected:** Tape backup utilities.

**Why it's a problem:** You're faced with discarding your old backups or re-creating them.

You may have several years' worth of valuable financial and other types of data on backup tapes.

In most cases, just switching to the latest version of backup software is all you need to do for Y2K compliance. But, according to Hewlett-Packard ([http://www.hp.com/isupport/cms/cbw\\_y2k.html](http://www.hp.com/isupport/cms/cbw_y2k.html)), users of HP's Colorado Backup for Windows 3.x have a big problem; this software creates backup tapes that can't be used on or after Jan. 1, 2000. The solution? Restore the backup to a

temporary folder, and back it up with a Y2K-compliant version of Colorado Backup for DOS or Colorado Backup for Windows 95.

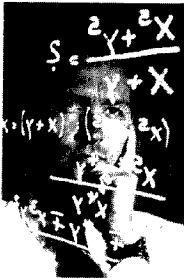
Regardless of your backup software, be sure to verify its Y2K compliance and determine what you must do to make your backups usable in the future.

### Don't Solve Only Half The Problem

You should be spending enough time in the next few months to correct the Y2K problem, but let's assume you pass the buck to somebody else and nobody finds and fixes the problems in time. Fixing just the hardware Y2K problem or upgrading all your software to Y2K standards isn't sufficient. You must take care of both sides of your computer environment to stay safe. Here are some of the problems you could see as 1999 becomes 2000.

Systems running with unresolved Y2K BIOS problems. Operating system or BIOS dates "fall back" to 1/1/1900, causing incorrect date/time stamping of files; incorrect backup software operation, voice mail programs, and other applications due to sorting "old 1900" files before "newer 1999" files; possible discarding of "old 1900" files because of apparent age, even though they are actually the newest files; and software failure because licensing routines look for valid dates and find OS/BIOS dates before their valid dates.

Systems running with Y2K compliant hardware but noncompliant software. Software will fail on and after 1/1/2000 if it is noncompliant; some of the problems include: incorrect sorting of data if the software uses two-digit year data, electronic banking transactions can't be completed, and unreadable date information displayed by applications and/or operating systems for files.



### Kick The Solution In Gear With A Reboot

Because some operating systems (such as Windows 95) will properly display dates past Dec. 31, 1999, if running during the changeover, many systems running utility programs (such as antivirus, backup, or disk maintenance) over the Friday night to Saturday morning roll-over time period may work correctly—until shutdown.

The problem will then take place when the BIOS/RTC is re-read during the next bootup. If Y2K-compliance steps aren't taken, the "century byte" will still indicate 19xx, and your operating system will display (and use) the wrong date, as will the applications that depend upon it.

There is no substitute for examining the hardware and software in your computer and those components connected to it. You must check for compliance and determine what to do now. Waking up after Christmas 1999 is way too late to start.

### Do You Have A Problem?

While the best way to determine if you have a Y2K BIOS problem is to test your system, you may find the following chart useful in estimating the likelihood of Y2K hardware problems.

Non-IBM 8088/8086-based computers with proprietary motherboards usually have real time clocks (RTCs), and all 80286, 80386, 80486, and Pentium class systems do. The interaction of this RTC and the BIOS chip is the source of the hardware side of the Y2K problem. While most of the pre-486 based sys-

tems are already gone, some remain as glorified terminals or low-end workstations. The following chart provides a general overview of the Y2K hardware risk by system type.

This chart, while it references CPU types, is not intended to suggest or state that CPUs are the cause of Y2K problems. According to Intel's Web site (<http://support.intel.com/support/year2000/status/categories.htm>), any Y2K hardware problem on these computer types is not caused by the processor itself. Instead, it's due to the interaction of the computer's BIOS and RTC circuits. All Intel processors, including predecessors to the 8088, have no Y2K issues.

**What about the increasing numbers of non-Intel processors?** Neither Cyrix (<http://www.cyrix.com>) nor "new kid on the block" IDT-Centaur, with its WinChip (<http://www.winchip.com>), discuss any Y2K issues on their Web sites. AMD, the leading non-Intel CPU maker for Windows-based systems, excludes time issues from its standard equipment warranty (<http://www.amd.com/legal/stdwarty.html>). However, because these chips are used with Windows-based systems, often as direct replacements for Intel processors, it's likely the non-Intel CPUs, like Intel's CPUs, are not the cause of any Y2K issues.

This chart reflects the fact that BIOS vendors produced many years of BIOS chips without Y2K compliance and only recently began to ship Y2K compliant products with Intel-compatible PCs.

Computer Category	With Clock	Likelihood Of Y2K Hardware Problem
8086/8086	No	No
8088/8086	Yes	Very Likely*
80286	Yes	Very Likely
80386	Yes	Very Likely
80486	Yes	Likely
Pentium	Yes	Less Likely
Pentium Pro	Yes	Less Likely
Cyrix CPUs	Yes	Varies
IDT-Centaur WinChips	Yes	Varies
AMD CPUs	Yes	Varies
Pentium II/Celeron	Yes	Unlikely*

\*Some of these computers have an RTC clock circuit on the system board while others (primarily IBM PC/XT and clones) have an RTC included as part of a third-party add-on board (such as the AST Six-Pack and Quadram QuadBoard). The presence of an RTC circuit would cause the problem. The American Quadram company is long out of business, and while AST is in business at <http://www.ast.com>, its Web site has no Y2K-specific information about any of its once-popular add-on boards with RTC circuits (such as the RamPage).

\*\*This is due to the relative newness of these systems, with most built in late 1997 and more recently, coming with Y2K compliant BIOSes as standard.

### Relax If You've Taken A Byte From Apple

Apple Macintosh users have an easier time of it, according to Apple's Apple And The Year 2000 Web site (<http://www.apple.com/macos/information/2000.html>). The earliest 1984-model Macs featured accurate real-time clock calculations into the early months of 2040, while today's Macs can work with dates as late as 29940.

The chart below compares Macintosh computers to Apple's historic Apple II series, still in use in limited quantities.

Computer Category	With Clock	Likelihood Of Y2K Hardware Problem
Macintosh	Yes	No
Apple IIs*	Yes	Varies*
Older Apple II family	No	Varies**

\*The Apple IIs requires System 6.0 or later operating system to be Y2K compliant when using GS-specific software. When using generic Apple II (8-bit) software, ProDOS 8 v2.0 must be used to be Y2K compliant.

\*\*These units can have a clock retrofitted to them to keep time internally. Check with the clock vendor for Y2K issues.

### Fixing Y2K Problems On Standalone

As we approach the next millennium, and subsequently, the Year 2000 problem, much of the attention has been focused on large network or mainframe systems and the problems they potentially pose. However, your standalone PC is not immune to Y2K problems. Here, we tell you where you may encounter trouble, and what you can do about it.

#### Determining The Problem Areas

Your computer is a combination of hardware, software, and firmware subsystems, and each of these subsystems must be able to keep working after the date changes from 12/31/(19)99 to 1/1/(20)00. On the next page, you can see the subsystems found in the typical computer (see the "Risk Of Y2K" chart).

Why are different parts of the system more likely to have problems with Y2K than others? The high-risk parts of the computer are those associated with system date/time calculation and determination. A popular Y2K utility program such as RightTime's ViewCMOS (available from <http://www.righttime.com>) shows that the Basic Input/Output System (BIOS) chip on the motherboard (BIOS chips are firmware, that is, software stored in a chip); the real-time clock (RTC) on the motherboard; and the operating system (such as Windows 95 or Windows 98) all independently track date and time changes. It's possible to have one or two of these components properly roll over to 1/1/2000, and have the remainder roll back to 1/1/1900. Detection and resolution of Y2K



problems must involve these parts of the computer.

Software residing on the computer also is a major risk for Y2K problems, depending upon its nature and its age. Software that works extensively with dates—accounting, home finance, spreadsheets, and database applications, for example—is extremely vulnerable to Y2K problems and can create Y2K problems through improper handling of date information. Many other types of software are less vulnerable to the creation of Y2K problems but can still be adversely affected by Y2K issues. Any attempt to detect and resolve Y2K problems on a given computer must include that computer's software.

Virtually any computer is connected to peripherals, whether sound cards, mice, modems, or printers. While these products could theoretically have Y2K issues, virtually none of them do. Storage devices and peripherals don't do any date processing; therefore, they can't cause any Y2K problems unless their driver software isn't Y2K compliant.

#### Working With Your Computer's High-Risk Areas

Because the BIOS chip and the RTC chip (both found on the motherboard) handle date and time information, they can be a major

cause of Y2K problems. To reliably detect a Y2K problem, you must start the computer with a special diskette, rather than perform date-time tests after Windows boots normally. If you perform date/time changes within Windows, here's what could happen:

Software with date-detection features for licensing (such as 30-day trial test versions) could stop working.

Software that is not Y2K-compliant could stop working or create bad data, so it's vital to perform all Y2K tests listed below from the bootable diskette.

#### Detecting Year 2000 Clock Problems (BIOS/RTC)

First, create a startup diskette by inserting a blank diskette into your diskette drive. Right-click the Desktop, then select Format from the pop-up menu. On the Format menu, select Full and Copy System Files. This will rewrite the diskette's magnetic structure and copy startup files to it. After the Format program has completed, shut down the PC.

Restart the computer and press the appropriate key(s) to take you into the BIOS setup screens. Most computers indicate on-screen which key(s) to press. If you don't see a message and if your computer doesn't come with a special utility startup diskette for BIOS changes, try one of the following keystroke(s) as you boot the computer: DELETE, F2, ESC, F1, CTRL-INS, CTRL-ESC, or CTRL-ALT-ESC.

Note the correct key(s) to use because you'll be adjusting the time in the BIOS setup screens again later. If the first keystroke you try doesn't work, press the F8 key in Windows 95 or F5 key in Win-

dows 98 and select a Command Prompt Only startup mode. After you see a system prompt displayed (C:\> or A:\>), press CTRL-ALT-DELETE to restart the computer and try the next keystroke(s). Repeat as needed until you see a BIOS setup screen or setup menu.

Go into the Advanced CMOS, Advanced Setup, CMOS Features, or similar screens and look for an option such as Boot Sequence or Boot Order. Write down the present setting and change it, if necessary, to A:, C:. This will use the special startup diskette you made, which the system will use to start the system. Save the changes to your BIOS setup and restart the computer. After restarting the computer, press the appropriate key(s) to enter the BIOS setup screens.

Go into the Standard BIOS Setup screen and find the date/time fields. Write down the present setting (which should be no more than a minute or two off your office clock's display). Change the date from the present value to 12/31/1999 (or 12/31/99). Change the time to 23:59:30 (30 seconds before midnight on New Year's Eve). Watch the clock advance toward midnight. If the date changes to 1/1/2000, your computer has passed its first Year 2000 test. If the time reverts to 1/1/1980 or any other date before 1/1/2000, your computer has flunked.

If your computer rolls forward successfully under power, go back to the time and date fields and change the date back to 12/31/1999 and the time to: 23:59:00. Save the changes and exit the BIOS setup screens. Turn off the power after the memory count is performed. Wait five minutes and restart the computer. Again, access

the BIOS setup screens and check the date and time. It should be 1/1/2000 and about five minutes after midnight. If the date is anything other than 1/1/2000, your computer has flunked the power-off Y2K rollover.

Many computers that were built before 1997 (and some newer models) are likely to fail either one or both of these tests. Be sure to reset correct date/time and boot order in your BIOS before removing the diskette and restarting the computer for normal operation.

### Solving The Y2K BIOS/RTC Problem

If your computer fails to roll over to 1/1/2000 during power up, try the following:

■ **Manual Reset.** Set the date manually to 1/1/2000 and the clock to 0:05:00 (five minutes after midnight), save the changes and shut down the computer. Restart the computer, enter the BIOS setup screens, and see if the date and time were retained. If the date remains 1/1/2000 and the clock is advancing normally, you can do the following to avoid a Y2K rollover problem:

■ **Shut down the computer before midnight Friday, Dec. 31, 1999.** Restart it Saturday morning or later and manually set the correct date and time. Many computers that can't roll over automatically can be forced to do so with this manual date/time setting method. Computers that can't roll over automatically must not be running overnight during the 12/31/1999 to 1/1/2000 rollover period.

If your computer must be kept running overnight at all times (because of a dial-up modem, Web connection, fax receiving, etc.), you have two options: use RTC date-correcting software or upgrade the BIOS.

Even if your computer can roll over to 1/1/2000 while you watch, you should still save the changes, power down, wait five minutes, and turn on the computer. Again, enter the BIOS setup screens and see if the date remains 1/1/2000 and the time has advanced normally. If the date is earlier than 1/1/2000, the computer cannot retain the Y2K date and you must upgrade the ROM BIOS.

### Why Use Software?

Many vendors offer a software solution to RTC/BIOS clock problems. These programs place a terminate-and-stay-resident (TSR) program in your computer's Autoexec.bat file, which is run whenever your computer is started. These programs correct clock errors in a similar fashion to a BIOS upgrade. Some are included as part of comprehensive utility software packages (such as Network Associates' Nuts & Bolts 98) or with Y2K testing programs.

This solution requires an online purchase or download, or the purchase of a commercial utility program. It can be implemented in less than 15 minutes, and it is easy to do; pricing varies.

Installing software to fix your RTC/BIOS clock problems is ideal if you have an older computer that you may not keep long after 1999, or if you have a system that doesn't permit any type of BIOS upgrade.

If you adopt this type of fix, make sure the program will work with any operating system your system uses (or that you may upgrade to), and make sure you don't remove the program from the Autoexec.bat file. As with any Y2K fix, test your system after installation to verify the fix works.

### Upgrading The BIOS.

If your computer can't be shut down and restarted during the 1999-to-2000 transition or won't retain the 2000 year, and you prefer a hardware fix over a software patch, you will need a BIOS upgrade. A Y2K-compliant BIOS will provide correct rollover of dates from 1999 to 2000 whether the computer is running or not during the transition.

In addition to providing Y2K compliance, many BIOS upgrades also will allow you to use large hard IDE/ATA hard drives (up to 8.4GB or more), provide proper support for upgraded CPUs, and provide support for LS-120, Zip, and other drives as BIOS-controlled, bootable devices.

**What to do first.** First, you need to back up your hard drive, especially the data you have created. In case of problems with your system, you'll want to be able to move your data to another system and keep working. You also will want to track down the software's CD-ROMs or diskettes in case you need to reinstall any software after the upgrade.

To get a BIOS upgrade, you can either download one from your system or motherboard vendor. All this requires is a bulletin board system (BBS) connection or World Wide Web connection, and about 15 minutes or so of your time. It is not difficult to do, and it usually is free.

Getting and using a downloadable BIOS upgrade. First, contact the system or motherboard vendor for the flash BIOS file you must download. Most system vendors have an online database of models and the appropriate BIOS files. If you're trying to upgrade a motherboard instead, check these sites:

- Windriver.com's list of manufacturer Web sites and FCC ID# search feature at: <http://www.windrivers.com/company.htm>.

- Award's motherboard site at <http://www.award.com/tech/upgrade.htm>, and Wim's BIOS site at <http://www.ping.be/bios> have cross-references that let you determine the motherboard manufacturer from the special code numbers displayed by many systems at startup time.

- Wim's BIOS site also has a link to Award's flash BIOS Web site for motherboard manufacturer-specific flash BIOS files at <http://www.award.com.tw/download>.

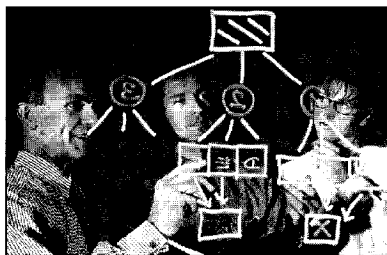
Also try <http://www.motherboards.org>.

Download the file, making sure the file you are receiving is the correct one for your system or motherboard (using the wrong flash BIOS file will

destroy your BIOS and disable your motherboard).

Install the BIOS upgrade to a diskette, then back up your present BIOS code to a different diskette, if possible.

Follow the BIOS upgrade procedure. This usually consists of booting the computer with the BIOS diskette; most upgrade programs will automatically start. Wait until the program is finished before rebooting or powering down the computer. The process typically takes between three and five minutes.



### Replacing Your BIOS With A Third-Party Update

Another way to upgrade your BIOS is to physically swap out the chip. This method is recommended when you can't get a BIOS upgrade from your system or motherboard manufacturer, you don't want to use a software patch, you don't want to use a BIOS upgrade card (see below), you plan to keep the computer for several years, or you cannot or prefer not to replace the motherboard with a new one with a Y2K-compliant BIOS.

You will need tools to open your system's case, and about one hour of your time. There is a moderate level of difficulty associated with this method, so if you are uneasy, get some help from an expert. This solution will cost you about \$60.

Ordering and installing a third-party BIOS upgrade chip. First, you will need to provide your vendor with motherboard details about your system. Watch for a long string of numbers across the top or bottom of your screen during the initial startup procedure (before the operating system starts). This information indicates your system's motherboard chipset and other details that are used to match a new BIOS to your existing motherboard. Ask your vendor which numbers are significant. Verify that the new BIOS

chip will provide Y2K compliance. It is likely to provide additional benefits to your system like the flash BIOS upgrades listed above.

Leading BIOS upgrade vendors include Micro Firmware at <http://www.firmware.com> and Unicore Software at <http://www.unicore.com>. These upgrades usually allow for additional upgrades in the future by means of flash BIOS downloads (see above).

Before you install the new BIOS upgrade chip, start your computer, enter the BIOS setup program, and record important information, including hard drive data (such as the number of heads, cylinders, sectors per track, landing zone, and write precompensation) for each hard drive in the computer. Don't record the size because the new BIOS will automatically calculate this from these numbers. You also need to record diskette drive data (which drive type for A: and B:, if you have two drives).

The drive information is listed in the standard setup screen. Change screens and record other setup information. You can do this most easily by attaching a printer to the LPT1 port and leaving it on while you start the computer with your boot diskette. This initializes the printer port so you can print screens. Restart the computer using CTRL-ALT-DELETE and enter the BIOS setup screens. Use the PRINT SCREEN key to print each screen (two screens will fit on each sheet of paper). Use this information to reconfigure the new BIOS chip.

Open the computer and locate the existing ROM BIOS chip. Ground yourself by using an anti-static wrist strap to avoid damaging parts with static discharges. You may need to remove inter-

face cards or other components to find the BIOS chip. It usually has a label indicating the BIOS manufacturer (such as Award, Phoenix, American Megatrends [AMI], or Microid Research [MR]) or system maker (such as Acer, Compaq, or IBM). Sometimes it is labeled simply with a sticker such as "B". It is a socketed rectangular chip about 2 inches by 1 inch. Note the orientation of the existing BIOS chip; the new one must be lined up in the same direction (look for a notch on one end). Remove it using the chip puller supplied with the new chip and place it on the antistatic foam in

case you need it again.

Carefully insert the new BIOS chip in place of the old one. Check to see that the notched end of the chip matches the notched end of the socket. Then, push it firmly into place.

Restart the computer and follow the new BIOS chip's instructions to enter its setup program and re-enter drive and other required information as recorded above. The setup screens may be different, so use the new chip's documentation as a guide.

Finally, test the system for Y2K compliance as before.

### Installing A Third-Party BIOS Upgrade Card

The last way you can update your BIOS is to install a third-party BIOS upgrade card. This method is recommended when you can't get a BIOS upgrade from your system or motherboard vendor, you can't purchase a BIOS upgrade chip, you prefer not to use a TSR program (see above), or you cannot or prefer not to replace the motherboard with a new one with a Y2K-compliant BIOS. These cards also may come with large (more than 8.4GB) hard drive support at an extra cost.

You will need the appropriate tools to open your PC's case, and a free ISA expansion slot inside your system. Consult your PC's documentation to locate this. This fix will take you a little less than an hour, and it costs about \$60. Again, there is a moderate level of difficulty with this upgrade, so if you are unsure about what you are doing, consult an expert.

Installing a BIOS upgrade card. First, open your computer and verify that you have the appropriate type of expansion slot available. Virtually all Y2K cards use either an 8-bit or a 16-bit ISA slot (which is longer than the PCI slot typically used for video cards on Pentium systems). Most 486 systems have these, and VL-Bus slots contain ISA slots. Make sure the slot isn't being "shared" with a PCI card in use (a shared or combo slot has less space between the ISA and PCI slots than normal, preventing simultaneous use).

Next, install the card into the open ISA slot and follow the manufacturer's setup instructions.

### Is Changing The BIOS Enough?

Opinions vary widely among users because a few specialized applications don't access the RTC through a software/firmware route (such as TSR software or the BIOS). Instead, they directly access the RTC, which on most computers doesn't track centuries. Such programs may still be vulnerable to Y2K problems, even with a Y2K-compliant BIOS. This problem is taken so seriously that the British standard for Y2K-hardware compliance calls for both the RTC and the BIOS to be compliant.



To determine if you have a risk, you should:

- **Contact your software vendor(s)** to determine how their applications access the RTC. If RTC access is via the BIOS, a TSR fix or BIOS upgrade will keep things working. If the RTC is accessed directly, you could have a problem.

- **Download RightTime.com's** testing software and use the included ViewCMOS utility to display the RTC, BIOS, and operating system clock during the 1999-to-2000 rollover. Try it in both a live rollover mode and after being turned on in "2000." If your RTC doesn't indicate "2000" when the BIOS and OS clocks do, any software that accesses the RTC could cause a Y2K date problem.

- **If you use software that directly accesses the RTC,** contact Dallas Semiconductor at (<http://www.dalsemi.com>). Many motherboards use Dallas RTC chips, and Dallas offers Y2K-compliant versions of these chips. You may be able to replace a noncompliant chip on your system.

### Dealing With Software

Even late-model computers with Y2K-compliant BIOS chips are still vulnerable to Y2K problems because of the software they use. Because computers without software are useless, it's vital to also check your software for problems.

- **Software Problems.** Whether it's your computer's operating system or applications, software issues fall into these categories:

- **Noncompliant**—the software program can't work with post-1999 dates and can't be

patched. You must replace it.

- **Compliant after updates**—the software must be patched in order to reach Y2K compliance.

- **Compliant**—the software is compliant with Y2K dates.

It's important to realize "Y2K-compliant" software definitions assume other parts of the computer also are handling date issues correctly. Thus, you should get your hardware working correctly before checking and updating your software.

Find your software vulnerabilities and solve them. First, you must determine what software your system has and contact the vendors of that software for Y2K-compliance information. You should create a checklist where you can record software information and vendor details about Y2K compliance.

Start with your operating system. Go to a command prompt and give a command such as VER (DOS/Windows) to determine your operating system version. This also is available by looking at the system properties sheet, but VER is usually more specific.

Then, move to your applications. Start with the ones for which you have Desktop shortcuts or Start button access. To determine the version, you have a couple of options.

You can start the application and look for version information in the "splash screen" logo most programs display, or after the program is started, get more detailed version information from the Help menu under the About (this program) option found in typical menu systems.

After you've noted version information about the programs on your Start menu and Desktop, you should also check for any programs you use that you start from the program icon in Windows Explorer. Use Windows Explorer to change to the appropri-

ate folder, run the program, and check the version information as listed above.

With the version information listed, it's time for research. Your fastest route to checking Y2K compliance is to go to your software vendors' Web sites and look for an option such as Y2K, Year 2000, and so forth. Most vendors put this link to their Year 2000 information on the home page. If you don't see it there, look for a Site Map or Site Directory button that displays the entire site. You should be able to find it there.

Once you've located the Year 2000 information, look for a software-version listing and look up your version information to determine Y2K compliance. Unless you're using the latest software releases, you'll usually find you must do one or more of the following:

For many recent (and even some current) software versions, you'll need to download one or more update, or "patch," files and install them. These patches will change the parts of the program you're updating to handle Y2K problems and many others issues (even if your software is already Y2K compliant, installing these downloads is a good idea). Before you start the process, note these details:

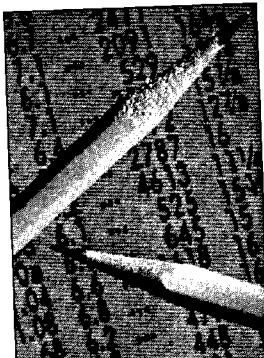
- **Which download(s) do you need?** Because software companies like to quietly make improvements to their software while keeping the same version number, some users of any program may need to make Y2K updates while others won't. Make sure you look closely at the version information, and take any additional steps needed to determine if any listed update is required for your software. For example, with one ver-

sion of Microsoft Access, the Y2K handling of dates changes according to the version of a single program file. If the site lists multiple service packs or patches, determine if you need only the latest one, some of the earlier ones and the latest one, or all of them (patching your software for non-Y2K issues also is a good idea).

#### How large is the download?

The larger the file(s), the more likely it is that you may experience a problem with the download. If your Internet service provider (ISP) or Web browser software (Navigator, Internet Explorer, etc.) automatically disconnects you after a period of inactivity, watch out. Downloading a large file without looking up pages makes these services believe you've wandered away from your machine, and they'll pull the plug on you. The only thing more frustrating than a long multimegabyte download is losing the connection before you're finished, forcing you to start over. To avoid this, you can do a bit of surfing to other sites while the download is continuing. You also may want to install a "ping" utility, which sends out signals to other Web sites to simulate activity and keep your connection running.

Make sure you have suitable storage available, especially if you can't download to the computer that needs the software upgrades. You'll typically need a Zip drive, LS 120, or compact-disc recordable/rewritable (CD-R/CD RW) drive to move your download to the machine you're updating because the typical patch file is much larger than the 1.44MB capacity of the typical diskette.



#### Check Your Data.

Even if you determine that your computer and programs are Y2K compliant, bad data could still haunt you. Watch for the use of two-digit year dates in your spreadsheets, accounting, database, and similar programs. Manufacturers of these products have recently begun to add "date-windowing" methods that make assumptions about which century "92" is in, but it's risky to depend upon these methods for long.

This is because different manufacturers use different date windows. Some versions of Quattro Pro, for example treat 50-99 as 1950-1999 and 00-49 as 2000-2049; however, Microsoft's Excel product has changed its assumed 19xx date window from 1920-1999 (20-99) to 1930-1999 (30-99) in the latest version. Sooner or later, two digit dates will cause you a problem because the software will make different assumptions about the century than you will.

#### How to fix two-digit dates.

There are a variety of methods you can use to fix two-digit dates. Before you try any of them, make backup copies of all your data files.

For spreadsheets, use software such as Network Associates' 2000 Toolbox (<http://www.nai.com>) and Norton 2000 (<http://www.symantec.com>) that checks for two-digit date fields. You can use these programs to alert you to date fields and calculations that use dates, and often can fix the data files themselves. Make sure all new spreadsheet data files use four digit years.

For accounting software, start 1999 off right and start using four-digit years. This is critical for two reasons: one is the "date window" issue mentioned above, and the second reason is that keying shortcuts are changing. In Intuit's popular Quicken home-accounting product, for example, the keyboard shortcut that means "20xx" in older versions now means "19xx." Check with the vendor to see if you need to fix existing 1998 or older files with two-digit year dates.

For spreadsheets and databases, see if you can do an extensive find/replace or search/replace. Make sure you confirm all of your changes, otherwise you may change numerical, nondate data by mistake. For all software, start using four-digit dates as soon as possible. You may not need to access old data, but new data could certainly cause you problems if the year isn't absolutely clear. If your present software doesn't support four digit years, check on an upgrade.

#### Fixing Typical Systems

To get you started on your Y2K odyssey, we'll show you how to fix a typical 486-based and Pentium-based system. However, this is not a blueprint for all PCs; remember,

there is no substitute for analyzing the hardware, software, and firmware in your own system.

#### 486-Based System

■ **Hardware.** This typical system fails Year 2000 BIOS rollover tests, but it can be manually set for 1/1/2000 and beyond. Recommended fix: turn off the system on 12/31/1999 and reset on or after 1/1/2000 to correct the date.

■ **Operating System.** Our typical system uses Windows 95 (original upgrade release). It does have minor issues that can be fixed with patch. Recommended fix: download and install patch. You can get the patch at <ftp://ftp.microsoft.com/softlib/mslfiles/WIN95Y2K.EXE>.

■ **Accounting Software.** We're using Intuit's QuickBooks Pro for Windows, version 5. Timer, electronic banking, and payroll features will not work after Dec. 31, 1999, but the rest will work. This product uses two-digit dates only. Recommended fix: plan an upgrade to the latest version of Quickbooks Pro, or download and install software patch when available (estimated ready date: end of May 1999).

■ **Desktop Publishing Software.** We have Microsoft Publisher 1.0a. This product is not Y2K compliant and no patch is available. Recommended fix: update to latest version of Microsoft Publisher.

■ **Zip File Management.** For our example, we're using Niko Mak's WinZip 6.2. The manufacturer recommends upgrading to the latest version, even though this version is Y2K compliant. Recommended ac-

tion: upgrade to latest version.

■ **Office Suite.** Using Corel WordPerfect Suite 8. This product is Y2K compliant. Date window of 50-99=1950-1999; 00-49=2000-2049. Recommended action: advise use of four-digit dates in Quattro Pro spreadsheet component to avoid ambiguities in data or chances of data corruption when transferring data to/from other programs.

#### Pentium-Based System

■ **Hardware.** Our example system fails year 2000 rollover tests, but it can be manually set to dates of 1/1/2000 and beyond. Because the computer is frequently used overnight, a BIOS upgrade is desirable. Recommended action: download flash BIOS upgrade from the manufacturer. Other benefits include upgrading to faster CPUs.

■ **Operating System.** We're using Windows 95 (OSR2.x/Win95b). It has minor issues that can be fixed with a patch. Recommended fix: download and install patch. You can get the patch at <ftp://ftp.microsoft.com/softlib/mslfiles/WIN95Y2K.EXE> (the same patch can be used for all Win95 releases; the install program detects Win95 release and installs correct patch).

■ **Desktop Publishing Software.** Our typical system uses Adobe PageMaker 6.0. It has not been tested for Y2K compliance by the manufacturer because it is not a current product. Recommended action: order and install upgrade to PageMaker 6.5.

■ **Graphics Utility.** We're using Hijaak Pro version 4.00 for file conversion. Software was sold by Quarterdeck at the time

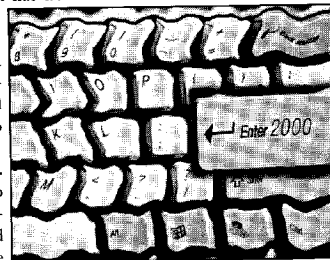
of purchase, but it is now a product of IMSI Software (<http://www.imsoft.com>). IMSI lists the product as Y2K compliant. Recommended action: no upgrade required.

■ **Internet FTP (File Transfer Protocol) Software.** Uses CuteFTP1.6. No Y2K-compliance information is available for this version. The present version, 2.6, is Y2K compliant. Recommended action: purchase version 2.6.

■ **Backup Software.** Uses Iomega Ditto Tools. No version information available, but the drive is more than 18 months old. The present version, 3.2, was introduced in September 1998 and is Y2K compliant. Recommended action: upgrade to version 3.2 at <http://www.iomega.com/software>.

■ **Uninstall Software.** Our typical system uses Quarterdeck Remove-It 95. No Y2K-compliance information is available. The present version, Remove-It 98, is Y2K compliant. Recommended action: purchase Remove-It 98.

■ Your desktop system may not force planes out of the sky or cause huge blackouts, but it can cause problems for you if you neglect fixing it. Don't wait. Bite the Y2K bullet now; it will save you a lot of trouble come December 1999.



**Risk Of Y2K**

Subsystem	Type	Problems
BIOS	Firmware	High
Operating System	Software	High
RTC	Hardware	High
Applications	Software	Variable
Utilities	Software	Variable
Video	Hardware	Low
Audio	Hardware	Low
Drives	Hardware	Low
Keyboard	Firmware	Low
Mouse	Hardware	Low
Data	Software	Variable
Peripherals	Hardware	Low

**Y2K? OK! Techie Quiz**

Don't believe all the gloom and doom you hear about year 2000 testing of PCs. Here are seven true-or-false questions to clear some of the fog. (Courtesy of Government Computing News)

**1. All real-time clocks— even those in the latest Pentium III systems—will fail year 2000 readiness tests.**

*True.* Real-time clocks will fail readiness tests. That's because the RTC was not designed to hold century information, which resides in the CMOS memory. Fixing the BIOS remains vital, however, because the BIOS controls the CMOS chip, which includes the RTC and memory banks.

**2. Because the RTC is hardware, it needs a hardware fix.**

*False.* Several companies claim the only way to fix an RTC is to install a new card or new chips—a waste of tax dollars. The BIOS controls the RTC and CMOS. A ready BIOS will update the CMOS date code information without a hitch.

**3. Fixing the BIOS will fix the hardware.**

*True.* Most Pentium systems have updated BIOSes you can download for free from the manufacturers' Web sites. A 486 or older PC needs a software patch that corrects any errors. Again, most computer makers offer this for free.

**4. A fixed BIOS means a fixed PC.**

*False.* A corrected BIOS only makes the computer hardware give the correct date. This is primary and vital, but the PC as a whole will not be ready until you fix any errors in the operating system, applications and data.

**5. PCs running Microsoft Windows NT do not require BIOS fixes for the year 2000.**

*True.* Windows NT controls the CMOS chip and acts as a wall

between the hardware and software. In other words, NT performs the BIOS function for the 2000 rollover. Updating the BIOS will not hurt and could prevent other glitches, but NT by itself will update the CMOS memory's century entry.

**6. When Jan. 4, 2000, passes, it's safe to uninstall year 2000 test software.**

*False.* Year 2000 readiness is ongoing. Data files and applications might have hidden problems after Jan. 1. A good software utility will keep you on track.

**7. Year 2000 is only a problem for computer dates.**

*False.* Think about how you habitually note the date on memos and personal checks. Do you write or type, say, 5/1/99 or May 1, '99? If so, you should immediately get in the habit of including the century digits. Computer software will make assumptions about which century you meant, and that could introduce errors. Perhaps you are referring to census data from 1920, but if you type 05/01/20, the computer might think you mean May 1, 2020.

*Did you score seven correct answers? You're a lucky one. You're ready for year 2000, and your agency's systems are in good hands. Six or five correct? Pretty good. You probably also know that 2001, not 2000, is the start of the next millennium. Four or three correct? Not great. Time to start asking the doomsayers some hard questions. Two or fewer correct? You're in trouble. But don't build a bomb shelter and stockpile food just yet. You have less than 250 days to study up.*



## Microsoft Announces Y2K Tools, Services

**F**or the many local units that use Microsoft products, you should be aware of Microsoft's Y2K site at [www.microsoft.com/y2k/](http://www.microsoft.com/y2k/).

Microsoft recently announced tools and services designed to assist customers through the Year 2000 date change. Available free of charge on the Microsoft Website, the tools include product analysis, Excel date-correction plug-ins, an upcoming upgrade to the Microsoft Systems Management Server 2.0, several information services, and shortly, a Windows 95 patch. Microsoft is also making available the Year 2000 Product Guide Workbook, a spreadsheet containing product names, languages, compliance status and available Y2K updates or patches.

Microsoft will provide consumers and IT professionals access to a free bi-weekly Y2K mailing list of product and information updates. A Year 2000 Newsgroup is now available. Chat with your peers and hear their solutions for troubleshooting year 2000 issues. The site also includes a Frequently Asked Questions page to help you understand this complex issue.

Microsoft said all future products will be Y2K compliant, but it did not commit to provide Y2K updates for all products. Information on Y2K status of individual products can be obtained on the web site. Customers pay need to pay for upgrades to the compliant versions of Microsoft applications in order to receive free updates and fixes.

### Microsoft Product Analyzer

Users will be most interested in an software inventory and analysis tool, Microsoft Product Analyzer, which collects a list of Microsoft software on a PC for comparison with a product compliance database. If upgrades or fixes are required, the Analyzer provides links for immediate downloading. The free utility, which is available on the Microsoft Y2K Web site at <http://www.microsoft.com/technet/year2k/pca/pca.htm>, and on a free Y2K Resource CD, which can be obtained by calling 1-888-673-8925.

The Microsoft Year 2000 Product Analyzer performs the following tasks:

- Identifies installed software products on specified drives by scanning the drives for executable files



- Compares the resulting list of products to the products listed in a compliance database
- Generates a report of the compliance levels of the products it discovered, based on the information in the compliance database

The Microsoft products compliance database is supplied with the Microsoft Year 2000 Product Analyzer. The PC Analyzer download is compact enough to be placed on a floppy disk for easy installation on multiple PC's.

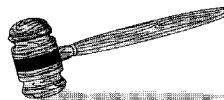
### Windows 95

Microsoft Corp. is preparing an update for Windows 95 intended to help IT managers make sure their desktops are Y2K OK. The Y2K update for Windows 95 will bring the company's most popular desktop operating system up to full Y2K compliance from its current status of "compliant with minor issues. In the case of Windows 95, those minor issues won't cause data to be lost but may cause the operating system to display certain dates incorrectly, said Don Jones, Microsoft's year 2000 product manager. The update, sources said, will be in the form of a patch that adjusts the way the OS addresses dates. An exact release date for the Windows 95 fix was unavailable. Users with concerns should watch the computer press or check the Microsoft web site regularly for release announcements.

### Excel

Excel users can download free enhancements to the spreadsheet application that search for and correct two-digit dates. The Date Fix Wizard searches for and changes dates in spreadsheet files. The Date Migration Wizard converts two-digit dates for years 20 through 29 in Excel workbooks. The Date Watch Wizard monitors new spreadsheet data files to prevent entry of ambiguous dates and date formats.

## Year 2000 Legal Liability — Articles And Other Material



There are a very large number of articles, books and websites that discuss the legal aspects of the Y2K problem. This article does not attempt to list all of them. The selection set forth below is intended only to acquaint readers with a small portion of the many books and articles that exist. These items are offered for informal, general information purposes and should not be relied upon as legal advice. Listing here should not be considered as an endorsement or recommendation of these articles and sites.

Local units should consult with their legal counsel to discuss the many legal issues associated with Y2K, such as how to prepare and follow a due diligence plan; what contractual or other remedies may be available; potential exposure to legal claims; the obligations of issuers of securities; and, the protections available under the Federal Year 2000 Information and Readiness Disclosure Act.

1. "Legal Issues Concerning the Year 2000 Computer Problem: An Awareness Article for the Private Sector", by Jeff Ginnett, Esq. <http://www.year2000.com/archive/NFlegalissues.html>. This article summarizes the major legal issues which may arise due to the Year 2000. It is written for lawyers and non-lawyers. It provides useful information on legal audits, contract forms, software licenses and copyright restrictions. It also provides information on accounting standards which may mandate disclosure and discusses other disclosure and insurance issues. It discusses potential causes of action against hardware and software providers, consultants, product manufacturers, insurers and possible defenses to such causes of action.

2. "Beyond Awareness: Ten Management and Ten Legal Pitfalls Regarding the Year 2000 Computer Prob-

lem That You May Not Have Considered, Yet!", by Warren S. Reid and Steven Brower. This article can be found at <http://www.wsrcg.com/BeyondA.htm>. This article discusses ten management issues and ten legal issues regarding Y2K such as who will be the most likely defendants, how vendors can limit their potential liability in new sales, goods and services and what type of insurance will be involved in Y2K lawsuits.

3. The Y2K Law Site <http://www.y2k.com/legalpage.htm>. This site of the firm of Williams, Mullen, Christian and Dobbins of Richmond, Virginia provides information regarding legal and business management issues that may arise as a result of Y2K.

4. Year 2000 Information and Readiness Disclosure Act, P.L. 105-271 (15 U.S.C. §1 note). In this act, Congress has encouraged the exchange of information about solving Year 2000 problems by establishing legal principles regarding disclosure and exchange of information relating to Y2K. It provides some legal protection for statements relating to "Readiness Disclosure."

5. "Reduce Your Township's Year 2000 Risk" by Robert E. Lee Wright, Esq. (on the Division of Local Government Services web site: <http://www.state.nj.us/dca/lgs/pages/y2kpg1.htm>). This is an article by a Michigan attorney regarding the potential legal problems for townships if they are not Y2K compliant. It discusses the claims that could flow and the steps that a township should take to evaluate the extent to which it is at risk of being sued. It also discusses how to determine if the township can legally correct software and equipment it uses. It provides information on precautions to take regarding written communications so as to optimize the township's litigation position.

6. "Year 2000 Contracting Issues With Customers and Vendors", by J. Stephen Hufford (Practicing Law Institute Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series (June, 1998)). This article addresses Year 2000 contracting issues with customers and vendors with an emphasis on issues relating to mergers and acquisitions.

7. "The Year 2000 Problem: U.S. Government Procurement", by Mary Shallman, (Practicing Law Institute Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series (June 1998 (Discusses the Federal Acquisition Regulations which express the Federal Government's intention to acquire only those products that will work in the Year 2000 (see 48 C.F.R.). It also provides the General Services Administration's model Year 2000 compliant warranty language.

8. The Securities and Exchange Commission Interpretation "Disclosure of Year 2000 Issues and Consequences by Public Companies, Investment Advisers, Investment Companies and Municipal Securities Issuers" 63 Fed. Register 41404 (July 29, 1998)

9. "The Year 2000 Headache 'Two Thousand Zero-Zero. Party's Over. Oops, Out of Time'", by Gary E. Clayton, John W. Lanius and Greg Noschese, 28 Texas Tech Law Review 753 (1997). This article examines the practical and legal ramifications of the Year 2000 problem, providing a framework for determining whether one has such a problem, how the computer industry is attempting to correct the problem and addressing the legal issues related to the determination of who will pay the costs required to correct the problem. It also discusses potential liability arising out of Y2K issues and possible defenses to such liability.

**Y2K? OK!****Y2K Embedded Systems -  
10 Steps to Y2k Readiness**

One of the big questions facing local government managers is how to handle embedded micro-processors. There are many resources available on the web to help you (see the Y2K Link List in this issue). We've gone through them and tried to boil them down to the essentials. A key conclusion from all this is that while there are many embedded chips out there, few are date sensitive, and fewer are high risk for failure; but you have to check! With that in mind, this information should help you meet the risk that Y2K poses to embedded systems.

**What are Embedded Systems?**

Embedded microprocessors and other time sensitive logic are silicon integrated circuits, generally with permanently coded instructions that are not designed to be easily changed. These monitor, regulate or control the operation of devices, systems, networks or plants. These are generally in the form of micro-processors, timers, sequencers and controllers built-in to machinery from small devices such as wrist watches and consumer electronics, to dedicated processors controlling large industrial plants. Some examples include alarm systems, ATMs, automobile power train control modules, business machines (for example, postage and fax machines), computer motherboards (BIOS chips, Real



Time Clocks on PC's), elevators, HVAC System controls, telecommunications, and valves in plumbing.

**STEP 1 How to Identify Embedded Chips**

To identify potential embedded chip problems, answer these six questions for stand-alone (non-computer) electronic devices:

**Does it operate with electricity?** If no, the device is low risk. If yes, look further. Examples of low-risk items: tables, chairs, wind-up clocks, etc.

*Devices:* lamps, hair dryers, electric pencil sharpeners, analog clocks, etc.

**Does it have a display?** If no, it's low risk. If yes, look further.

*Low-risk devices:* paper shredders, power supplies, refrigerators, older microwaves, etc.

**Does it have a microprocessor?** If no, it's low risk. If yes, look further.

*Low-risk devices:* television sets, stereo equipment, computer monitors, etc.

**Does it have a calendar?** If no, it's low risk. If yes, look further.

*Low-risk devices:* microwave ovens, coffeepots, printers, most copier machines, etc.

**Does the device use the calendar to schedule events?** If no, it's low risk.

*Examples:* digital clocks or calendars that don't schedule anything, cameras, watches, etc. These are low risk because operation of the device is not dependent upon an accurate calendar. The device doesn't care what date is shown; it simply shows a date.

*Examples of high-risk devices:* phone systems, fax machines, irrigation systems, energy management systems that control lights, heat, etc., based on time and date.

**STEP 2 Determining if the Chip has a Problem**

The following guidelines will help you identify devices with embedded systems that may cause year 2000 problems. If you answer "yes" to any of these questions for a specific device, it should be researched for Y2K compliance and potential testing.

**Does the system display or print a date or time?** This would indicate some type of date function is integral to the operation of the device.

**Does the system produce regular reports?** If reports are generated by the device, and dates are part of the report, there may be a problem.

**Does the system store historical records?** If dates are stored, they may also be manipulated and sorted.

**Does the system time-stamp data?** If a system date-stamps records, logos, or products, it will likely be dependent on utilizing a date that may not be able to handle the year 2000.

**Does the system implement a timed sequence?** If the system starts or stops a function based on date or time, it may have a problem.

**Does the system perform an operation on a time or date basis?** Systems that perform a function based on date or time, such as locking doors on weekends, depend on the correct date.

**Does the system perform a calculation based on the differences between time or date?** Systems that determine intervals, averages, or total times could be at risk for year 2000 problems.

**Does the system request the date/time on start-up?** When power is turned on, a system dependent on date may request it as input.

**Y2K? OK!****Y2K Embedded Systems-10 Steps to Y2k Readiness**

**Does the system send date or time information to other systems?** If a system receives date information from other systems, it may have a date problem. Systems that must synchronize themselves with other systems will typically be dependent on knowing the exact date and time.

**Does the system receive date information from other systems?** If it doesn't have a date problem, it may be dependent on another system that does.

**Does the system have a command that allows the date to be set?** If the device or system allows a date to be input, there is likely a need for a correct date.

**Does the system know which day of the week is based on a particular date?** For example, if the system can tell that June 1, 1998 is a Monday, then some kind of calendaring function exists, and consequently a year 2000 problem is likely.

**Does the system generate an alert based on some type of interval?** If a system creates some kind of notification based on an elapsed period, an elapsed time counter may be involved, which has no date problem, but a real time clock may also be involved, which does. It is difficult to know which is being used, so these systems are suspect.

**Does the system display or print data based on a time sequence?** Logs or listings of events by date or time indicate a dependency upon knowing the correct date.

**STEP 3: Preliminary Risk Analysis**

Now that you've identified potential chip problems, identify those that are critical embedded systems: those that contribute to core missions, programs or support services. Categorize them such that the loss or degradation of these systems in the following areas:

**Health and Safety** - could jeopardize the health and safety of employees or the public

**Environmental Impact** - could negatively impact the environment

**Operational Impact** - could negatively impact the ability to perform its missions

**Public Confidence** - could cause the public to lose confidence

**Other** - could have other serious ramifications

Within each category, designate the risk as high, medium or low.

**STEP 4 Site Survey**

Next step, document essential information about the critical ones. Focus on those that:

- respond differently on the weekends, such as sprinklers, traffic lights or security systems
- shut down unless a maintenance schedule is adhered to
- produce regular (hourly, daily, weekly reports)
- rely on external Global Positioning Satellite (GPS) data
- use or produce time-stamped data
- maintain historical state-of-system data

You will need to gather information on these systems with the department name, facility name and address, the manufacturer/vendor name, model or serial number, and point of contact for the system involved.

**STEP 5 Assessment: Vendor Management**

In some cases, the Year 2000 status of the equipment is available from vendor websites on the Internet. Especially for non-critical systems, checking the status of equipment there may be sufficient. There are a number of sites that list status of equipment or have links to vendors systems. Check the list of links in this issue for details.

Based on the information on the site, you may want to document your work by printing out the information, or sending an e-mail to the vendor for detailed information. As always, document your work!

**STEP 6 Assessment: Testing**

Compliance testing is the testing of systems to determine whether it is Year 2000 compliant, non-compliant or unknown. It is performed (1) due to lack of vendor response; (2) to verify system compliance regardless of vendor response; or (3) to test system compliance for custom-developed systems for

which there is no single vendor, i.e. systems built in-house. The object of the test is to observe system performance after the Year 2000, using simulated dates.

**STEP 7 Remediation: Further Risk Evaluation**

Given the information that has been gathered during the survey and assessment phases, re-evaluate the risk categories of the various systems and the risk ranking (high, medium or low). Identify possible scenarios resulting from failure of the system and estimate costs and recovery time, along with the likelihood of these scenarios. Prioritize the systems for remediation.

**STEP 9 Remediation**

For those that fail testing or validation, remediation solutions will fall into the following categories:

**Do Nothing:** the system is Year 2000 compliant, is no longer used, is deemed non-essential, or is such that it cannot be upgraded or replaced.

**Upgrade:** A Year 2000 compliant version, release or retrofit for the system is available.

**Replace:** A Year 2000 compliant version or release is either not available or is undesirable due to cost, additional requirements or schedule, but a functionally equivalent Year 2000 compliant system is available from a vendor.

**Workaround:** A solution that provides a temporary or permanent Year 2000 solution such as manual date rollover action(s) or utilizing other means to achieve functionality until system can be fixed.

**Undetermined:** responsible vendor could not be determined and/or additional further review is necessary.

**STEP 10 Contingency Planning**

Finally, plans should be made in the event that remediation of the high risk systems does not work as intended, that the work cannot be done in time, or that outside failures (e.g. power, telecommunications, etc.) cause the systems to fail.



# Y2K? OK!

## Link List

### General Y2K References:

This page shown with live links:  
<http://www.state.nj.us/dca/lgspages/y2kpg1.htm>  
**Mining Company:** <http://home.miningco.com/computer/> then search for "y2k"  
**Ziff-Davis:** <http://www.zdnet.com/zy2k/index.html>  
[http://www.zdnet.com/anchordesk/bcenter/bcenter\\_287.html](http://www.zdnet.com/anchordesk/bcenter/bcenter_287.html)  
**Netscape site:** <http://home.netscape.com/y2k/>  
**Mitre:** <http://www.mitre.org/research/y2k/>  
**Descriptions of Y2K sites:** <http://www.y2ktimebomb.com/Special/Reviews/index.htm>  
**CNET:** <http://www.cnet.com> and click on the Y2K item at the bottom of the page.  
**MSNBC -** extensive web links: <http://www.msnbc.com/news/227213.asp#BODY>

### Best Practices:

**Overall Y2K:** <http://www.itpolicy.gsa.gov/mks/yr2000/best/yr1bpfed.htm>  
**Health Care Equipment: Home Page:** <http://www.rx2000.org> (PERMA to join)  
**Search biomedical sites:** <http://hilary.hypermart.net/healthcare/biomedical.html>  
**Biomedical Database:** <http://www.y2k.gov.au/biomed/index.html>  
**FDA Biomedical database:** <http://www.fda.gov/cdrh/yr2000/y2kintro.html>  
**Medical and lab equipment:** <http://www.willitwork.com/>

### Product Inventory Sites:

**General/Comprehensive Links:**  
<http://www.support2000.com/mpos.htm>  
<http://www.vendor2000.com>  
<http://y2k.policyworks.gov/>  
<http://www.isa.gov/ais/2000/emp/emp/emp1.htm>  
<http://hilary.hypermart.net/index.html>  
<http://www.willitwork.com/>  
**Computer hardware and software:** <http://www.nycenet.edu> (click on Y2K link )  
**Computers:** <http://www.compinfo.co.uk/y2k/manufpos.htm>  
**Hardware and software:** <http://hilary.hypermart.net/computer-software.html>  
**Index of vendors:** <http://www.state.ak.us/y2000/index.htm>  
**Building Systems:** <http://www.boma.org/year2000/vendors.htm>  
**Building facilities:** <http://y2k.lmi.org/gsa/y2kproducts/default2.htm>  
**Embedded systems in facilities:** <http://www.lanl.gov/projects/ai/year2000/embed/>  
**General software:** [http://www.mitre.org/research/cots/COMPLIANCE\\_CAT.html](http://www.mitre.org/research/cots/COMPLIANCE_CAT.html)  
**Petroleum equipment:** <http://www.peinet.org/forms/Y2K/categories.htm>  
**Natural gas companies:** <http://www.aga.org/naturalgas/y2k/utilityy2k.html>  
**Embedded Systems Checking:**  
<http://www.auto2000.nrdirect.co.uk/y2kindex.htm>  
<http://www.iee.org.uk/2000risk>  
[http://www.year2000.ca.gov/Correspondence\\_Embedded.pdf](http://www.year2000.ca.gov/Correspondence_Embedded.pdf)  
<http://www.state.co.us/Y2K/embedded/briefing.pdf>  
<http://www.state.ak.us/y2000/testing/embedtest.htm>  
<http://www.tnn.com/~frautsch/y2k2.html>

### Evaluations of Y2K Testing Programs:

**Article:** <http://www.gcn.com/gcn/1999/January11/1d.htm>  
**Table of results:** <http://www.gcn.com/gcn/1999/January11/y2kchart.htm>  
**Sm@rt Reseller looks at four Y2K inventory tools that check PC networks:** <http://chkpt.zdnet.com/chkpt/y2ke9801275/www.zdnet.com/stories/issue/04537.384250.00.html>  
**CNET, the computer system web site reviewed five Y2K testing programs:** <http://home.cnet.com/category/topic/0,10000,0-4020-7-271710,00.html>  
**Emergency Communications Equipment:**  
**CML Technologies:** <http://www.cmltech.com>  
**Data 9-1-1:** <http://www.data911.com/>  
**E.F. Johnson:** <http://www.efjohnson.com/>  
**Intergraph:** <http://www.intergraph.com/pubsafety>  
**Kenwood:** <http://www.kenwood.net/>  
**Motorola:** <http://www.motorola.year2000.lmpx.motorola.com/yr2000/home.asp>  
**Orbacom:** <http://www.orbacom.com>  
**PEI (Plant Equipment Inc.):** <http://www.peinc.com>  
**PRC Public Sector:** <http://psweb.prc.com/>  
**SCC Communications:** <http://www.scc911.com/HTML/products.html>  
**Standard Communications:** <http://www.standardcomm.com>  
**Uniden:** <http://www.uniden.com/>  
**Vertex (Yaesu):** <http://www.yaesu.com/product.html>

### Computer Products:

**Novell**  
**General Information:** <http://www.novell.com/year2000/>  
**Product Status:** <http://www.novell.com/year2000/product.html>  
**Testing Product:** <http://www.novell.com/year2000/tools.html>  
**Hewlett Packard**  
**General Information:** <http://www.hp.com/year2000/>  
**Product Status:** <http://www.hp.com/year2000/allproducts.html>  
**Technical Information:** <http://www.hp.com/year2000/help/addinfo.html>  
**Microsoft**  
**General Information:** <http://www.microsoft.com/technet/topics/year2k/>  
**Product Status:** <http://www.microsoft.com/technet/topics/year2k/product/product.htm>  
**Testing Tools:** <http://www.microsoft.com/technet/year2k/tools/tools.htm>  
**Dell**  
**General Information:** <http://www.dell.com/year2000/>  
**Product Status:** <http://support.dell.com/advisor/>  
**Testing Tools:** <http://www.dell.com/year2000/tools/patch/prgmpatc.htm>  
**IBM**  
**General Information:** <http://www.ibm.com/IBM/year2000/>  
**Product Status:** <http://www.ibm.com/IBM/year2000/content/productoffer.html>  
**Testing Tools:** <http://www.ibm.com/IBM/year2000/testing/>

### International Y2K Efforts

**U.S. Government links to International Y2K programs:**  
<http://www.itpolicy.gsa.gov/mks/yr2000/g7yr2000.htm>

**Y2K? OK!****For Water and Wastewater Utility Operators**

Are you a utility operator? There are a number of resources and sites on the Web that are dedicated to dealing with Y2K and drinking water and wastewater systems.

The **Municipal Excess Liability Fund** commissioned a professional study of a typical wastewater treatment system to identify the Y2K exposures. That document is an excellent resource for utility operators to see where their risks lie. The document is available on the DLGS Y2K web site at <http://www.state.nj.us/dca/lgs/pages/y2kpg1.htm>, and can be downloaded as a Microsoft Word document or as an Adobe Acrobat portable document.

**New Jersey DEP** has recently released a report on wastewater treatment plants. It can be found at <http://www.state.nj.us/dep/dwg> and has been mailed to all NJPDES wastewater permit holders.

The **U.S. Environmental Protection Administration's** web site contains a good deal of general and enforcement policy information. Every operator should review the enforcement policy page.

**Y2K and Utility Operations:** <http://www.epa.gov/year2000/y2k2.html>

**Drinking and Waste Water:** <http://www.epa.gov/year2000/ow.htm>

**Solid Waste:** <http://www.epa.gov/year2000/oswrpage.html>

**Y2K Enforcement Policy:** <http://es.epa.gov/oece/eptdd/ocy2k.html>

The **Association of Metropolitan Water Agencies** has an excellent site called the Millennium Bug Page (<http://www.amwa-water.org/y2k/>). The site describes the contents as follows:

■ **Model Y2K Action plan for utilities:** Are you ready for the year 2000? Many AMWA members started some years ago to prepare their utilities for possible problems with date sensitive computer chips as the new millennium starts. This site attempts to capture some of the experience those members have gained and share it with others by using a Model Y2K Action Plan.

■ **Internet Links to Y2K Resource Sites:** There are a variety of resources

on the Internet which are useful in developing and carrying out Y2K assessments. A selection of those resources are listed here. Please feel free to suggest other sites that might be useful to drinking water utilities to the national office.

■ **AMWA Y2K Discussion Forum:** This site contains a Y2K discussion forum where you can ask questions or share information about specific Y2K issues.

The **American Water Works Association** site at <http://www.awwa.org/y2k.htm> includes the results of surveys of water system operators on Y2K readiness. While the industry consensus seems to be that water systems are not a high risk system, each system operator must act to limit any exposures they find.

For wastewater system operators, the **Water Environment Federation's** web site, <http://www.wef.org/docs/search.html>, has an extensive list of links to suppliers. While there are few computer exposures in the wastewater industry, this site should be able to find out the status of the equipment that is microprocessor driven.



**Y2K? OK!****From the Association of Environmental Authorities:  
Countdown Under Way for Ridding the Y2K Bug**

The countdown to 2000 is starting to resemble a space shuttle launch. One by one we are checking down the list, waiting to hear a reassuring word that the things we depend on - electrical power, fire and police, banks, communications - are **Y2K? OK!**

Water and sewer authorities are counting down, too, and working hard to ensure that all phases of operations continue without a glitch after the clock strikes 12 this coming New Year's.

As the only statewide professional association representing authorities in New Jersey, AEA is informing its members about what they need to know and do to achieve Y2K readiness. At our Annual Meeting last November AEA conducted a panel discussion where speakers from state government, banking, utilities and the computer industry discussed how to avoid Y2K problems. This message will be repeated at our Spring Meeting and with subsequent workshops and mailings throughout the year.

One of our members participated in a recent study by the New Jersey Utilities Authority Joint Insurance Fund that demonstrated what authorities must do to ensure Y2K readiness. The study provides a road map for authority executive directors who want to know once and for all what they must do to meet their public responsibilities.

The state utilities JIF hired CARA Corporation\* of Oak Brook, Ill. to study the Y2K readiness of an AEA member Municipal Utilities Authorities as a pilot project. This suburban South Jersey authority provides sewer and water service to about 14,000 customers. It's not the largest system in New Jersey by far, but large or



small, those who provide vital public utility services confront the same serious questions about whether and how operations will be unaffected by Y2K-related computer problems.

The first step in the process was to assume the worst - that there were Y2K readiness problems that would shut down operations unless they were fixed. The next step was to set two major goals: Assess the MUA's Y2K preparedness and whether its existing readiness plans were adequate; and determine the magnitude of its readiness problem and provide recommendations on managing the Authority's Y2K risk.

The project took a hard look at embedded systems, which are essential to a broad range of modern tools and control systems - and they are everywhere. The consultant and staff toured eight MUA sites - wells, sewage treatment plants and offices - to make an inventory of embedded systems. It turns out that MUA will have to spend a lot of money to make these systems Y2K compliant. The authority will also have to upgrade half of its office personal computers and much of its software.

But the good news at the end of this exhaustive study is that the MUA had no major Y2K problems that could not be fixed in time.

There were two important take-aways for water and sewer authorities. First, since microchips are embedded everywhere, you have to look

at practically everything to make sure a date-sensitive component isn't lurking that can cause problems. There are microprocessors in temperature sensors, smoke and gas detectors, circuit breakers and valve actuators. Some have a timing functions, some don't. Many of these devices have subassemblies that may or may not have a Y2K problem that could potentially derail monitoring, diagnostic or control systems.

The other important lesson is that the potential for Y2K mayhem never seems to end. In a real sense, it doesn't. You have to test your systems, upgrade, test some more and then create a contingency plan just in case Murphy's Law is Y2K compliant.

The final report recommended contingency planning based on the assumption that power will be unavailable for a period of days and may have problems for two to three months afterward. The backup system would include the diesel generators already onsite and enough fuel to provide power to vital water and sewer systems for the entire first quarter of 2000.

The report is exhaustively detailed and is available on the Division of Local Government Services website: <http://www.state.nj.us/dca/lgs/pages/yk2pg1.htm>.

AEA will also make this report available as part of our continuing effort to inform our members about what they need to know and do to become Y2K compliant. As we count down to 2000, we want the public to know that water and sewer is one of the vital services so important to our daily lives that will be there after we all ring in the new century.

\* CARA Corporation has since been renamed ACS Technology Solutions, a division of Affiliated Computer Services, Inc.

**Y2K? OK!**

### Few Building Systems Are Affected by the Y2K Problem

*From the President's Council on Year 2000 Conversion*

John A. Koskinen, Chair of the President's Council on Year 2000 Conversion, recently welcomed the findings of a new survey that shows most organizations identify less than 5 percent of building systems as being affected by the Year 2000 (Y2K) computer problem, but cautioned that building owners and operators must assess the readiness of all systems and take the necessary steps to ensure that they are able to make a successful transition to the Year 2000.

"It is encouraging to see that relatively few building systems are affected by the Y2K problem, and that mirrors what we have found in Federal buildings," said Koskinen. "But it does not lessen the urgency of making sure that all building systems are able to make a successful transition to the Year 2000. Building systems are involved in critical functions from security to environmental control, and it is in the interest of every organization to see to it that these and other activities are not disrupted by the date change."

Koskinen was joined at the all-day "National Summit on Y2K Building Systems," by David Barram, Administrator of the General Services Administration (GSA), Robert Peck, Commissioner of Public Buildings for GSA, and Bill Garland, President of the Building Owners and Managers Association (BOMA) International. Results of the survey, which BOMA and GSA conducted with the assistance of Buildings magazine, were released at the summit's opening session.

## Y2K News from the Federal Government...

### Y2K Fire Service Rumors are False from the U.S. Fire Administration

The U.S. Fire Administration (USFA), part of the Federal Emergency Management Agency (FEMA) recently announced two recent rumors about fire service equipment failing in the Year 2000 computer conversion are false. The rumors concern emergency vehicle ignition systems and aerial ladders.

"We should all be concerned about automated and intelligent systems not designed to account for the date change of the year 2000, said US Fire Administrator Carrye B. Brown. "But there is a great deal of misinformation on this topic being circulated."

The General Services Administration recently investigated and disproved a report that originated with an emergency services unit at a federal facility in New Mexico that mistakenly claimed that emergency vehicle ignition systems would not work on January 1, 2000. In the second case, an official from the Baton Rouge Fire Department was misquoted, leading to a report of Y2K problems with aerial ladders that is incorrect.

The USFA follows these stories with the purpose of confirming and sharing the facts. Its Web site at [www.usfa.fema.gov](http://www.usfa.fema.gov) is a prime source for current Y2K information for the fire and emergency services community.

Working with the National Association of State Fire Marshals and the National Emergency Number Association (NENA), the USFA continues its Y2K assessment of fire service operations and public safety communication networks. The State Fire Marshals are assessing a representative sample of fire departments in all States and NENA is soliciting input from Public Safety Answering Points. A comment section on the USFA Web site allows for direct input by individual fire and emergency services units and can be accessed at <http://www.usfa.fema.gov/y2k/y2kform.htm>.

"We must work together and share correct information so that the fire service is ready for the Year 2000," Brown said.

"GSA and BOMA have worked together in a productive partnership to assess the impact of the Y2K problem on building systems, and I congratulate them for their good work," said Koskinen. "The Council looks forward to receiving data from additional follow-up surveys in this area and tracking the progress of building owners and operators as we move through the remainder of the year."

The President's Council on Year 2000 Conversion, established on February 4, 1998 by Executive Order 13073, is responsible for coordinating the Federal Government's efforts to address the Year 2000 problem. The Council's more than 30 member agencies are working to promote action on the problem and to offer support to public and private sector organizations within their policy areas. Visit the Council via the Internet at [www.y2k.gov](http://www.y2k.gov). For consumer information on the Year 2000 problem, call the Council's free information line at 1-888-USA-4Y2K (1-888-872-4925).

**Y2K? OK!****Y2K Humor? AY2K Perspective**

So we don't lose our sense of perspective on Y2K, the following is alleged to be an article from a London Newspaper (circa 999 A.D.)

Canterbury, England. A.D. 999.

**A**n atmosphere close to panic prevails today throughout Europe as the millennial year 1000 approaches, bringing with it the so-called "Y1K Bug," a menace which, until recently, hardly anyone had ever heard of. Prophets of doom are warning that the entire fabric of Western Civilization, based as it now is upon monastic computations, could collapse, and that there is simply not enough time left to fix the problem.

Just how did this disaster-in-the-making ever arise? Why did no one anticipate that a change from a three-digit to a four-digit year would throw into total disarray all liturgical chants and all metrical verse in which any date is mentioned? Every formulaic hymn, prayer, ceremony and incantation dealing with dated events will have to be re-written to accommodate three extra syllables. All tabular chronologies with three-space year columns, maintained for generations by scribes using carefully hand-ruled lines on vellum sheets, will now have to be converted to four-space columns, at enormous cost. In the meantime, the validity of every official event, from baptisms to burials, from confirmations to coronations, may be called into question.

"We should have seen it coming," says Brother Cedric of St. Michael Abbey, here in Canterbury. "What worries me most is that THOUSAND contains the word THOU, which occurs in nearly all our prayers, and of course always refers to God. Using it now in the name of the year will seem almost blasphemous, and is bound to cause terrible confusion. Of course, we could always use Latin, but that might be even worse — The Latin word for Thousand is Mille which is the same as the Latin for mile. We won't know whether we are talking about time or distance!"

Stonemasons are already reported threatening to demand a proportional pay increase for having to carve an extra numeral in all dates on tombstones, cornerstones and monuments. Together with its inevitable ripple effects, this alone could plunge the hitherto stable medieval economy into chaos.

A conference of clerics has been called at Winchester to discuss the entire issue, but doomsayers are convinced that the matter is now one of personal survival. Many families, in expectation of the worst, are stocking up on holy water and indulgences.

**Memo Found  
on the Internet**

Hi Boss,

I hope I haven't misunderstood your instructions. Because to be honest, none of this Y to K problem makes any sense to me.

At any rate I have finished converting all the months on all the company calendars so that the year 2000 is ready to go with the following new months: Januark, Februark, Mak, Julk.

In addition, I have changed the address of our corporate offices on all our envelopes so that everything will be sent to New Kork. (It's sure gonna sound funny talking about the world champion New Kork Kankees). :)

Well, that's all for now. Gotta go.

- Bob

PS Some empokees are upset, especiallk Jerrk, Terrk, Ginnk, Timothk and Cknthia.

**Y2K? OK!**

Published by the  
**State of New Jersey**  
Christine Todd Whitman, *Governor*

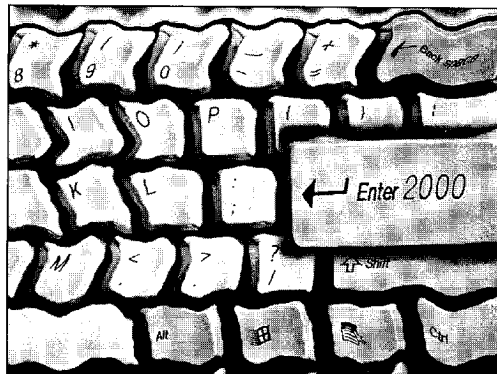
**Department of Community Affairs**  
Jane M. Kenny, *Commissioner*

**Division of Local Government Services**  
Al Steinberg, *Director*  
Marc H. Pfeiffer, *Editor*

Guy A. Lebo, *Graphic Designer*

Prepared with the cooperation and  
assistance of:  
Wendy W. Rayner  
*Chief Information Officer*  
and  
Jack Longworth  
*State Y2K Coordinator*  
*Office of the Governor*

**Y2K? OK!** is also on the web at  
<http://www.state.nj.us/dca/lgs/pages/y2k/y2kok2.pdf>



**Advice For New Jersey Local Government Officials:  
Reproduction of this Booklet Encouraged**

**Y2K? OK!**  
New Jersey Department of Community Affairs  
Division of Local Government Services  
101 South Broad Street  
PO Box 803  
Trenton, NJ 08625-0803

First Class Mail  
US Postage  
PAID  
Trenton, NJ  
Permit No. 21

JUN 15 '99 14:33 FR NJ DEP

1 609 292 7900 TO 98833862

P.02/03



**State of New Jersey**

Department of Environmental Protection

Christine Todd Whitman  
Governor

Robert C. Shinn, Jr.  
Commissioner

May 26, 1999

Rick Engler, Director  
N.J. Work Environment Council  
198 West State St. - 3<sup>rd</sup> floor  
Trenton, N.J. 08609-1103

Dear Mr. Engler:

I am writing in response to the New Jersey Work Environment Council's (WEC) letter of May 7, 1999 as addressed to Governor Christine Todd Whitman. The letter outlines the public health risk posed by potential chemical releases resulting from inability of date-sensitive equipment to properly process dates into the Year 2000. It goes on to recommend the detailed steps that DEP should take to determine the level of readiness and report same to the public.

In reply, I must stress that DEP has partnered with EPA, State Police and local emergency response community to raise the level of awareness of the Y2K problem in the regulated community through ongoing coordination and cooperation with various trade associations. Specifically, DEP and EPA made presentations at the New Jersey Water Environment Association Technology-Transfer Seminar on March 4, 1999. Don Flattery, National Lead Y2K Sector Outreach, presented the national Y2K perspective. Kathleen Malone, Y2K Coordinator, EPA Region II, presented the EPA enforcement policy. The EPA letter explaining this policy contained a paragraph addressing special New Jersey Compliance and Enforcement requirements. The policy encourages prompt testing of computer-related equipment to ensure that environmental compliance is not impaired in the Year 2000. As an incentive to do this, the policy provides relief from testing-related violations if certain conditions are met. The policy letter has been distributed to over 4000 facilities (all media) in New Jersey. Similar presentations were made at the Air and Waste Management Association seminar on March 16, 1999. This particular audience included Toxic Catastrophe Prevention Act (TCPA) community representation.

In cooperation with the Chemical Manufacturers Association and the Chemical Safety and Hazard Investigation Board, EPA organized a trade group meeting of smaller chemical companies with a membership of approximately 7,000 to 10,000 chemical manufacturers, formulators, retailers and distributors. This group has undertaken an additional survey to determine the extent of the Y2K problem among smaller companies and the remaining effort required to make them Y2K compliant. Remediation and contingency guidance documents will be developed by EPA for these targeted small/medium sized, vulnerable companies. DEP will insure that these documents are made available to all such New Jersey facilities and, in conjunction with our aforementioned partners, use them to continue to increase awareness and develop viable contingency plans.

ENCLOSURE 3

New Jersey is an Equal Opportunity Employer  
Recycled Paper

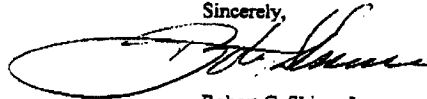
With respect to the TCPA regulated community, DEP will get a sense of readiness status from the submission of the mandated Risk Management Plans (RMP), which are due not later than June 21, 1999. As James Makris, EPA's Director of Chemical Emergency Preparedness and Prevention Office, testified at the May 10, 1999 Hearing, EPA has placed a notification on their website that the RMP's must include how facilities will ... "prevent or minimize accidents." The Risk Management Plan (RMP) must also address, among other items, the worst-case release scenario(s) and the alternative release scenario(s), including administrative controls and mitigation measures to limit the distances for each reported scenario. To that end, EPA has encouraged chemical facilities to include potential Y2K releases as one of the alternative scenarios. Again, we share the EPA objective of linking sound Y2K planning to the Risk Management Program as the standard approach of utilizing existing regulatory and voluntary programs to address Y2K readiness.

Given our individual and collective efforts to date, it is clear that the Department has, in fact, taken an aggressive role in conveying the importance of dealing with Y2K to the regulated community, including those TCPA facilities, which were of specific concern in your letter. The Department will continue to monitor all of the various survey results in order to obtain an ongoing assessment of where the regulated community stands in terms of the Y2K readiness.

In addition, all New Jersey facilities are well aware of our Compliance and Enforcement position and with respect to the TCPA facilities, the upcoming receipt of the Risk Management Plans (RMP's) will provide additional insight into Y2K readiness. While we cannot assume the operating responsibility for all of New Jersey's facilities, a point which we have made clear, we will continue the efforts outlined in this response. In addition, we are preparing an information packet to transmit to facilities in New Jersey, which again will continue to address the awareness issues that are essential to the Y2K readiness. Specifically, as future facility inspections are done by our Compliance and Enforcement staff or permits are issued through Environmental Regulation, we will see that these awareness packets are transmitted to the respective facilities. In addition, we will reach out to our CEHA partners and seek a similar distribution to facilities that they deal with on a day-to-day basis.

Again, I want to emphasize the fact that operators of regulated facilities have an affirmative responsibility to meet their legal obligations to prevent releases of hazardous substances into the environment. We feel confident that the Y2K phenomenon is well-known and we are actively working to insure that relevant resource information to effectively address Y2K issues is made available. I feel confident that these efforts are necessary and sufficient to achieve our common objective.

Sincerely,



Robert C. Shinn, Jr.  
Commissioner

c: Governor Christine Todd Whitman  
Jane Nogaki, Board Co-Chair, NJWEC

RESPONSES OF FRANCIS J. FRODYMA TO QUESTIONS SUBMITTED BY  
CHAIRMAN BENNETT

*Question 1.* You mentioned in your statement that the Standard on Process Safety Management of Highly Hazardous Chemicals (PSM) does not cover many facilities considered to be at risk due to Y2K. Can you elaborate on this, and explain what has been done to reach those facilities not covered by PSM?



Answer. OSHA's PSM standard only applies to establishments that have more than a threshold quantity of certain highly hazardous substances on site. This list of highly hazardous substances, which was promulgated separately through a notice-and-comment rulemaking, is limited to approximately 135 hazardous substances and does not include all flammable, toxic and reactive substances that could potentially create a Y2K-related safety hazard. Therefore, many facilities that one might assume are covered by PSM, such as chemical plants processing substances not covered by PSM, or gas stations, are not covered. A facility's coverage status can vary as hazardous substances are moved on to or off of the worksite. OSHA is aware that there are many facilities that store large quantities of flammable and reactive substances and are at potential risk from Y2K-related problems, but there is no requirement for such facilities to identify themselves to OSHA. There is no "master list" of PSM-covered facilities for OSHA to target. Therefore OSHA has initiated a general outreach program to all industries, including the development of a concise Y2K fact sheet to alert employers to the potential for Y2K-related problems at their worksites. This fact sheet has been posted on OSHA's Internet web site, is handed out to employers during OSHA inspections and consultation visits, and was recently sent out to 12,500 employers in a mass mailing.

*Question 2.* It is clear from your statement that OSHA believes that PSM inspections are not an effective tool to be utilized in assuring Y2K compliance due to resource limitations and the existing focus of the PSM program. What has OSHA done, as an alternative to using PSM inspections, to assure that Y2K safety related hazards have been properly addressed?

Answer. There is no way for OSHA to "assure" that Y2K-related safety hazards have been properly addressed by every employer in every industry. Even if OSHA devoted all of its resources entirely to the Y2K issue, and had airtight legal authority to cite employers for failure to properly address Y2K-related safety hazards, the agency could not inspect all of the workplaces that are at risk. Therefore, OSHA has chosen to address Y2K through outreach and education, by disseminating information to as many employers as possible.

*Question 3.* You mention in your statement that OSHA concentrates its efforts on those industries having the worst safety records and higher-than-average injury and illness rates, and that the chemical industry actually has one of the best records in this regard. However, experts in the chemical industry, including the Chemical Safety Board, recognize the great vulnerability of the chemical industry to Y2K related safety problems. Do you mean to state through your remarks that OSHA has intentionally ignored an area in which there is great potential for health and safety risks, simply because statistics on past incidents don't support it? Shouldn't OSHA be as concerned about the potential risk areas, as they are with demonstrated risks?

Answer. OSHA has not ignored the potential for Y2K-related safety problems in the chemical industry. On the contrary, we have developed a Y2K fact sheet, publicized its availability, posted it on our Internet web site, instructed our inspectors to hand it out at each inspection, asked the Consultation Programs to distribute it during their visits, and included it in a mass mailing to 12,500 businesses. We worked with the Environmental Protection Agency on the development of their Y2K fact sheet, and have included a link to EPA's fact sheet on our web site. We also participated in the Y2K workshop organized by the Chemical Safety Board in December, 1998.

As for concern about potential risks versus demonstrated risks, OSHA believes we have found an appropriate balance between the two. In the case of Y2K, we have chosen to address this potential risk through outreach and education.

*Question 4.* Would you explain in more detail what a "Special Emphasis Program" is and why that would not help greatly raising awareness on Y2K? It sounds like that is just the sort of program OSHA needs. Just the creation of a program and the associated publicity would generate a lot of positive activity in the short time remaining.

Answer. Special Emphasis Programs (SEPs) give OSHA a mechanism to conduct programmed compliance inspections in high potential injury or illness rate situations which are not covered by normal inspection scheduling systems. SEPs can be targeted based on a number of different factors, including specific industry, substance or other hazard, type of workplace operation, type or kind of equipment, etc.

As I stated in my written testimony, OSHA does not have a standard, other than the Process Safety Management Standard (PSM), under which employers could be cited for failure to assess their Y2K readiness and address any areas of vulnerability that are discovered. Only about 25,000 establishments, out of the more than 6 million workplaces in the nation, are covered by the PSM standard. Assuming that OSHA enforcement could compel Y2K safety, it must be noted that stringent legal tests must be satisfied for OSHA to successfully cite an employer under the General

Duty Clause. Therefore, the General Duty Clause is not an appropriate foundation for a Special Emphasis Program. Further, SEPs in the chemical industries have proven to be resource-intensive, and an SEP on Y2K would divert resources from other, equally important agency functions.

*Question 5.* You cite several problems which seem to have handicapped OSHA in its ability to play a more direct role in mitigating potential Y2K related hazards in the chemical industry, such as the applicability of the General Duty Clause. What has OSHA done to overcome these impediments? Both Congress and the White House have been asking the agencies for quite some time now about what additional legislation or authority they needed in regard to Y2K. Why weren't these issues raised earlier?

Answer. Even if the legal impediments to OSHA citation were removed, OSHA does not believe that a massive program of inspection and citation is the appropriate method for dealing with Y2K. There is no "one-size-fits-all" solution when it comes to Y2K, as each workplace is different. We believe that education and outreach is the better approach. It is in employers' own self-interest to find and fix Y2K-related safety hazards. We think that if employers are made aware of and given information about the Y2K problem, they will take the initiative to address it.

---

PREPARED STATEMENT OF PAULA R. LITTLES

Good morning, Mr. Chairman, Members of the Committee, my name is Paula Littles. I am the Citizenship-Legislative Director for the Paper, Allied-Industrial, Chemical and Energy Workers International Union, AFL-CIO (PACE). Our union represents 320,000 workers employed nationwide in the paper, allied-industrial, chemical, oil refining, and nuclear industries. It is my pleasure to appear before this Committee today to address the issue of Y2K and the chemical sector. According to the U.S. Environmental Protection Agency (EPA), 85 million Americans live, work, and play within a five-mile radius of 66,000 facilities handling regulated amounts of highly hazardous chemicals. Workers at these facilities are responsible for critical plant operations. They implement the contingency measures used during emergencies, from inclement weather to system failures to fires and/or explosions.

The Chemical Safety Board (CSB) Report released in March 1999 explained that "The Year 2000 technology problem is significant in the chemical manufacturing and handling sector, posing unique risks in business continuity, and worker and public health and safety." Small and medium-sized businesses are "of major concern" the report states because "efforts on the Y2K problem appear to be less than appropriate."

Y2K problems may be found in computer systems and machinery containing embedded chips. These chips are far too numerous and dispersed throughout our primary industrial sectors to be adequately assessed, remediated and tested before the Y2K rollover. Because of the lack of adequate planning for reaching Y2K compliance, contingency planning and worker training should be initiated immediately to build an emergency response infrastructure to respond to environmental disruptions, chemical releases, and worker and public health and safety.

Chemical workers, emergency responders, and local government agencies that focus on environmental and emergency response should be provided with training and tools to adequately address Y2K issues.

Workers are currently provided training on contingency plans for single device failures, however multiple device failure possibilities are not normally considered in the current process hazard analyses. It is unclear what the outcome might be due to such failures—possibly multiple control system failures, multiple utility failures, or a combination of both.

Contingency planning for Y2K-related emergencies has to be designed and implemented with worker involvement and should also be designed to include safe operations, safe shutdown, and emergency response. Any such planning must also take into account human factors such as appropriate staffing, hours of continuous work/rest intervals, and worker stress levels.

We have discussed this issue with the companies that employ our members at their facilities, and it is believed that the larger companies are taking the Y2K problem seriously and are expending large amounts of resources to correct the problem. A number of these facilities have shared their concern regarding the reliability of their utility suppliers. Petrochemical facilities have a great dependency on purchased utilities for their day-to-day operations. We strongly urge greater communication between the utility providers and the facilities they serve, to ensure that each entity is doing their part in addressing this issue.

We are concerned about the small and mid-sized facilities that we represent. Unfortunately, we do not believe these facilities have the capability to expend the necessary resources to test the design and Y2K contingency measures for all their systems, and provide the necessary training for their employees.

As a labor organization, we have been encouraging the companies that operate the facilities that we represent and are ahead of the curve on their Y2K efforts to provide assistance to those that are not proportionately comparable. In the short period of time remaining before Y2K, we feel this is one viable option to assist these employers that have been unable to adequately address this issue. No matter what size the company, the Y2K issue could threaten worker and public health and safety. We would urge companies to follow the proposed emergency response planning as specified in the Chemical Safety Board Report through Y2K contingency planning on three levels:

- Level 1 should address continued safe operations that include pre-planning of actions that will allow the facility to continue to run in a safe and environmentally sound manner;
- Level 2 should address safe shutdown. This level of planning ensures the availability of personnel, equipment, utilities, services and other resources needed to ensure safe shutdown; and
- Level 3 is activated when Contingency Level 1 fails to ensure continued safe operations and Level 2 fails to ensure safe shutdown. This will likely initiate a process safety incident (See Attachment I).

PACE believes that both employers and government agencies should designate worker representatives and include them in discussions regarding Y2K contingency planning, because ultimately workers will be the ones responsible for implementing these plans.

Thank you for allowing me the opportunity to speak on behalf of PACE today to present our position on this important issue.

---

RESPONSES OF PAULA R. LITTLES TO QUESTIONS SUBMITTED BY  
CHAIRMAN BENNETT

*Question 1.* In your statement, you point out that lack of resources is a problem for small and medium size companies. We hear this often, yet we have never been provided with any hard data. Can you quantify this for us in any way? Also, what do you think could be done to financially aid such companies in the short time remaining?

Answer. In March of 1999 the PACE International Union requested their local union officers to request that their represented companies address the following areas:

- a) Identification of any Y2K problem;
- b) Inventory of what chips are affected and the location of the chips;
- c) Testing to see if the chips work and correcting them if they do not;
- d) Testing of corrected systems and certification that all systems are viable; and
- e) Contingency plans and training to work around problems that the facilities can not correct in a timely manner, or problems at utility sites or other industrial facilities (upstream or downstream).

Based on the responses received, we concluded that there was a greater problem with the small to medium-sized companies that we represent. In the short time remaining, training funds should be provided to assist in the training of workers in these facilities to better equip them to handle Y2K-related incidents.

*Question 2.* You mentioned that PACE is encouraging its better-prepared members to lend assistance to those members who are less prepared. Has a formal program been established in PACE, or any chemical industry association to provide such assistance?

Answer. No, we plan to offer training to our members to better prepare them for what to expect. Unfortunately a formal program would have to be developed, with the collaboration of management or an industry association to really have value to these companies that are less prepared.

*Question 3.* You represent a large number of workers in a number of industries that may be vulnerable to Y2K problems in manufacturing process automation. What is the general level of concern about worker safety among your membership regarding the Y2K issue?

Answer. We currently have three general levels of concern regarding worker safety and Y2K:

- 1) Are the workers and the workplace being accurately prepared for Y2K? For example, if a company decides to staff-up for manual operations/shutdown, would ev-

eryone know what their roles would be? Will everyone have sufficient training in their assigned roles to perform necessary tasks in a timely, safe, and proficient manner?

2) In the event of a Y2K-related action, has a discussion and plan been developed for worker interaction with community responders from surrounding communities and tested for its effectiveness?

3) Have companies and their utility suppliers had sufficient interaction to work together towards limiting the problems that could surface due to Y2K? Overall, the concern among our membership, like the general public varies from extreme concern to those who feel the problem will not be that great.

*Question 4.* You raised many important issues in your discussion of the three levels of contingency planning in your statement. What formal activities has PACE engaged in to spread this information across the industry?

Answer. Unfortunately PACE has limited influence in disseminating information across the industry. In order to facilitate this, there would have to be better collaboration with management. Regrettably all of our represented companies are not willing to work with the union in some areas. What we have done is to provide all of the union's International Representatives with a copy of the Chemical Safety Board Report that gives an in-depth overview of the three levels of contingency planning. Our Representatives were asked to share this information with local union officers and representative companies.

*Question 5.* PACE represents a diverse cross section of the chemical processing industry. Is there any one sector in which your concerns are greater than they are in others?

Answer. No. With the diverse cross section of the chemical processing industry, if a facility manufactures chemicals or just uses chemicals in its process, their work-site could still be subject to Y2K-related failure. Depending on related circumstances, the facility that you would least expect to experience major problems could be the worst case for the type of process they use.

*Question 6.* Are there any issues regarding union membership rights, contract restrictions, or other worker protection issues that might somehow complicate planned Y2K responses and contingency plans in the industry? (Overtime restrictions, holiday pay considerations, and hourly work restrictions).

Answer. The majority of our contracts are not restrictive as it relates to business emergencies. We expect our representative companies to provide a safe work environment, and we would be willing to work with them on their planned Y2K responses and their contingency planning and training. We are concerned about rate retention in the event of a Y2K problem. The employer has a responsibility to keep all workers whole, meaning no loss of pay and benefits. Discussions between represented companies and the union should start sooner rather than later on this subject.

*Question 7.* Would you say more about the worker training and tools you believe are needed? Is there time to develop such tools and training programs?

Answer. The development of training and educational materials for front-line workers in chemical dependent industries, local community residents, and the emergency response community should be developed to specifically focus resources on the unique hazmat response challenges of Y2K-related chemical and hazardous materials, related incidents and scenarios. These scenarios should include:

- an individual worker's or responder's role in a process shutdown;
- how an emergency plan should change if there is no outside response;
- the possibility of creating a dangerously confined space if doors don't automatically open; and
- what to do if there is lack of power or air to re-supply breathing apparatus.

The NIEHS Worker Education and Training Program (WETP) has included Year 2000 conversion and chemical safety awareness and response in all of their planned safety and health activities. We feel that with the time remaining for training, we should utilize training programs that are well established and proven such as the NIEHS's WETP.

---

PREPARED STATEMENT OF JAMES L. MAKRIS

**Mr. Chairman and Members of the Committee:**

I am Jim Makris, Director of the Environmental Protection Agency's Chemical Emergency Preparedness and Prevention Office. I am accompanied today by Oscar Morales, Associate Director of the Information Management Division, Office of Prevention, Pesticides, and Toxic Substances, and Don Flattery, EPA's Year 2000 Sector Outreach Coordinator. It is a pleasure to be here today to discuss the implica-

tions of the Year 2000 (Y2K) technology problem for chemical safety. We appreciate the Committee's efforts in both educating and alerting government, industry, and the public at large to our potential vulnerability to the Y2K problem. We welcome the Committee's invitation to appear here today to discuss the chemical safety aspects of Y2K which we all agree is an important topic for this hearing.

Just to bring the Committee up to date since our appearance at your field hearing in Anaheim in December, EPA has continued to make substantial progress in putting our own house in order by ensuring that our internal systems are Y2K compliant. I am pleased to report that we have evaluated all of our mission-critical systems for vulnerability and have completed the appropriate conversion steps. This success was recognized by the Subcommittee on Government Management, Information, and Technology of the House Committee on Government Reform, and we remain in OMB's top tier ranking of Federal agencies making very satisfactory progress. My ensuring the readiness of these systems, we expect to be prepared to continue to protect public health and the environment on January 1, 2000, and beyond.

Now let me turn specifically to the subject of the impact of Y2K disruptions on chemical safety. As you know, EPA is the Federal agency with primary responsibility for ensuring that the environment and the public are protected from the unreasonable risks of toxic chemicals and other dangerous substances. We identify chemical hazards in the environment, regulate the use of pesticides, protect the public from existing and proposed new toxic chemicals in the marketplace, prevent and respond to the accidental release of hazardous chemicals, and assess the risks of such releases to public health and the environment. In doing all this, EPA operates under four major legislative mandates: the Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA), the Toxic Substances Control Act (TSCA), the Emergency Planning and Community Right-To-Know Act (EPCRA), and Section 112(r) of the Clean Air Act Amendments of 1990.

#### *EPA's Relationship With the Chemical Industry*

Under TSCA and FIFRA, the Agency evaluates pesticide and chemical products entering commerce to safeguard against public health hazards and environmental harm. Under FIFRA, this is accomplished by registering and reregistering new and older pesticide active ingredients and by establishing maximum levels for pesticide residues in food. EPA also promotes the use of safer chemicals and manufacturing processes and technologies. Through our pollution prevention programs under TSCA, we encourage the chemical industry to test chemicals in advance of introducing them into the marketplace, to design them at the molecular level to be less toxic to humans and the environment, and to re-engineer chemical processes to make them safer and less wasteful so as to minimize their environmental impact at the time of manufacture.

Following the world's largest chemical accident in Bhopal, India, Congress enacted the Emergency Planning and Community Right-To-Know Act in October 1986, as Title III of the Superfund Amendments and Reauthorization Act. EPCRA helps communities prepare for chemical emergencies and grants citizens and government officials access to information about potential chemical hazards. The law requires industries to participate in emergency planning and to notify their communities of the existence and/or releases of hazardous chemicals. EPCRA's goal is to help citizens, officials, and community leaders to be better informed and understand the risks associated with toxic and hazardous materials in their communities through emergency planning, hazardous chemical inventory reporting, public access to chemical information, hazardous substance release reporting, and the Toxic Release Inventory (TRI) database.

By its enactment of Section 112(r) of the Clean Air Act Amendments of 1990, the Congress recognized the need for facilities to develop or improve their planning and accident prevention programs to reduce the risk of chemical accidents and to allow local communities to enhance emergency preparedness and accident prevention. The law also affirms the rights of citizens to have access to information about the hazards these facilities present. Under the chemical accident provisions of section 112(r), facilities must conduct hazard assessments, establish accident prevention programs, and bolster emergency response planning. EPA implements these requirements through the Agency's Risk Management Program (RMP) regulations which are aimed at reducing the likelihood and severity of chemical releases.

The Risk Management Plan regulations require facility hazard assessments from over 69,000 facilities nationwide which use or store any of 140 specified chemicals. These assessments address off-site disaster risks caused by chemical releases, fires, explosions, or other natural events. Covered facilities must submit to EPA a Risk Management Plan in 1999, have an accident prevention program in place, and have developed an emergency response plan.

EPA also addresses chemical safety through the Emergency Response Program, a coordinated effort among five EPA headquarters offices and our ten Regional Offices using legislative authority derived from EPCRA, the Comprehensive, Environmental Response, Compensation and Liability Act (CERCLA)—also known as Superfund—the Clean Water Act (CWA), and the Oil Pollution Act. Under this program, EPA coordinates and implements a wide range of activities to ensure that adequate and timely response measures are taken in communities affected by chemical releases. The program's primary objectives are to take reasonable steps to prevent such emergencies; to prepare emergency response personnel at the Federal, State, and local levels for such emergencies; and, to respond quickly and decisively to such emergencies wherever and whenever they occur within our national borders. EPA and a network of Federal, State, and local responders stand ready twenty-four hours a day to contain and clean up released chemicals.

#### **Y2K Chemical Sector Outreach**

Based on our legislative authorities in this area and our long-standing relationship with the chemical industry, EPA was asked by the President's Council on Year 2000 Conversion to take responsibility for outreach to three of the more than twenty-five sectors of economic activity identified as high priority. They are water, waste, and chemicals. As the chemical sector lead, we have been working with chemical industry trade associations to help them address Y2K chemical safety concerns, implement plans to assess and repair potential problems, make contingency plans, and keep the public and Federal, State, and local governments informed of progress.

EPA's goal in our outreach to the chemical industry is to encourage and complement industry efforts to the best of our ability. We believe that we can most effectively address potential Y2K-related chemical risks and accidents by building upon our relationships with the industry through our existing statutory and voluntary programs.

In this regard, we have undertaken a broad array of outreach activities with the chemical industry. EPA speakers have addressed numerous fora. We have distributed specific "tool kit" materials including brochures, handouts, articles, and guidance documents. We have coordinated extensively with chemical industry trade associations. One of the larger trade associations, the Chemical Manufacturers Association (CMA), representing over 190 chemical companies, has initiated programs to share solutions and information with its member companies through the development of a comprehensive Internet website, Y2K contingency planning workshops, and a Y2K workgroup with an extensive industry-wide membership.

The chemical industry and its trade associations are our primary and best source of information related to plant operations, process management, and equipment and systems. In our chemical sector outreach, we will continue to provide additional helpful information regarding Y2K impacts on chemical company operations. We recognize, however, that chemical plant managers possess the knowledge, experience, and expertise on which we must rely. To this end, we have strongly encouraged the trade associations to develop additional information-sharing opportunities as they continue Y2K planning activities in the balance of 1999. CMA has positively responded to this challenge by agreeing to use its Responsible Care program to share Y2K information among members. In addition, the Chemicals Information Technology Association (CITA), a sub-group of CMA member companies participating in the CMA Y2K Workgroup, has developed a Y2K contingency planning guide for use by Association members.

#### **Raising Y2K Awareness**

EPA has chosen a coordinated approach of direct outreach to relevant stakeholders, data submitters, and pesticide registrants to ensure that no environmental programs are compromised and that every effort is taken to minimize the potential deleterious effects of computer problems on the regulated community. EPA's Office of Prevention, Pesticides, and Toxic Substances has directly contacted its primary group of data respondents—including Toxic Release Inventory (TRI) facilities—and pesticide registrants to remind them of their obligation to ensure the integrity of data reported to the Agency. Companies were also encouraged to work closely with testing laboratories and field sites to ensure that the data, which the Agency must act upon, is valid and reliable.

To further increase Y2K awareness among chemical companies, EPA's Chemical Emergency Preparedness and Prevention Office (CEPPO) developed a Year 2000 Chemical Safety Alert for the chemical industry. The Alert, a copy of which I am submitting with my statement, summarizes the steps that facilities need to take to address Y2K problems and lists the technical resources available on the Internet to help them, such as guidelines, planning documents, testing tools, solutions, services, and product status databases. The Alert urges facilities to prioritize critical systems

for Y2K remediation and testing and emphasizes Y2K contingency planning in coordination with emergency planning and response partners.

#### **Assessment of Chemical Industry Readiness**

As is the case in other sectors, assessments of readiness are largely based on Y2K industry surveys. A number of these surveys have been conducted throughout the chemical industry. The most complete survey work has been done by CMA. As of March 1999, nearly 40% of CMA's respondents—those who provided dates—expect to be Y2K ready by the end of March 1999; 90% say they will be ready by the end of September 1999; and, all respondents indicate they will be Y2K ready by December 1999. The survey results also indicate that as of February 1999, all of the respondents have action plans in place to address their potential Y2K problems. Of the respondents, 99% have plan elements that include prioritization of the company's hardware, software, and embedded systems according to their mission-critical functions; 96% of the plans include elements to assess supporting infrastructure systems such as communications, power, and other building systems; 98% have addressed the readiness of key suppliers, customers, and organizations that make up the supply chain; and 97% address safety, environmental, and health systems. Testing of mission-critical systems is a plan element for 98% of the respondents; 89% have plans to communicate Y2K readiness internally; 81% plan to communicate externally; and, 92% of the respondents have contingency planning elements for all business systems.

In addition to the CMA survey, which serves as an indicator of sector readiness, many CMA members are members of other trade organizations currently working with the President's Council on Y2K issues. The most notable trade association with strong ties to and shared membership with CMA is the American Petroleum Institute (API). API surveys have reported high states of readiness among member companies.

Based on these surveys and others conducted by the Chlorine Institute and the Pharmaceutical Research and Manufacturers of America, we feel confident that large companies with sufficient awareness, leadership, planning, and resources are unlikely to experience Y2K failures. We are not as confident, however, about the readiness of small and medium-sized plants. Our participation in the U.S. Chemical Safety and Hazard Investigation Board's December 18, 1998 workshop, convened to discuss Y2K and chemical safety issues, bears out this finding. As highlighted in the Board's report, we simply do not have adequate information about the readiness of smaller companies.

#### **Small and Medium-Sized Company Preparedness**

To address the issue of preparedness among small and medium-sized companies, EPA's Office of Chemical Emergency Preparedness and Prevention (CEPPO) and our Office of Prevention, Pesticides, and Toxic Substances (OPPTS) have initiated a number of recent activities. In cooperation with CMA and the U.S. Chemical Safety and Hazard Investigation Board, EPA organized a trade group meeting of smaller or specialty chemical companies with a membership of approximately 7,000–10,000 chemical manufacturers, formulators, retailers, and distributors. This group has undertaken an additional survey to determine the extent of the Y2K problem among smaller companies and of the Y2K remediation efforts which may still be needed. We expect the results of this survey in late spring. Using these results, we hope to formulate more targeted plans for those companies identified as vulnerable.

EPA implemented an outreach campaign aimed at distributing the Y2K Safety Alert to small and medium-sized companies during the Spring of 1999. CEPPO also sent an electronic copy of the Alert to a group of small business trade associations and State Small Business Assistance Centers with which we maintain regular contact. EPA also made the Alert available to the 69 district offices that participated in the recent Small Business Administrator's "National Small Business Y2K Action Week."

In addition, we are encouraging the development of a new guidance document based on expertise drawn from this group for use by small and medium-sized chemical companies. This document will be jointly developed and distributed by EPA, the Board, CMA, the Center for Chemical Process Safety (CCPS), and the consortium of smaller and specialty chemical associations. In order to help us determine the most useful Y2K information needed by the smaller companies, the trade associations will be soliciting recommendations from their membership.

#### **Preparedness to Respond to Potential Chemical Industry Y2K Failures**

EPA's approach is to build upon—not create anew—the existing Federal emergency planning network to address Y2K risks in a number of ways. EPA's Office of Chemical Emergency Preparedness and Prevention (CEPPO) and Office of Emergency and Remedial Response (OERR) actively manage EPA's national level program for preparedness, planning and coordinating response to chemical releases.

EPA is involved in a network of contingency plans, representing different levels of geographical scope, which forms the backbone of our country's efforts to prepare for and coordinate responses to emergency incidents, including those resulting from Y2K malfunctions. This network is called the National Response System.

The National Contingency Plan is the Federal government's primary plan to prepare for chemical emergencies and to coordinate with other emergency responders. The Federal government also prepares Regional and Area Contingency Plans that coordinate effective responses within each of the ten standard Federal Regions and other designated Areas covering Alaska, the Caribbean, and several islands in the Pacific. At the local level, Local Contingency Plans are developed to prepare and organize local resources in the event of the accidental release of hazardous substances.

Under the Emergency Planning and Community Right-to-Know Act of 1986 (EPCRA), State governors establish State Emergency Response Commissions (SERCs), which, in turn establish Local Emergency Planning Committees (LEPCs) for districts within each State. These emergency planning organizations are responsible for developing local contingency plans using chemical inventory information collected as part of the law's community right-to-know provisions. EPA has urged the SERCs and the LEPCs to encourage their local industrial facilities to address Y2K problems and to coordinate Y2K emergency response plans with the LEPCs.

We are working directly with the Federal Emergency Management Agency (FEMA) and the National Response Team (NRT) to carry out a full range of Y2K contingency planning activities across all Federal agencies. Recently, EPA served as a key participant in FEMA-organized Y2K contingency planning workshops. These workshops were designed to allow Federal planners to exchange readiness and planning information with emergency responders at the State and local level. Approximately 2,000 emergency management specialists, with representatives from every State, attended these workshops. EPA has been vigorously participating in many planning efforts as a Federal Response Plan lead agency with a particular emphasis on carrying out our responsibilities as the Chair for the Emergency Support Functions for Hazardous Materials. As a result of the Emergency Planning and Community Right-to-Know Act, Local Emergency Planning Committees (with participation from State and local planners and other community officials and representatives) already have contingency plans in place for emergency response. These contingency plans are designed for many types of hazardous materials emergencies, including those caused by potential Y2K disruptions.

#### **Y2K Planning Linked to the Risk Management Program**

Mindful of the potential for process shutdowns and accidental releases, EPA has encouraged facility managers to think about their Y2K readiness as they prepare their Risk Management Plans (RMPs). EPA's previously described Y2K Chemical Safety Alert reminds managers that addressing Y2K risks is part of their responsibility to prevent accidents under the General Duty Clause of Section 112(r) of the 1990 Clean Air Act Amendments and Risk Management Program requirements. We also have placed Y2K reminders in the RMP reporting instructions and on our Website. RMP plans submitted to EPA must describe how facilities prevent or minimize chemical accidents and how they will promptly respond to accidents that do occur. EPA is encouraging facilities to address their Y2K readiness in an RMP executive summary. Linking sound Y2K planning to the Risk Management Program is consistent with our approach of utilizing existing regulatory and voluntary programs to address Y2K readiness.

#### **Y2K Enforcement and Compliance Assurance Program**

EPA expects the chemical sector, like every other sector, to be in compliance with environmental regulations before, during, and after the Year 2000. Regulated entities will not be allowed to use computer-based failure as a shield for not discharging their environmental compliance obligations. At the same time, EPA's Office of Enforcement and Compliance Assurance is actively working in several ways to promote the timely assessment and correction of Y2K problems.

EPA issued its Y2K enforcement policy on November 30, 1998. The policy is designed to encourage prompt testing among all sectors of computer-related equipment to ensure that environmental compliance is not impaired by the Y2K computer bug. Under the policy (published on the Internet at [www.epa.gov/year2000](http://www.epa.gov/year2000) and in the March 10, 1999 *Federal Register*), EPA states its intention to waive 100% of the civil penalties that might otherwise apply, and to recommend against criminal prosecution for environmental violations caused during specific tests that are designed to identify and eliminate Y2K-related malfunctions. The civil penalty waiver and recommendation against criminal prosecution are limited to testing-related violations disclosed to EPA by February 1, 2000, and are subject to certain conditions, such as the need to design and conduct the tests well in advance of the dates in question, the need to conduct the tests for the shortest possible period of time nec-



essary, the need to correct any testing-related violations immediately, and other conditions to ensure that protection of human health and the environment are not compromised.

EPA's recent publication of the policy in the *Federal Register* incorporated numerous clarifications suggested by commenters, some of which are directly relevant to chemical industry safety. For example, the policy now clarifies that Y2K testing protocols should be designed to prevent or limit violations that may result from such testing (e.g., through adoption or revision of appropriate contingency plans). This will help to ensure that all prudent steps are taken to ensure that such testing is as safe as possible. For violations occurring after January 1, 2000, EPA's long-standing enforcement response and penalty policies will continue to recognize a chemical facility's good faith efforts to test and remediate Y2K problems and other potentially mitigating factors in determining an appropriate enforcement response.

The enforcement and compliance assurance program is also reaching out to educate the chemical industry about Y2K problems. ChemAlliance, the Internet-based compliance assistance center for the chemical industry, posts a Y2K notice on its front page. (ChemAlliance is the product of a partnership between the chemical industry through various industry organizations, EPA's Office of Enforcement and Compliance Assurance, academia, and others.) The website ([www.chemalliance.org](http://www.chemalliance.org)) highlights the six-step action plan, described in EPA's Y2K Fact Sheet, "The Millennium Bug," and provides real life examples of equipment failure at chemical plants caused by confusion over leap year and Y2K testing, and offers links to EPA, other Federal, and trade and industry resources for Y2K. We believe these actions will help to motivate chemical companies to proactively meet their Y2K responsibilities.

#### *Summary*

In closing, we believe the chemical industry is making good progress in its efforts to identify and fix potential Y2K problems. EPA intends to continue working with chemical industry associations, private groups, and the U.S. Chemical Safety and Hazard Investigation Board to assess readiness, to promote effective planning, and to encourage the sharing of preparedness information with chemical customers, the general public, and local, State, and Federal officials. In doing so, we will utilize the many existing mechanisms available which are designed to allow us to perform our statutory responsibilities in this area as well as to effectively address potential Y2K problems in the chemical sector. We intend to continue to make this effort a priority with the help of this Committee.

Again, thank you for the opportunity to appear here today. I would be pleased to answer any questions you may have.

---

#### RESPONSES OF JAMES L. MAKRIS TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

*Question 1.* The recent GAO study on the Y2K activities of state regulatory agencies in the water and wastewater industry revealed a lack of engagement on the Y2K issue on the part of many state regulatory agencies. One of our other witnesses here today has criticized the New Jersey Department of Environmental Protection's for being inactive on Y2K. What is EPA's assessment of the activity level of state environmental protection agencies across the country on the Y2K issue in the area of chemical safety? What effort has EPA made to engage the state environmental protection agencies on the Y2K issue?

Answer. To date, Year 2000 issues at the State level have typically been centrally managed by State Chief Information Officers. The President's Council has been coordinating very closely with the State CIO community directly and through the National Association of State Information Resource Executives (NASIRE) which represents State CIOs to address readiness internally and externally within each of the States. Surveys conducted by NASIRE have included questions on State outreach to key industries. Information from the NASIRE surveys do not provide enough information to reach reliable conclusions for environmentally-related sectors.

In an additional attempt to obtain Y2K sector readiness information at the State level, EPA encouraged the Environmental Council of States (ECOS), an organization representing State environmental officials to conduct a survey of their members which addressed internal and external readiness. While this survey, completed in April, indicated substantial progress in addressing state environmentally-related systems, the amount of data on sector progress collected by the State environmental agencies confirmed that the State CIO organizations remain the primary responsible organization for determining State readiness.

Despite an apparent lack of State sector information available through formal surveys, EPA believes progress in being made based upon on-going staff to staff discus-

sions. We believe that the State environmental agencies are engaging businesses and municipalities on Y2K issues. EPA has been widely sharing fact sheets, guidance documents and reference materials which we have been encouraging the States to use and disseminate. One of the more widely distributed of these documents, "Prevent Year 2000 Chemical Emergencies", has been distributed to State emergency planners and environmental program administrators. In some instances, we have assisted the States in preparing mailings of such material.

In March, EPA's Deputy Administrator asked our Regional offices to engage directly State environmental administrators to discuss readiness in sectors which have a potential affect on the environment and public health. This request was followed up with a letter from EPA's Assistant Administrator for Water to the EPA Regional offices asking that Y2K readiness of drinking water and wastewater treatment facilities be included in regularly scheduled annual State program reviews. In the coming months, we expect Y2K issues and readiness at the State level to be an important topic in meetings and discussions.

Finally, EPA is currently involved in the implementation of the Risk Management Program established as a result of Section 112(r) clean Air Act Amendments. The Risk Management Program requires chemical facilities to submit plans which describe how facilities prevent or minimize chemical accidents. EPA has issued a specific reminder that each facility has a general duty to address Y2K vulnerabilities in their plans. State environmental agencies are active participants in the RMP process.

*Question 2.* The EPA has taken a very positive step in its amendment of its enforcement policy in regard to violations occurring during Y2K testing. Has EPA been able to analyze the effectiveness of the policy change yet? Do we have any firm evidence that it has in fact encouraged more testing? Has EPA received any reports of testing related problems or violations?

*Answer.* EPA has not conducted analyses concerning the effectiveness of the policy or obtained empirical evidence demonstrating that its Y2K Enforcement Policy has encouraged more testing. Anecdotal reports, however, suggests that the policy is contributing to the momentum towards early testing. The public comments on EPA's policy have been very positive, and comments at conferences and in other contexts since then also have been very favorable. In addition, other Federal agencies and several States recently have adopted identical or very similar policies to encourage testing, and EPA has heard that other States are in the process of following suit. Given the dual State/federal nature of environmental regulation, we believe that regulated entities will feel even more comfortable doing Y2K testing as more and more States follow EPA's lead in adopting this type of enforcement policy.

On June 17, 1999, the Associated Press (AP) reported that a water reclamation plant malfunctioned during a test of the facility's contingency plan and spilled four million gallons of sewage into a San Fernando Valley park near Los Angeles, California. The AP report stated that the sewage welled up out of a manhole near the plant in Van Nuys, California, on the night of June 16th and flowed about 100 yards into the park, according to Linda Aparicio, a spokeswoman for the city Public Works Department. Crews reportedly worked to vacuum up the spill, but health officials recommended that a portion of the park remain closed for two days as a precaution. The AP report further stated that Y2K test simulated a scenario in which the power failed. The emergency generator reportedly kicked in as expected, but a gate failed to reopen, Ms. Aparicio said. "Our computers did not tell us that gate was closed," she said. "No one knew that sewage was backing up." She said it was unclear weather the problem was related to the test or was coincidental. The AP reported that the sewage system was back in operation by Thursday morning, June 17. On June 18, 1999, the Los Angeles Times carried an expanded report on the spill. EPA is doing some further investigation of this incident.

*Question 3.* Does EPA have any evidence to suggest that funding has been an impediment for small or medium size companies? If so, what has been done to alleviate this impediment?

*Answer.* EPA regularly engages the small business community in a variety of fora to discuss regulatory and administrative issues. We have addressed Y2K readiness with small business representatives on a number of occasions. We have not heard from participants in these discussions that lack of financial resources will impair Y2K readiness nor do we have any evidence to suggest that funding has been an impediment for small and medium sized companies.

Recognizing that technical and financial resources may be an issue with some businesses, EPA has developed a "Tool Kit" for small business distributed by the Agency's Small Business Ombudsman. This tool kit contains fact sheets, guidance documents, check lists and other reference materials to conduct an in-house assessment and remediation effort. In addition, information about SBA loan and technical

assistance efforts has also been shared with the small business representatives with whom the Agency meets regularly.

In the Chemical sector, EPA has been working closely with a cluster of small and specialty chemical trade associations to develop a survey of readiness among the smaller chemical companies. This survey, completed in May, indicates high levels of readiness by the end of the calendar year. In addition, we are assisting this group of trade associations with a guidance documents, "Addressing Year 2000 Issues in Chemical Facilities: Guidance for Small and Medium Sized Companies". This document will be available this summer.

*Question 4.* How will EPA fit into the overall federal government strategy of monitoring events occurring around the date change? Will there be any mechanisms established to provide real time monitoring of Y2K related incidents in the chemical industry?

Answer. EPA is working within the existing framework established by the Catastrophic Disaster Working Group (CDRG), which is composed of Federal agencies and departments to collect information on significant Y2K incidents. The CDRG will be following a Federal Response Plan Operation Supplement for Y2K Consequence Management, which will be finalized next month. Reporting for Y2K incidents will follow a local-to-state-to-region-to-FEMA headquarters scheme. The information collected will allow the CDRG to identify and respond to those incidents of a magnitude that would require notification of and assistance from other Federal Agencies. In addition, EPA will have its own Emergency Operations Center activated to collect information on chemical accidents for which EPA Regions normally receive notification from the National Response Center. EPA and the CDRG are currently working with the newly established Y2K Information Coordination Center (ICC), which will be collecting information about system operations during the date roll-over period and providing this information to decision-makers and the public. The ICC will collect information from all of the existing government emergency operation centers as well as from industry information centers.

*Question 5.* What are EPA's greatest concerns regarding the potential for hazardous material releases due to Y2K problems?

Answer. Our greatest concerns are those accidents which could seriously threaten the safety or health of workers, the local community and the environment. However, it is unlikely that a single Y2K failure could by itself cause a catastrophic chemical accident. It is difficult to predict what the outcome might be from multiple failures or combination of control and utility failures. We are optimistic that industrial facilities that manufacture or use chemicals are making reasonable efforts to address potential Y2K problems as well as preparing contingency plans. However, the ability to respond to a chemical accident could be hampered by Y2K disruptions in electricity, water supply, and communications. Therefore, it is necessary that response agencies have contingency plans in place to work around these problems as well as fix their internal Y2K problems. Response agencies should also be prepared to handle a larger number of incidents over the transition period if Y2K problems cause industrial accidents.

*Question 6.* How has EPA engaged State Emergency Response Committees or Local Emergency Response Committees in preparing for Y2K incidents in the chemical industries?

Answer. SERCs establish LEPCs, which in turn are responsible for developing local contingency plans using chemical inventory information collected as part of community right-to-know regulations. Thus, these organizations should be prepared to handle chemical incidents regardless of whether they are caused by Y2K or some other problem. Approximately 2,000 emergency management specialists attended ten FEMA-organized Y2K contingency planning workshop where EPA was a key participant. EPA's Y2K Chemical Emergency Alert (posted on our Web site) encourages facilities to communicate and coordinate Y2K contingency plans with their LEPCs. EPA has distributed the Alert to LEPCs and SERCs. In addition, EPA has urged SERCs and LEPCs to encourage state and local emergency service providers to conduct internal Y2K audits to ensure that they are able to carry out their emergency response functions. The SERCs and LEPCs were also asked to encourage their industry contacts to conduct Y2K audits of systems that protect against releases of hazardous chemicals to the environment. LEPCs may also conduct their own follow up of Y2K readiness of facilities that use chemicals. For example, the City of Ann Arbor and Washtenaw County LEPCs are requiring a Y2K compliance plan for all facilities in their county that use, produce or store more than 55 gallons of chemicals.

Finally, FEMA has provided a guide for State and Local Emergency Managers, Contingency and Consequence Management Planning for Year 2000 Conversion, to help them protect public safety and health if Y2K incidents (not limited to chemical

incidents) occur. EPA has developed and made available on its Web site, a paper with Y2K planning ideas that can be used by emergency response organizations.

*Question 7.* Hazardous chemicals must be treated with a "cradle to grave" approach in today's world. The proper treatment of the waste is just as important as the care of the raw material and manufactured products. Does EPA have concerns about the machines that produce date information that goes with labels or manifests for chemical waste products?

*Answer.* First a brief word about manifests. Hazardous waste manifests only accompany hazardous waste shipped off-site by a generator. Usually, a hazardous waste manifest is a multipart form, which is created for each specific, individual shipment of waste. Currently, the federal Uniform Hazardous Waste Manifest (EPA Form 8700-22) includes the name of the designated receiving facility, the shipper's EPA identification number, and a description of the waste based on Department of Transportation (DOT) requirements. DOT's requirements usually include information about the proper shipping name and hazard class.

The only dates of concern regarding a hazardous waste manifests are: (1) the date the transporter accepts the waste, and (2) the date it's delivered to a treatment, storage, or disposal facility. All of this information is specific to each waste shipment, and is manually written on the manifest.

*Question 8.* Would you explain how the responsibilities for chemical incidents involving waterways are divided between EPA and the Coast Guard? Has EPA coordinated its emergency response plan with the Coast Guard for chemical incidents on waterways that may occur with the millennium rollover?

*Answer.* EPA and the USCG share responsibility for providing On Scene Coordinators (OSCs) to respond to chemical or oil emergencies. USCG has primary responsibility on land or water in the coastal zone. EPA has primary responsibility on land or water in the inland zone. Each EPA Region has a Memorandum of Understanding with USCG which specifically delineates the line between inland and coastal zones; for example, EPA Region III and the USCG (MSO Baltimore) might delineate the break point along the Potomac River at the Key Bridge. In some cases responsibility may be shared, or assumed by the first responder able to arrive at the site.

EPA and USCG cooperate in standing Regional Response Teams and the Area Committees to ensure coordinated and efficient emergency response plans, including potential incidents that may occur with the millennium rollover.

---

PREPARED STATEMENT OF CHARLIE B. MARTIN, JR.

#### **Introductory Comments**

Chairman Bennett and members of the Committee, my name is Charlie B. Martin and I am the Site Safety Coordinator at Hickson DanChem Corporation. Thank you for inviting me to appear before you today on this distinguished panel. Although our company is not physically located in New Jersey, the issue we are addressing here today does not vary across state lines. I am here today to present my industry's perspective on Y2K contingency planning for both inside and outside the company fence.

Hickson DanChem is engaged in the custom manufacturing of organic and inorganic specialties for major chemical companies. It also produces a comprehensive line of textile chemical auxiliaries and specialty surfactants. In layman's terms, we make the chemicals that are used for fabric conditioning, paint additive, and personal care products. The company employs 132 persons at our plant in Danville, VA and uses batch manufacturing processes.

My company is a member of the Synthetic Organic Chemical Manufacturers Association (SOCMA). SOCMA is the leading trade association representing the batch and custom chemical industry. This industry produces over 90 percent of the 50,000 chemicals produced in the U.S. while making a \$60 billion annual contribution to the economy. SOCMA's 300+ member companies are representative of the industry and are typically small businesses with fewer than 75 employees and less than \$40 million in annual sales.

As the site safety coordinator, I serve on our Y2K compliance team. Since the last panel addressed Y2K activities generally, I will focus my comments on the last step of Y2K preparation—contingency planning. It should be noted that our company will be Y2K compliant on June 30, 1999. In developing the final draft of our emergency contingency plan, Hickson DanChem tried to foresee every possible situation, however remote. Our plan covers safe process operations, emergency response planning and community dialogue.

We are pleased to see that today's panel reflects those stakeholders that should be involved with industry's community awareness and emergency preparedness ef-

forts. An effective and successful plan must involve the collaborative participation of the company, its workers, government, emergency responders and the community. My testimony today will address Hickson DanChem's continued dialogue with these groups and describe how many of the activities related to Y2K contingency planning are a normal part of business for the chemical industry as a result of voluntary initiatives such as Responsible Care® and federal and state regulations.

#### **Employee Participation**

As Hickson DanChem conducted its Y2K assessment, employees played a critical role. In fact, employee involvement is not unique to Y2K safety activities. Recognizing that the involvement of our employees is paramount to a successful employee health and safety program, we have always included our employees in developing safety plans and procedures. This involvement complements our implementation of federal regulations such as the Occupational Safety and Health Administration's Process Safety Management Rule (PSM), company safety policies, and the chemical industry's health, safety and environmental initiative, Responsible Care®. Specifically, SOCOMA's guidance for the Responsible Care® Employee Health and Safety and Process Safety Codes provides guidelines for company practices that complement federal occupational safety regulations. Coupled with regulatory requirements, these guidelines address many of the potential results of Y2K technology problems.

Specific activities in place at Hickson DanChem include a formal Site Safety and Health Committee comprised of eight task groups that participate in various areas of our safety program. They also perform housekeeping and hazard assessment audits throughout the site. We hold monthly shift training sessions on related OSHA and home safety topics as well as conduct training on regulatory topics using the computer. Departmental safety meetings are also held monthly and five minute supervisory safety talks are performed daily. Hazard/Operability (HAZOP) studies are performed on new and existing processes and include countermeasures for suspected failures. HAZOP action items result in decisions such as installing emergency shutdown devices in conjunction with process control systems for specific processes.

Regarding impacts specific to Y2K, our on-site Y2K assessment team performed formal evaluations for Business Information Systems, Process Control Systems, Fire and Security Systems, Field Control Units, and QC Lab Equipment. During the roll over period of December 31, 1999–January 1, 2000, provisions were considered for a phased start-up of utilities, system checkouts, and status verifications with Emergency Response agencies before manufacturing processes are resumed.

With their assistance, we have integrated Y2K related activities into our existing safety program.

#### **Emergency Response**

Another important aspect of an effective company safety program is involvement with local emergency response teams. Hickson DanChem has an Emergency Response Plan and has incorporated Y2K related activities into it.

Under Title III of the Superfund Amendments and Reauthorization Act (SARA), States are required to establish Local Emergency Planning Committees, better known as LEPCs. Each LEPC is responsible for working with industry to develop emergency response plans for its community that take potential risks from a chemical related accident into account; collecting and storing information provided by facilities; and making it available to the public. Representatives to the LEPC include individuals from the fire department, emergency management agencies, local health agencies and hospitals, local officials, community groups, media, and local businesses. Hickson DanChem participates in the Pittsylvania County LEPC by providing technical expertise in the planning process, assisting with the training of local responders in handling hazardous chemicals, providing information about chemicals and transportation routes, offering in-kind assistance in the planning process and hosting regular plant tours and emergency response drills for local responders. In fact, we held a major emergency response drill on March 11, 1998, in which many Y2K related activities were addressed such as internal and external alarm system notifications to both County and City emergency response agencies. The drill was noted as being the first of its magnitude in our area. Since that time, lessons learned have enabled us to identify potential challenges and make continuous improvements in our system.

Responsible Care® also plays a significant role in Hickson DanChem's interaction with local emergency responders. The Community Awareness and Emergency Response Code, or CAER Code, encourages facilities to take a leadership role in the LEPC and initiate activities that go beyond the requirements of SARA. For example, The CAER Code provides guidelines on participation in the community emergency response planning process to develop and periodically test the comprehensive community emergency response plan developed by the LEPC. Because of our involve-

ment with our County LEPC, I am proud to say that I have just been named to serve on the City of Danville Emergency Planning Committee.

As you can tell, handling chemicals has led the industry to develop extensive plans to address potential incidents covering both on-site and off-site consequences. However, Y2K presents a unique set of potential consequences, such as potential multiple system failures. As such, our emergency response plans designate actions to be accomplished should these type situations arise.

#### **Dialogue with Community**

Communicating Y2K compliance with your local community establishes public confidence and provides opportunities for open dialogue between the community and the plant. Several of our customers, suppliers, and business support agencies have requested and been provided information on our Y2K progress. Our information systems manager participated in a Y2K drill with our regional medical center. The drill proved beneficial for both Danville Regional Medical Center and Hickson DanChem. Participation in seminars as a member of the Pittsylvania County Safety Roundtable provided information to local small industries on Risk Management Plan (RMP) preparations. A symposium hosted by the Danville LEPC was held on April 29, 1999 to further enhance their understanding. Hickson DanChem has also sponsored programs, such as Educators in the Workplace to provide awareness information to local area teachers and counselors.

#### **Conclusion**

Hickson DanChem is committed to having an effective emergency response plan that avoids the potential Y2K technology concerns. Many of the contingency planning activities for Y2K readiness in the chemical industry are being addressed through procedures and practices that are already in place. However, Hickson DanChem has added additional measures to ensure the safety of our employees, neighbors, environment and equipment come December 31, 1999 and January 1, 2000. The involvement of our employees and local emergency responders has led us to develop an effective and open community dialogue and on and off site contingency plan.

Though Y2K presents cause of concern, we have addressed these issues in the same manner as we address all emergency response issues— by assessing the potential problems carefully and thoroughly, implementing preventative measures, and testing to ensure that potential problems have been adequately addressed. Contingency planning is an important part of doing business for our company. Hickson DanChem can say with confidence that we are prepared for the safe transition to the year 2000.

Mr. Chairman, we appreciate the opportunity to appear before you today. The Y2K issue warrants the collaborative efforts of all of the stakeholders before you today. We welcome your leadership and look forward to a transition to a safe and prosperous new millennium.

---

#### RESPONSES OF CHARLIE B. MARTIN, JR. TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

*Question 1.* You indicated that your company has tried to anticipate a wide range of contingency planning scenarios. Do you think the industry has placed sufficient emphasis on the need for contingency planning?

Answer. Risk management plays an important role in the daily operations of chemical manufacturing facilities. My initial statement for the committee referred to the Responsible Care® program as an example of risk management activities that take place at many chemical facilities. The industry's commitment to this program shows that contingency planning is, and has been, in place for many years. Many Y2K-related activities and emergency planning are inherent, although not expressly designed for Y2K, within the Responsible Care® program. Although Responsible Care® is not practiced at every chemical manufacturing facility in the United States, participation in the program is a requirement of active membership in the Synthetic Organic Chemical Manufacturers Association (SOCMA). The Chemical Manufacturers Association and other chemical industry trade associations.

In addition to programs such as Responsible Care® members of our industry are also subject to a number of federal regulatory requirements that indirectly address the types of risks and necessary planning that are implicated by Y2K issues. For example, most chemical manufacturing facilities must submit facility-specific risk management plans to the U.S. Environmental Protection Agency (EPA) by June 21, 1999, to comply with the Risk Management Planning Rule (RMP) under the Clean Air Act § 112(r). 40 CFR § 68. Under the RMP, chemical facilities must submit their facilities' plans to address potential risks and hazards at the facility level. In the

preparation of their RMPs, most companies will be evaluating potential Y2K-related events such as loss of power and chemical releases.

Similarly, Title III of the Superfund Amendments and Reauthorization Act (SARA), requires states to establish Local Emergency Planning Committees (LEPCs). Each LEPC is responsible for working with industry to develop emergency response plans for its community that take potential risks from a chemical-related accident into account; collecting and storing information provided by facilities; and making it available to the public. As I stated in my testimony, our company has been very actively working with our LEPC on Y2K-related issues. Although I believe this is true for other companies in the industry, I do not have specific information in this regard.

*Question 2.* The Chemical Manufacturer's Association and its associated Chemical Information Technology Association have developed contingency planning guidance. Do you have a feeling for how widely distributed and used these materials have been?

Answer. Hickson DanChem is not a member of the Chemical Manufacturers Association and therefore, I cannot comment about the distribution of the document. Members of the Chemical Manufacturers Association or the association's staff would be better equipped to respond to this question.

*Question 3.* You mentioned that it is very important that chemical plants have a dialogue with their local communities. In your opinion, is the majority of the chemical industry engaging its local community (hospitals, emergency services and the general public) in a Y2K dialogue?

Answer. My knowledge and experience of this issue involves specific activities that have taken, or will take place at Hickson DanChem. As I stated in my testimony, on March 11, 1998, Hickson DanChem participated in one of the first Y2K-related emergency response drills in our area. I am not in a position to answer this question on behalf of the industry as a whole.

*Question 4.* You mentioned that the Pittsylvania County Safety Roundtable provided many small industries with valuable Risk Management Plan information. In your opinion, is an adequate job being done in reaching out to the industry and the public to raise awareness on the Y2K issue?

Answer. The chemical industry has been made aware of the Y2K situation through various media including insurers and computer providers. The chemical industry trade associations also have provided information to their members about the Y2K situation. For example, SOCMA has been actively involved with the Y2K issue for quite some time. Specifically, the association has written numerous articles in its magazine, has had technology experts give presentations at meetings and has dedicated a page on its Internet Web site to address the issue and link to numerous sources of information and guidance materials. Additionally, SOCMA currently is working with EPA and other chemical industry trade associations to develop a document intended to assist small and medium-sized companies with their Y2K assessments and contingency plans. All parties contributing to this effort are committed to distributing the document beyond their respective memberships and constituencies.

Generally speaking, I am not in a position to determine whether Y2K awareness activities in general, or to the public at-large are adequate.

*Question 5.* The Chemical Safety Board recommends that all chemical processors continuing operations through the year 2000 transition should have plans and trained staff who could manually assume control of the plant. What do you think of these recommendations? In your opinion, is the industry incorporating these suggestions into their contingency and continuity plans?

Answer. The CSB's recommended procedures are part of our daily operating schedule. As a batch processor, our company's manufacturing processes require intermittent introduction of frequently changing raw materials, and have varying process conditions. Therefore, equipment often is idle while waiting for raw materials, waiting for quality control checks, undergoing cleaning, etc. Due to the nature of batch manufacturing, it rarely pays to automate a system. Additionally, batch chemical processes start and shut down daily, if not multiple times during any given day. Consequently, at our company, as at the most batch operations, we depend upon by highly skilled operators who manually control operations.

Although I would expect that most batch processors similarly would in the normal course depend upon manual operation of their plants, I do not have specific information in that regard.

---

## PREPARED STATEMENT OF JANE NOGAKI

Mr. Chairman and Members of the Committee:

Thank you for extending to the New Jersey Work Environment Council and the New Jersey Environmental Federation the opportunity to testify here today about concerns that citizens and workers of this state have regarding potential Y2K problems in facilities using hazardous chemicals. My name is Jane Nogaki and I have been involved in community and environmental Right to Know issues for 20 years. I am a Board Member of the New Jersey Work Environment Council, a statewide alliance of labor and environmental activists, and I am the Pesticide Program Coordinator for the New Jersey Environmental Federation, a nonprofit coalition composed of 80 organizations and 90,000 members. I am also a resident of Marlton and a public member of the Burlington County Local Emergency Planning Committee.

The New Jersey Work Environment Council and the New Jersey Environmental Federation are concerned about the potential public and occupational health risk posed by chemical releases resulting from Year 2000 ("Y2K") computer problems. It is our contention that, despite corporate and government efforts to identify and remedy Y2K problems, the situation in New Jersey remains perilous for workers and residents alike. At the same time, if policies are properly designed and implemented to address this potential health risk, New Jersey's workers and residents—working in cooperation with facilities using hazardous chemicals and the state's Department of Environmental Protection—may be able to seize opportunities to increase awareness about toxics in our neighborhoods and workplaces.

**THE CURRENT Y2K PROBLEM**

As you know, Y2K refers to computer programs and chips embedded in millions of control devices worldwide that—unless fixed—may incorrectly read the year 2000 as an entirely different date come the start of next year. Despite assurances, no one knows how many glitches may occur when the clock strikes midnight. The results could include catastrophic chemical releases putting thousands of workers and citizens at risk and damaging the environment.

On April 2, President Clinton said, "We have made tremendous progress in our efforts to address the Year 2000 (Y2K) computer problem. In spite of this progress, however, too many businesses, especially small and medium-sized firms, will not be ready unless they act immediately."

This is indeed true here in New Jersey. We are the most densely populated state and, at the same time, we are a major chemical producer. Not surprisingly, we have the highest concentration of toxic air and water releases of any state in the nation. We have enacted our own laws, such as the Toxic Catastrophe Prevention Act (TCPA), to safeguard workers and the public. Yet there have been 8,247 reported releases of extremely hazardous substances reported to the Department of Environmental Protection (DEP) since 1986, when that law was enacted.

Y2K presents a daunting challenge for the chemical, petroleum and related industries. These sectors of our state's economy are particularly vulnerable, because of their reliance on embedded chips for process control and monitoring. Embedded chips are in alarm systems, computer motherboards, utility and lighting controls, process controllers, refrigeration devices, and pumps and valves. System failures could include emissions sampling and related laboratory analyses, pollution treatment systems, leak detection systems, safety alarms, safety relief devices, security systems (which could lock out critical personnel), and power and water surge detection systems. Nonetheless, some chemical plants, according to one chemical engineering consultant, ". . . have not provided a manual means of shutdown independent of the programmable logic controller." And although many systems are designed to "fail safe" in response to single incidents, experts agree that Y2K glitches may set in motion multiple mechanical failures.

Complicating matters, *most* chemical facilities depend on thousands of outside suppliers—and these vendors may not fix their own problems. Outside vendors can affect plant operations through failure to deliver essential data or chemical feedstocks, or utilities such as power and water. Vendors may spread corrupted data which can infect the plants' own repaired computer systems. Some larger companies are auditing the facilities of their important suppliers to determine if they can count on supplier efforts to remedy Y2K vulnerabilities.

To underscore the problem in the chemical industry, the U.S. Environmental Protection Agency has issued a memo calling attention to the possibility of chemical plant problems stemming from the Y2K issue. The agency has urged state and local emergency planners to prepare and to carry out the emergency response functions.

**NEW JERSEY'S EFFORTS**

We can be proud of the effectiveness of New Jersey's TCPA program, which covers 911 facilities using extremely hazardous substances. We also look forward to expan-



sion of the program, under the U.S. Environmental Protection Agency's Clean Air Act Section 112(R), to approximately 70 additional facilities. Together, these laws authorize the state DEP to collect voluminous risk information data about roughly 160 facilities using high-risk toxics, and they are considered a model for chemical accident prevention.

Yet state government efforts to address potential Y2K problems in the chemical and related industries appear inadequate. Last fall, for example, the DEP conducted an informal survey of 20 New Jersey chemical facilities, concluding that these manufacturers had few date-dependent processing units. DEP simply accepted management's verbal assertions and did not request independent verification and validation data. In addition, DEP ignored invitations and chose not to send a representative to the federal Chemical Safety and Hazard Investigation Board's December, 1998 Y2K conference.

Thus it appears that the DEP, the agency charged with preventing toxic disasters, has put its head in the sand when faced with challenges posed by the "millennium bug." Moreover, it is also apparent that no other agency in New Jersey is independently verifying even the most basic assertions from chemical facilities.

It is clear that Y2K safety issues will continue to be the subject of considerable public discussion and media interests. It is worth noting, therefore, that under Section 112(R) of the Clean Air Act amendments of 1990, June 21 is the deadline for many chemical manufacturers and other employers in New Jersey to make public detailed Risk Management Plans (RMPs). These plans include information about "worst case scenarios" such as fires, explosions and toxic gas clouds. Needless to say, this looming deadline for legally-mandated disclosure of information about potential chemical accidents makes all the more important a strong government response to rising citizen concerns about potential Y2K problems.

#### PROPOSALS

To safeguard against preventable Y2K-related chemical releases, and to assure New Jersey's citizens that both the DEP and facilities in the state that use hazardous substances are taking adequate precautions, we propose the following:

**1. The New Jersey Department of Environmental Protection (DEP) should distribute a Y2K-Preparedness Survey to roughly 160 facilities covered by the Toxic Catastrophe Prevention Act and the EPA Clean Air Act Section 112(R).** This survey should request information about Y2K efforts, including preparedness and planning, to help the DEP determine whether each company is Y2K-compliant. The survey should also include questions about equipment suppliers and other contractors. In addition, respondents should be asked to produce all Y2K-related documents, such as 10(Q) forms filed with the Securities and Exchange Commission. A reasonable deadline should be set to allow companies to complete the survey. Copies of the survey, a list of the companies receiving it and an introductory letter about the importance of Y2K-preparedness should be sent to the appropriate mayors, and Local Emergency Planning Committee members in municipalities throughout the state. The DEP letter should briefly describe the potential human, environmental and economic costs of non-compliance.

**2. For those companies that do not respond to the survey by the deadline, the DEP should conduct follow-up enforcement activities.** These activities should begin with a phone call to companies. If, after telephone contact, companies still do not submit the survey, the DEP should conduct a site visit of the facility or facilities. Note that, according to the TCPA Section 8(a), the DEP has "the right to enter any facility at any time in order to verify compliance with the provisions of this act."

**3. The DEP should conduct Independent Validation and Verification (IVV) audits of a limited number of facilities.** This auditing process would involve spot checks of certain facilities—including review of relevant documents and a possible site visit—to corroborate disclosures made about Y2K preparedness. It would aim to provide some assurance to citizens that assertions made by facilities are valid.

**4. The DEP should generate a brief report detailing the results of the survey and the IVV audits, and make this information available to the public.** This report should document the response—or lack of response—by specific facilities. A summary should then be published in newspapers throughout the state; and the full report should be posted on the agency's Home Page on the World Wide Web and sent to Local Emergency Planning Committees. Moreover, if DEP does not currently have the staff or financial resources to conduct an audit and produce a report, such resources should be made available immediately.

**5. The DEP should initiate a series of local hearings on Y2K preparedness in chemical facilities.** These hearings would provide a forum for citizens, workers

and emergency responders to interact with plant managers about Y2K preparedness.

**QUESTIONS RESIDENTS AND WORKERS SHOULD BE ASKING CHEMICAL FACILITIES**

Among the questions we should be asking chemical facilities at such public hearings are:

1. *Have you completed Y2K-related remediation and testing of your safety-related systems?*
2. *Have you consulted with employees, neighbors and emergency responders in all phases of your Y2K remediation, testing, drills and planning for high-risk periods?*
3. *Have you conducted or planned any facility-wide Y2K testing, either independently or in coordination with outside utilities or suppliers, that has or will shut down your facility?*
4. *From what sources has your facility's Y2K effort been independently audited (sometimes called "independent verification and validation" or "IVV")? Corporate headquarters? Major customers? Local government?*
5. *Have you conducted IVV on your major suppliers?*
6. *Do you intend to employ a "Safety Holiday" strategy (i.e., temporarily shut down your facility during high-risk periods for Y2K problems)? If yes, are you committed to maintaining pay and benefits for employees during this period?*
7. *Have you stockpiled—or do you plan to stockpile—essential chemical supplies for anticipated Y2K outages? If yes, do any of these stockpiled chemicals add to the accident risk at your facility?*
8. *How much (approximate or range in dollars) is your total budget for Y2K work?*
9. *Have you developed Y2K Risk Management Programs (RMPs) as part of your ongoing work under OSHA's Process Safety Management and EPA's Risk Management Planning regulations?<sup>1</sup>*
10. *Under these laws, you must calculate toxics "worst case scenario" releases.*  
*How far is your calculated downwind distance?*  
*How long (in minutes) would it take a facility to realize it had such a release?*  
*How long would it take for the facility to decide not to try to handle it on its own?*  
*How long would it take to notify the fire department?*  
*How long would it take for the public to be notified?*
11. *Have you arranged to make RMP documents available in a public library or other location with ready public access?*

**CONCLUSION**

The NJ Work Environment Council and the NJ Environmental Federation have worked for many years to strengthen right-to-know laws providing citizens and workers access to information about hazardous chemicals used at work and in the community. We have built a statewide coalition of workers, citizens, scientists, and lawyers to monitor these problems. We believe it is in the interest of everyone in New Jersey to ensure that the facilities within the state that use extraordinarily hazardous chemicals—especially those covered by the TCEA and the Clean Air Act—are prepared for potential Y2K computer problems and make every effort to provide information to the public. Given the complex and costly nature of this preventive work, the DEP must also play a more prominent role than it has to date. Y2K poses a daunting challenge, but it also offers an important opportunity for government and business to work in cooperation with citizens, workers and emergency responders to avert potentially dangerous chemical releases that can damage human health and our environment.

Thank you for the opportunity to testify.

---

RESPONSES OF JANE NOGAKI TO QUESTIONS SUBMITTED BY  
CHAIRMAN BENNETT

*Question 1.* In your statement, you criticize the New Jersey Department of Environmental Protection (DEP) for its failure to address critical Y2K issues in the chemical industry. What factors do you believe contributed to the DEP's lack of en-

---

<sup>1</sup> Under the U.S. Environmental Protection Agency's Risk Management Program and U.S. Occupational Safety and Health Act's Process Safety Management program, certain facilities are required to develop and implement risk management programs (RMPs) by June 1999. Under the RMP initiative, regulated facilities are required to conduct a hazard assessment, develop and implement a prevention program, and implement an emergency response program. The hazard assessment includes development of worst-case and alternative release scenarios for a number of highly toxic chemicals as well as compilation of 5-year accident history.

gagement on this issue? In your opinion, what should be done to get the DEP more proactive in this area?

Answer. Since the Committee's May 10 field hearing in Trenton, the DEP itself has responded to our criticisms. It is clear from the agency's response that it has defined its role in an extremely limited manner. Specifically, DEP appears to see itself as an enforcement agency that will inspect and cite employers after an incident occurs, but with no responsibility for a preventive Y2K strategy beyond the deterrent value of its inspection program. Our testimony maintained that the DEP appears to have its "head in the sand" regarding Y2K issues. It now appears the agency's heels are also dug in. Clearly, Governor Whitman should step in and direct the agency to undertake a more aggressive Y2K effort that would include:

- a survey of Y2K compliance efforts of facilities using extraordinarily hazardous chemicals;
- inspections and penalties for facilities failing to respond to such a survey;
- independent audits of the Y2K compliance efforts of a limited number of facilities;
- production of a report on the results of the survey and audits; and
- a series of local hearings—involving workers, citizens and facility managers—on the Y2K issue.

As we made clear in our statement, resources should be allocated for this effort, including additional DEP staff, if necessary.

It should be noted that since issuing our proposals to the Governor and testifying before the Special Committee, WEC has conducted its own 34-question survey of 160 facilities using extraordinarily hazardous chemicals. Responses are currently being analyzed.

*Question 2.* What specific concerns have your members voiced, from the workers' perspective, regarding the safety hazards Y2K presents to them as they carry out their duties each day?

Answer. Unfortunately, it appears that not enough workers on the shop floor are aware of the increased accident risks related to Y2K computer mishaps. The reasons for this are many, but include:

- a lack of urgency on the part of our state government to disseminate information regarding possible threats to workplace, environmental and public safety or to initiate any preventive programs beyond the deterrent impact of existing enforcement strategies;
- a perception, promoted by many large chemical corporations and bolstered by a variety of local, state and federal government officials, that they are adequately and responsibly addressing problems when, in fact, preparation by even the largest companies (e.g. Occidental Chemical) appears to have a long way to go;
- the grim reality that workers toiling in toxic jobs have to endure an ongoing, everyday threat to their health and safety and thus may be inured to any additional hazards posed by Y2K computer problems.

That said, those workers aware of Y2K problems have raised a number of concerns. For example, many are worried about re-starting operations that have shut down safely and about multiple and simultaneous process failures. Workers know that companies have "fail safe" systems in place that will safely shut down a process if, for example, there is a power interruption. But a real danger may emerge if a series of failures occur simultaneously or when systems that have "failed safe" are starting up again. The Y2K issue; these workers say, raises the following "systems of safety" questions:

- Have companies conducted Process Hazard Analysis (PHA) as required by OSHA's Process Safety Management Standard?
- Have facilities conducted a specific Y2K PHA on all their processes?
- Do facilities have adequate staffing to not only run the process but to handle emergency shutdowns?

Many safety committee members in chemical facilities are also aware that PHA's are too often ignored, conducted inadequately, or conducted but not utilized. Since downsizing is widespread in the chemical industry, many facilities are also woefully understaffed. Informed workers contend that these factors combine to create a prescription for Y2K problems. Indeed, a recent example of a Y2K-like scenario is the explosion that killed six workers in Anacortes Washington on November 25. A power failure caused the plant to shut down, which occurred without incident. But management rushed to start up once the power came on, did not fully safeguard systems, and six workers died. The Seattle Times reported that the explosion occurred when a pocket of hot liquid fuel was exposed to air after workers unsealed the bottom of a large steel "coker" drum. "Though workers followed safety precautions," the newspaper reported, "the hot fuel was not detected by temperature indicators be-

cause it had been insulated by a cool crust of residue that formed after a power failure the day before.”

*Question 3.* You mention in your statement that New Jersey’s Toxic Catastrophe Prevention Act (TCPA) has been very effective, but at the same time you are highly critical of the DEP regarding its Y2K efforts. How do you rectify these seemingly contradictory viewpoints? To what extent, if any, has the TCPA contributed to an effective response to Y2K in the chemical industry?

Answer. TCPA has indeed been an effective enforcement program. But the DEP has not extended the TCPA’s reach to encompass broader preventive efforts—such as public or worker education—regarding Y2K or, for that matter, chemical safety in general. Thus, TCPA’s ability to push a facility to address specific problems related to Y2K—e.g. disruptions among vendors—is negligible.

*Question 4.* How would you gauge the effectiveness of Environmental Protection Agency and OSHA efforts on Y2K in the chemical industry?

Answer. OSHA’s effort, as noted by Senator Bennett at the May 10 hearing in Trenton, has been meager at best. The EPA has provided more information, but, according to our members, has yet to have any real impact either with workers inside facilities or with neighbors outside.

*Question 5.* In the list of questions for chemical facilities that you provided in your statement, you alluded to the fact that Risk Management Plans should be readily available to the general public. The EPA initially wanted to make these available on the Internet, but decided not to do so because of security concerns expressed by the FBI in regard to the increased vulnerability to terrorism such widespread dissemination of this information might cause. What is your opinion about this?

Answer. Worst case scenarios included in the Risk Management Plans were intended for use by the public to help communities prepare for and prevent chemical accidents. We feel that denying or limiting access to this information based on purported threats of terrorism would be ill-conceived. The public’s right to know would be reduced by these measures, but chemical facilities would not be required to take steps to improve site security, to establish buffer zones, or to make chemical plants safer. We see no reason to pit community right to know against chemical industry complacency in reducing risks to New Jersey communities. Moreover, we see a great value in establishing a national, public RMP data system that would enable citizens to access and analyze RMP information.

---

PREPARED STATEMENT OF GERALD V. POJE

Good afternoon, Mr. Chairman and Senator Lautenberg. I am Gerald V. Poje, Ph.D., one of four members nominated by the President and confirmed by the U.S. Senate to the U.S. Chemical Safety and Hazard Investigation Board (CSB). Our chairman, Dr. Paul L. Hill, the other board members and I thank you for inviting the CSB to testify regarding:

1. The critical findings and recommendations from the CSB’s Year 2000 (Y2K) Technology report,
2. Significant activities that have occurred within the chemical industry to address areas with the greatest Y2K risk,
3. Assessment of the chemical industry’s ability to continue uninterrupted operations in spite of Y2K, and
4. Actions that Congress and others should take to reduce the risks of Y2K failures.

The Chemical Safety Board is an independent federal agency with the mission of ensuring the safety of workers and the public by preventing or minimizing the effects of industrial and commercial chemical incidents. Congress modeled it after the National Transportation Safety Board (NTSB), which investigates aircraft and other transportation accidents for the purpose of improving safety. Like the NTSB, the CSB is a scientific investigatory organization. The CSB is responsible for finding ways to prevent or minimize the effects of chemical accidents at commercial and industrial facilities and in transport. The CSB is not an enforcement or regulatory body. Additionally, the CSB conducts research, advise Congress, industry and labor on actions they should take to improve safety, and makes regulatory recommendations to the U.S. Environmental Protection Agency and the U.S. Department of Labor.

I am trained in toxicology and specialize in policies dealing with chemical hazards. I oversee the board’s efforts on reducing risks of accidents associated with Year 2000 computer problems. Let me state clearly, that the CSB views the Y2K issue within the larger evolutionary trend of expanding automation and information technologies in the chemical handling sectors. New technology will continue to pene-

trate the workplace, affecting management, workers, equipment and interrelationships with suppliers, customers, regulators and the surrounding community. How our nation and businesses manage the Y2K problem will provide important lessons for other new technology issues.

Currently, I work with the Intergovernmental Forum on Chemical Safety and the Organization for Economic Cooperation and Development to promote global remediation and contingency planning around Y2K problems.

In February 1999 I also testified before the Senate Environment and Public Works Committee's Subcommittee on Clean Air, Wetlands, Private Property and Nuclear Safety on the Year 2000 Computer Technology Problem And Chemical Safety Issues.

#### **BACKGROUND**

The U.S. Chemical Safety and Hazard Investigation Board, at the request of Senators Bennett and Dodd of the U.S. Senate Special Committee on the Year 2000 Technology Problem, has investigated the issues of chemical safety and the year 2000 computer technology problem. In December 1998, the board convened an expert workshop on Y2K and Chemical Safety involving leaders from industries, equipment vendors, insurance companies, regulatory agencies, research agencies, universities, labor organizations, environmental organizations, trade associations, professional engineering associations, and health and safety organizations. The process of our safety board's efforts could prove to be a useful model for other critical issues associated with the year 2000 technology problem and for further elaboration of the chemical safety issues at hearings and workshops organized at the national, state and local levels.

The board members have reviewed and approved the report which is available via Adobe Acrobat at the Chemical Safety Board's website: <http://www.csb.gov/y2k/y2k01.pdf>.

In developing the report, the Chemical Safety Board was guided by the request of the Senate Special Committee to evaluate:

- the extent of the Year 2000 Problem as it pertains to the automation systems and embedded systems that monitor or control the manufacture of toxic and hazardous chemicals, or safety systems that protect processes,
- the awareness of large, medium, and small companies within the industry of the Year 2000 threat,
- their progress to date in addressing the Year 2000 problem,
- the impact of the Risk Management Plans required in June 1999, and
- the role federal agencies are playing in preventing disasters due to the Year 2000 problem.

In synopsis, the Year 2000 Problem is a significant problem in the chemical manufacturing and handling sector. All enterprises with sufficient awareness, leadership, planning, lead time, financial and human resources are unlikely to experience catastrophic failures and business continuity problems unless their current progress is interrupted or there are massive failures of utilities. Many larger corporate entities fit this profile. The overall situation with small and mid-sized enterprises is indeterminate, but efforts on the Y2K problem appears to be less than appropriate based upon inputs from many experts. While the impact of the Risk Management Plans should be positive, there are no special emphases or even specific mention of Year 2000 technology hazards in either U.S. Environmental Protection Agency (EPA) or Occupational Safety and Health Administration (OSHA) regulations regarding process safety. Federal agencies are aware of and involved in Year 2000 technology and chemical safety issues. However, significant gaps exist, and there do not appear to be specific plans to address these gaps.

#### **Scope of Issues**

The Expert Workshop, as well as the research conducted for our report, concluded that the Year 2000 problem is one of major proportions and has the potential for causing disruption of normal operations and maintenance at the nation's chemical and petroleum facilities. Compliance activities reported to the Chemical Safety Board to date have not found a single failure (embedded microchips or software) which by itself could cause a catastrophic chemical accident. However, it is unclear what the outcome might be from multiple failures, e.g., multiple control system failures, multiple utility failures, or a combination of multiple utility and control system failures. Surveillance of the industrial sector that handles high hazard chemicals is insufficient to draw detailed conclusions applicable to all localities.

One theme upon which experts agree is that failures from Y2K non-compliance at small and mid-sized enterprises is more likely. The reason is a lack of awareness

regarding process safety in general and the Y2K impact in particular, lack of resources, and technical know-how for fixing the problems. Given the time constraints, altering this situation would require a massive effort. The Board has concluded that this effort should focus on: 1. providing easy-to-use tools, 2. promoting accessible resources, and 3. providing attractive incentives for Y2K compliance efforts. Additional efforts should be the focus of an urgent meeting of agencies convened by the Administration.

#### **Facility Issues**

The potential for catastrophic events, at US chemical process plants, stemming from Year 2000 non-compliance, can be divided into three categories: failures in software or embedded microchips within the process plants, external Y2K-related problems (e.g., power outages), and multiple Y2K-related incidents that may strain emergency response organizations. A check list of devices to be assessed for Year 2000 compliance at a chemical plant is identified in Appendix A.

The limited scope of the Y2K Expert Workshop and the research conducted for this study concluded that large multinational companies are, in general, following a well-thought out and well-managed path towards Y2K compliance. These multinational enterprises have, in addition to their Y2K compliance efforts, made contingency plans, including, in some cases, plans to shutdown batch operations for limited periods at the turn of the century.

Particularly in the contingency planning area, the CSB's efforts benefited from the specific presentations by the Occidental Chemical Corporation and the Rohm and Haas Company. The efforts of the Chemical Information Technology Association have culminated in contingency planning guidelines, available at the Chemical Manufacturers Association website <http://www.cmahq.com/cmawebsite.nsf/pages/newsinfo>. I have appended the PowerPoint presentations regarding approaches to managing this issue from two major chemical manufacturers: Appendix B from the OxyChem corporation and Appendix C from the Rohm and Haas company.

While existing disaster recovery plans focus on loss of data centers, facilities, or communications circuits, Year 2000 contingency planning must focus on loss of external services and multiple simultaneous occurrences. With Y2K issues, problems will be more complex and they will happen simultaneously. Unpredictable human behavior will make them worse. The same problem may occur in multiple places, and some problems will ripple into other areas threatening health and safety, individual business continuity and supply chain failures.

The CSB conclusions vis-a-vis large and multinational companies should not be construed to mean that there is no potential for Y2K-related catastrophic events at these facilities. It is possible that some Y2K-impacted components may not have been identified, compliance programs may not achieve 100% completion before critical dates, or multiple failures that may not have been considered may result in accidents.

In addition, the erosion of commodity pricing, merger and acquisition activity and loss of critical Y2K staff through 1999 may create unique threats to successful completion of Y2K projects.

The major control and instrumentation vendors canvassed in our study are involved in an extensive program to provide Y2K compliance for their products. There is, however, reason to believe that some independent control systems integrators may have developed and implemented control systems for which there is little or no documentation of Y2K-related vulnerabilities. In addition, some vendors are no longer in business or not as cooperative as the major control and instrumentation vendors.

#### **Regulations**

EPA's Risk Management Program and OSHA's Process Safety Management program mandated by the Clean Air Act Amendments of 1990 may provide significant benefit in terms of improving overall safety programs, reliability of chemical process plants, emergency response plans, and other programs at regulated and compliant facilities. As a result, the overall capability and readiness of the chemical process industry to deal with and effectively overcome the Y2K threat is likely to be very high. However, it must be pointed out that none of these regulatory programs or activities have any direct relationship with Y2K compliance.

Instituting new regulations to standardize testing or certification is not a reasonable approach for three reasons. First, in the remaining time, it is not possible to develop the mechanism and logistics needed for rulemaking, standard development, and establishment of reporting procedures. Second, implementation of any standardized method or regulation may create penalties and unnecessary complications for many companies that do not fit the selected standard but have already expended

an extensive amount of effort on Y2K compliance. Third, it is critical to minimize overall administrative efforts in order to focus available resources on the remedial efforts within this limited time frame.

#### Other Issues

The existing chemical sector and its system of safety will be tested by Y2K problems. Some aspects are worth noting.

1. The chemical sector and its surveillance systems are quite heterogeneous. For example, the Chemical Manufacturers Association (CMA) has approximately 190 members who represent nearly 90% of the chemical producing capacity in the United States.

CMA developed and implemented a Y2K survey beginning in July 1998 (see, the CMA website (<http://www.cmahq.com/cmawebsite.nfs/pages/newsinfo>). Several associations within the larger Council of Chemical Associations have recently adopted and applied the CMA surveillance tool to their members. Other associations may lack resources to survey their members and/or power to assure their compliance. Many more facilities handling significant amounts of high hazard chemicals may not belong to industrial associations.

The two major regulatory agencies, EPA and OSHA, have not undertaken a surveillance of the Y2K compliance efforts of their regulated community, nor have they funded other entities to do such. Therefore the chemical sector has much less of a coordinated approach than other sectors (see, for example, the North American Electric Reliability Council 3rd report to the Department of Energy, [ftp://ftp.nerc.com/pub/sys/all\\_updl/docs/y2k/4-30-y2k-report-to-doe.pdf](ftp://ftp.nerc.com/pub/sys/all_updl/docs/y2k/4-30-y2k-report-to-doe.pdf)).

2. Independent validation and verification also is heterogeneous in the chemical sector. Many larger corporate chemical companies employ rigorous independent auditing of their facilities for a variety of performance measures, including risk management and Y2K compliance efforts. Many companies are auditing suppliers and customers for Y2K compliance and allowing themselves to become subject to similar audits. Such practices have proven highly valuable in improving quality, promoting confidence in management and business continuity and building trust among the key stakeholders. However, the percentage of facilities handling significant amounts of high hazard chemicals that employ this approach is not known.

Other sectors managing hazardous materials are employing public oversight. The Nuclear Regulatory Commission recently has developed an inspection manual and checklist guidelines for power plant inspectors (see Final NRC Inspection for *Review of Year 2000 (Y2K) Readiness of Computer Systems at Nuclear Power Plants* <http://www.nrc.gov/NRC/Y2K/Audit/TI2515-141.pdf> and a *Y2K Review Checklist* <http://www.nrc.gov/NRC/Y2K/Audit/TI2515-141A.pdf>). Similarly, the Connecticut Department of Public Utility Control is employing an independent auditing firm to oversee Y2K compliance at public utilities (see [http://www.dpuc.state.ct.us/DPUcinfo.nsf/6388afa2e804605f852565f7a66dc559a4ee99b385256705006be862?Open Document](http://www.dpuc.state.ct.us/DPUcinfo.nsf/6388afa2e804605f852565f7a66dc559a4ee99b385256705006be862?Open+Document)).

The role for federal, state, local agencies and private third party auditing of Y2K compliance, through either comprehensive or special emphasis programs, is not specified within the chemical sector.

3. Policymakers likely will become involved if the existing system of surveillance, auditing and technical assistance is proven insufficient to prevent extraordinarily manifest Y2K failures. After the Bhopal, India disaster in December 1984, Congress enacted Title III of the Superfund Amendments and Reauthorization Act (SARA) in 1986. SARA Title III required states to establish state and local emergency planning committees (LEPCs), mandated that facilities must make information on hazardous chemicals available to the public, created basic research programs at universities, and established training programs for workers and emergency responders. Additional catastrophic failures in the United States during 1988 and 1989 prompted the 1990 Clean Air Act Amendments which established: a general duty obligation in regard to process safety, OSHA Process Safety Management (PSM) rule, the EPA Risk Management Program (RMP) Rule, and the formation of the Chemical Safety and Hazard Investigation Board.

If Y2K failures become sufficiently apparent in 1999–2000, policy makers likely will need to consider three major issues: 1. The absence of adequate data regarding Y2K compliance, despite widespread recognition of the problem, deadlines for compliance and consequences, 2. Inadequate application of established principles for managing process safety in facilities, particularly as it relates to automation and information technologies, and 3. Gaps in process safety training, technical assistance, and research, particularly as it applies to small to medium sized facilities and those in low income and minority communities.

### **Priority Issues and Findings**

Special Expert Workshop attendees reached consensus on the importance of four issue areas related to Y2K problems and chemical safety. First, small and medium-size enterprises (SMEs) risks and needs are greater than those of larger corporate entities. Second, existing risk management programs provide a more substantial framework for addressing Y2K related problems. Third, the discontinuity of utilities threatens all chemical handling entities. And fourth, managing Y2K problems will require responsive communication among the stakeholders.

### **Recommendations**

The following recommendations were developed based on input from the workshop attendees and research conducted during the CSB Y2K study.

#### **Executive Administrative Agencies**

- The Administration should promote the development of an information clearing-house. Information such as checklists and lists of devices or equipment susceptible to Y2K failures should be provided specific to industry sectors. A Federal government agency should be a focal point for the clearing-house in coordination with other public and private entities, and thereby shielding organizations that provide Y2K-related information from the threat of lawsuits.

- The President's Council on the Year 2000 should coordinate a contingency planning phase to build public awareness and promote the ability of emergency response infrastructure at the federal, state, and local levels. The U.S. Environmental Protection Agency (EPA) should promote the development of contingency plans to assure capable emergency response and promote communications among facilities, local governmental agencies and the nearby communities should problems arise. Federal initiatives should include the organization of regional conferences focusing on ways to assess risks appropriately and how to prioritize which systems and facilities pose greater risks.

- EPA and the Occupational Safety and Health Administration (OSHA) and other safety organizations should increase Y2K awareness in small and mid-sized enterprises (SMEs).

#### **Facilities**

- All processors that will run through the transition should have plans and sufficient and trained staff on hand to manually take control of the process. Facility managers should be prepared to shut down the process quickly and safely should control problems occur. Manual operations, especially over extended periods of time, may require significant changes in staffing and comprehensive training of managers, operators and other workers.

- Batch processors should consider delaying batches involving hazardous materials that will be in the process as the clocks turn to 2000, and at other sensitive dates, for processes where testing was not done or testing results were inconclusive.

- Chemical workers, emergency responders and local governmental agencies that focus on environmental health and emergency response should be provided with training and tools (e.g., guidelines, checklists, and software) to address Y2K issues.

- Facility managers should phase-in and coordinate shut downs, resulting either intentionally as a safeguard against Y2K-related failures or as a direct result of Y2K failures, and startups with local utilities and agencies, including emergency response agencies and Local Emergency Planning Committees.

#### **Other Sectors**

- Power outages and other utility failures could constitute as much of a threat, or even more so, than internal process plant Y2K-related failures. Thus, utilities and oversight agencies should expend every effort to preserve the integrity of the national power grid system, local power supplies and other appropriate utilities. Chemical facilities individually and aggregately can exacerbate unusual loading patterns and minimum generation condition on the electrical grid. Therefore, contingency plans for utilities and chemical facilities should incorporate specific elements for cross sector communication.

#### **All Stakeholders**

- Communication tools should be developed to improve the status of SMEs and to aid worker and public understanding. While it is critical to develop and implement Y2K compliance programs, it is equally important to inform workers and the public about the extensive work being done, in order to allay fears, avoid panic and promote community contingency planning. This communication can be made through federal agencies, such as EPA, OSHA, and the Chemical Safety and Hazard Investigation Board (CSB), state and local agencies. Other important venues for outreach include: unions, trade and professional organizations, such as the American Institute of Chemical Engineers (AIChE), American Petroleum Institute (API),



American Society of Safety Engineers (ASSE), Chemical Manufacturers Association (CMA), Chlorine Institute, and International Society for Measurement and Control (ISA), and research organizations such as the Mary Kay O'Connor Process Safety Center at Texas A&M University.

**Summary**

In summary, the Year 2000 technology problem is a significant problem in the chemical manufacturing and handling sector, posing unique risks to business continuity and worker and public health and safety. All enterprises with sufficient awareness, leadership, planning, financial and human resources are unlikely to experience catastrophic failures and business continuity problems unless their current progress is interrupted or there are massive failures of utilities. Many larger corporate entities fit this profile. The overall situation with small and mid-sized enterprises is indeterminate, but efforts on the Y2K problem appears to be less than appropriate based upon inputs from many experts. Federal agencies are aware of and involved in Year 2000 technology and chemical safety issues. However, significant gaps exist, and there do not appear to be specific plans to address these gaps.

**APPENDIX A**

**EXAMPLE CHECKLIST OF DEVICES TO BE CHECKED FOR YEAR 2000  
COMPLIANCE FOR AN EXAMPLE CHEMICAL PLANT**

**APPENDIX A**  
**EXAMPLE CHECKLIST OF DEVICES TO BE CHECKED FOR YEAR 2000**  
**COMPLIANCE FOR AN EXAMPLE CHEMICAL PLANT**

COMPONENT (to check for compliance)	Worst Case Failure Effects
<b><u>Embedded Microchips</u></b>	
Controllers Weighers Reactor Charging Temperature Pressure Cleaning Stripper Dryer Centrifuge Storage Video Cameras Still Cameras Alarm Systems Clocks Elevators Phones Answering Machines	In accurate readings resulting in poor conversion  Wrong amounts reacting-poor conversion Poor conversion-explosion Poor conversion-explosion Inaccurate timing-process interruption-release Contamination of product Water contamination of product Poor separation Overflow-release Failure to work Failure to work Failure to work Show incorrect time Failure to work Failure to work Failure to work
<b><u>Software</u></b>	
Main frame, network, desktop, & communication computers  Office computers Purchasing Inventory Distribution Sales Accounting Personnel  Process Computers Control Transportation Quality Control	Data generated errors may result in inaccurate data or system failures  No supplies Excess supplies Will send out incorrect orders Will not be able to keep up with orders Will compute incorrectly Will not be kept up correctly  Explosion-release Buildup of stock Poor quality

**APPENDIX A  
(continued)**

<b>COMPONENT (to check for compliance)</b>	<b>Worst Case Failure Effects</b>
<b><u>Supply Chain</u></b>	
Utilities	
Electricity	Process shut down
Water	Process shut down
Waste	Waste buildup beyond capabilities
Communications	No communication
Raw material suppliers	
Primary feedstock	Process shut down
Initiator-catalyst	Process shut down
Service providers	
Insurance	Extra expenses
Hospitals	No medical care
Vending	No food
Customers	No incoming funds
<b><u>Security</u></b>	
Video cameras	Failure to work
Security lights	Failure to work
Access	
Parking	Failure to work
Building	Failure to work
Room	Failure to work
Alarms	
Fire	Failure to work
Intrusion	Failure to work
Warning	Failure to work
Process	Failure to work

**Note:** The information given in this table is provided as an example only. Checklists like this should be developed on an individual plant-specific basis using criteria and knowledge that are unique to the plant.

## **APPENDIX B**

**PRESENTATION ON YEAR 2000 COMPLIANCE EFFORTS BY OXYCHEM  
GIVEN AT THE EXPERT WORKSHOP CONVENED BY  
THE U.S. CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD AT THE REQUEST  
OF THE SENATE SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM\***

\* Also available as an audio presentation at  
<http://www.chemsafety.gov/1999/news/n9907.htm>

**Occidental Chemical Y2K Program**

Occidental Chemical's Y2K Program Focuses on Five Key Areas:

- Information Technology**
- Control Systems**
- Suppliers**
- Customers**
- Contingency Planning**

**Occidental Chemical Y2K Program**

Each and Every Area of the Y2K Program depends on a process that includes the following steps:

- Inventory**  
...or identification of all the devices, systems or relationships where there is a concern about Y2K failures.
- Investigation**  
...or determining the true likelihood of failure and the impact should a failure occur.
- Remediation**  
...or actions that will correct the Y2K related deficiency or mitigate the impact of a failure.
- Documentation**  
...or creation of information needed to share results and show due diligence.

**Occidental Chemical Y2K Program**

When focusing on Process Plant Safety, the two most important parts of the Y2K Program are:

- IT** → **Control Systems** ...or the process being used to identify and correct the problems associated with microprocessors and programming that is embedded in systems and devices used to monitor and control process plants.
- Suppliers**
- Customers** → **Contingency Planning** ...or the process being used to identify the likely scenarios and make plans to deal with it AND to mitigate possible situations and to ensure ability to respond to them.
- Contingency Planning**

**Occidental Chemical Y2K Program**

Handling Control Systems includes the following elements:

- Inventory**
  - Identify ALL systems and devices including microprocessors and programming.
  - Identify all identified issues according to both "likelihood" of failure and "impact" should a failure occur.
- Investigation**
  - Create a standard methodology for investigating devices - include:
    - Usage by safety - eliminate function items
    - Shared Information - eliminate those modules have turned and confirmed to be compliant or not a Y2K device
    - Vendor Information - eliminate those vendors have turned and confirmed to be compliant or not a Y2K device
    - Physical Inspection - Binary or Digital vs. Analog Signals
    - Details Testing - Algorithm preparation and execution
  - Create Database to Record Results and Share Information
    - Think about and create before starting Database design
    - Don't spend all your time working on the "names to be used"
  - Provide Adequate Technical Support. While not a particularly technically demanding issue, there are some important subtleties about Y2K.
    - Check-cyclic issues
    - Imprecise and non-synchronous
    - Overall process flow - Providing is on the right things.
    - Y2K issues that will not occur in the year 2000 or impending Y2K thinking in everyday functions.

**Occidental Chemical Y2K Program**

Handling Control Systems (continued):

- Inventory**
  - Create a standard methodology to streamline getting things done.
    - Don't try to be comprehensive ... fit the Y2K problem
    - Take position and flow supplied by vendor
    - When a vendor doesn't have a plan ... line up the team earlier
  - This is not the time for annual budget cycles
    - Track modifications to current systems
    - Test other alternatives
- Remediation**
  - Create a minimum standard requirement for documentation
    - Describe What, Why, When, Where
    - Don't duplicate
    - Avoid wilds words in being done

**Occidental Chemical Y2K Program**

Addressing Contingency Planning includes the following elements:

- Preparing for the "Most Likely worst case scenario."
  - What is the likely scenario for IT Systems?
  - What is the likely scenario for Control Systems?
  - What is the likely scenario for suppliers?
  - What is the likely scenario for client-related customers and other customers?
  - What is the likely scenario for the surrounding community?
  - Create a "contingency" scenario. Assume that multiple problems occur simultaneously.
    - Conduct "What-if" exercises
    - Conduct Table Top exercises
- Preparing for Emergency Response.
  - Identify "Unlikely" situations.
  - Identify "Unmanageable" situations.
    - You know where your Roundup year session.
    - What did you talk for granted?
  - Identify recognized situations you have been "Unable to address".
  - Test Emergency Response capacity in addressing situations described above.

Occidental Chemical	Y2K Program
Successful Y2K programs will incorporate the following characteristics:	
<b>Project Management</b> <ul style="list-style-type: none"> <li>- Upon his arrival at the Death Star, when construction was behind, Darth Vader's retreating line was "It's time to get you back on schedule." You'll need a Death Vader.</li> </ul>	
<b>Process Development</b> <ul style="list-style-type: none"> <li>- No one has ever submitted Y2K before ... and it doesn't come naturally. You'll need someone who understands and can anticipate how the process will work in a plant.</li> </ul>	
<b>Process Implementation</b> <ul style="list-style-type: none"> <li>- There have been billions of dollars and millions of man-hours spent on process re-design in the last few years --- go find one that is working or intended. You'll need someone who can get things functioning as designed across a wide variety of sites.</li> </ul>	
<b>Accountability/Ownership</b> <ul style="list-style-type: none"> <li>- Y2K is one of those things most people would like to see just go away ... it won't go away. You'll need to point at someone and say "It's your job." That person will need the resources to do his or her job.</li> <li>- Visual methods of resource allocation will hinder progress. You'll have to decide if you can stand the delay.</li> </ul>	

Occidental Chemical	Y2K Program
Occidental Chemical's Y2K Contingency Program Has Three Main components:	
<b>Contingency Level 1: Continued Safe Operations</b>	
<b>Contingency Level 2: Safe Shut Down</b>	
<b>Contingency Level 3: Emergency Response</b>	

Occidental Chemical	Y2K Program
<b>Contingency Level 1: Continued Safe Operations</b>	
<i>These things necessary to keep the facility operating in a safe and environmentally sound manner...</i>	
Should the Y2K Program Steps fail to prevent a problem, ...	
what pre-planned actions can be taken that would allow the facility to continue operations safely and in an environmentally sound manner?	

Occidental Chemical	Y2K Program
<b>Contingency Level 1: Continued Safe Operations</b>	
<b>Examples</b>	
<ul style="list-style-type: none"> <li>• Minimize finished product inventories and waste/effluent levels to allow as much reaction time as possible to unusual situations</li> <li>• Maximize raw material inventories (within safe limits) in case your supplier fails</li> <li>• If you purchase a small amount of steam, you should consider renting a mobile steam generator for back up should your supplier fail</li> <li>• "Ditto" for air or nitrogen with bottled gas for back up</li> <li>• Consider low tech/cheap walkie-talkies to back up sophisticated communication systems</li> </ul>	

Occidental Chemical	Y2K Program
<b>Contingency Level 1: Continued Safe Operations</b>	
<b>Examples (Cont.)</b>	
<ul style="list-style-type: none"> <li>• Increase operations &amp; craftsman staffing during critical periods to be able to quickly respond to unusual situations</li> <li>• Shut down non essential units; restart them later after critical periods have passed and essential units are running well</li> <li>• Make pre arrangements with trucking firms to handle material if primary transportation modes are not available</li> <li>• Develop a plan to manually control output from variable frequency drive controllers (switch to fixed speed and control volume output via dampers, valves, etc.)</li> <li>• Identify and test manual overrides for security systems</li> </ul>	

Occidental Chemical	Y2K Program
<b>Contingency Level 2: Safe Shut Down</b>	
<i>These things necessary to shut the facility down in a safe and environmentally sound manner...</i>	
Should the Y2K Program Steps fail to prevent a problem, and the Contingency Level 1 plans fail to keep the facility operating safely, ...	
what pre-planned actions can be taken that would allow a safe and environmentally sound shut down of the facility?	

Occidental Chemical	Y2K Program
<b>Contingency Level 2: Safe Shut Down Examples</b>	
<ul style="list-style-type: none"> <li>• Rent portable electrical generators or lights for emergency use</li> <li>• Increase operations &amp; craftsmen staffing during critical periods to monitor and react quickly for shut down purposes</li> <li>• Shut down non essential equipment before critical periods to allow more attention time for shut down of critical systems</li> <li>• Ensure (test) all emergency shut down equipment and safety systems are fully functional before critical periods</li> <li>• Test UPS back up systems to ensure power is supplied to control systems that allow safe shut down</li> </ul>	

Occidental Chemical	Y2K Program
<b>Contingency Level 2: Safe Shut Down Examples (Cont.)</b>	
<ul style="list-style-type: none"> <li>• Consider having a back up low tech. communication system for use in plant if the main system fails</li> <li>• Pre test emergency vent scrubbing systems to eliminate or minimize emissions during shut down</li> <li>• Conduct S/D drills—consider more than one system failure</li> </ul>	

Occidental Chemical	Y2K Program
<b>Contingency Level 3: Emergency Response</b>	
<i>These things necessary for an adequate and proper emergency response to facility incidents...</i>	
<p>Should the Y2K Program Steps fail to prevent a problem, and the Contingency Level 1 plans fail to keep the facility operating safely, and the Contingency Level 2 plans fail to shut the facility down safely, ...</p> <p>what pre planned actions can be taken that would ensure adequate and proper emergency response to facility incidents?</p>	

Occidental Chemical	Y2K Program
<b>Contingency Level 3: Emergency Response Examples</b>	
<ul style="list-style-type: none"> <li>• Consider having the Plant Emergency Response Team on "Active" stand-by</li> <li>• Work with "outside" responders and pre plan a back up communication mechanism and practice a response plan</li> <li>• Develop a system to warn neighbors in case the local emergency warning system fails</li> <li>• Conduct drills considering multiple system failures               <ul style="list-style-type: none"> <li>- Internally</li> <li>- With "outside" response agencies</li> </ul> </li> </ul>	

## APPENDIX C

PRESENTATION ON YEAR 2000 COMPLIANCE EFFORTS BY ROHM AND HAAS  
GIVEN AT THE EXPERT WORKSHOP CONVENED BY  
THE U.S. CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD AT THE REQUEST  
OF THE SENATE SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM\*

\* Also available as an audio presentation  
<http://www.chemsafety.gov/1999/news/n9907.htm>

### Chemical Process Safety and the Year 2000

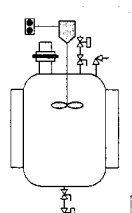
- Basic process control safety
- The implications of Y2K
- Program overview
  - Scope
  - Requirements
- Findings
- A final layer of protection

### The Layers of Protection in a System

- Any physical device can - and will, at some point - fail
- Systems must be designed to withstand failures
- Failure protection is layered:
  - Basic equipment protection
  - Basic control system architecture
  - Fail-safe design
  - Operators and engineers
  - Administrative procedures

*Increasing Robustness*

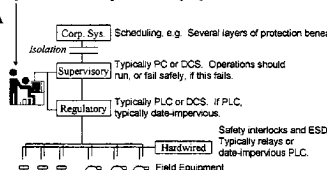
### Basic Equipment Protection Layer



- Local motor control
- Pressure relief devices
- Manual shut-off valves

### Basic Control System Architecture Layer

*Operators are an important line of defense*



Increasing the likelihood of safe dependence

- Corp. Sys. Scheduling, e.g. Several layers of protection beneath.
- Supervisory Typically PC or DCS. Operations should run, or fail safely, if this fails.
- Regulatory Typically PLC or DCS. If PLC, typically date-impervious.
- Hardware Safety interlocks and ESD. Typically relays or date-impervious PLC.
- Field Equipment Typically date-impervious.

### Fail-Safe Design Layer

- Systems are designed to fail safely
- Facilities and control systems are designed to withstand the loss of:
  - Process and control devices
  - Power
  - Water
  - Other utilities
- All systems are subject to formal design reviews:
  - HAZOP
  - Failure modes and effects analysis
- System design emphasizes ability to achieve safe shutdown

### The Implications of Year 2000

- Systems and processes are designed to deal with single failures
- Year 2000 could cause multiple concurrent failures
  - Control failures
  - Utilities
- Safe design and a Year 2000 program provide good protection against multiple control failures
- Greatest exposure is in utility failures



**Rohm and Haas Corporate Policy**

*Rohm and Haas Company is committed to identifying and correcting date-based problems in computer systems (hardware and software), commonly referred to as the "Year 2000 Problem", so that all critical operations continue without disruption.*

*This policy applies to all Company units, world-wide, including subsidiaries, joint ventures, and other related units.*

**Rohm and Haas Scope**

- Business computer systems
- Technical infrastructure
- End-user computing
- Customers and suppliers
- **Manufacturing and warehousing**
- **Environmental**
- Research and development
- Other

**Two Classes of Manufacturing Systems**

- Process control systems
- Other physical systems

- Similar approach for both
- Slightly different requirements for each class
- Both efforts coordinated by same group

**Control Systems Scope**

Computer-based equipment that directly controls the manufacture of chemicals, e.g.:

- Process control computers
  - Distributed control systems
  - Programmable logic controllers
  - PCs
- Purchased equipment containing computers

Pneumatic and electromechanical control is excluded

**Other Physical Systems Scope**

- *Physical plant equipment used in the manufacturing process, e.g.:*
  - Raw material handling systems
  - Equipment monitoring systems
  - Waste treatment systems
- *Physical equipment necessary to ensure uninterrupted operation of the plant, e.g.:*
  - Fire detection and suppression systems
  - Perimeter security systems
  - HVAC systems

**Why the Distinction?  
How We Started**

- Original focus was on control systems
  - Highest degree of risk
  - Strong central understanding
  - Central leverage with key suppliers
  - Consistent approach to critical systems needed
- Intended to let sites manage other physical equipment independently
  - Range of equipment significantly more diverse
  - Most selection and procurement was local

**Physical Systems Added to Central Program**

- Different sites took very different approaches to physical systems
- Some overlap between control and other physical systems became apparent
- Found that there would be benefit in central organization
  - ┆ Better communication and information sharing
  - ┆ More uniform guidelines
  - ┆ Corporate view of status and issues at each site

**Site Requirements: Control Systems**

- Each site is required to build a five-tier safety net:
  - ┆ Obtain vendor certification of **every** control component
  - ┆ Test **every** system - demonstrate ability to produce
  - ┆ Analyze code where critical
- Arrange technical coverage through and beyond midnight
- Be prepared to identify and handle upsets and to shut down safely if necessary

**Site Requirements: Control Systems**

- Submit inventory
- Report testing
- Describe upset handling procedure
- Report remediation requirements
- Site manager's certification that assessment is complete

*Generally complete*

---

- Complete contingency plan
- Complete transition / staffing plan
- Site manager's certification of readiness

*1999 requirements*

**Site Requirements: Other Physical Systems**


- Inventory
- Rank criticality
- Determine appropriate assessment technique(s) for critical items
  - ┆ Vendor certification
  - ┆ Testing
  - ┆ Code analysis
- Determine and implement remediation requirements
- Report all of the above
- Determine approach for less critical items

**Findings: Control Systems**

- **Every** failure found was predicted by the vendor
- Use of dates limited to data acquisition and reporting
- Old control systems require upgrades
- Vendors are generally cooperative
- To date, have found only one catastrophic control system failure


**Findings: Other Physical Systems**

- About 5-7% of physical systems require remediation
- Typically involve PC upgrades
- Have found no catastrophic failures of physical systems
- Many identified failures have straightforward workarounds
  - ┆ Manual reset of date after 1/1/00
  - ┆ Elimination of systems
  - ┆ Manual intervention
  - ┆ "Do nothing" - noncompliance is inconvenient, but acceptable



## A Final Protection Layer

- Most major problems occur while a plant is running
- Shutting down operations through the millennium transition is a prudent precaution, where practical
- Many of our plants are traditionally idle at year-end, and will be for the transition
- Planned shutdown for other sites is under consideration as part of contingency planning



RESPONSES OF GERALD V. POJE TO QUESTIONS SUBMITTED BY  
CHAIRMAN BENNETT

*Question 1.* Your testimony and the CSB report of March has called for the urgent meeting of Federal agencies convened by the Administration on this topic. Would you tell us what you believe the goals and desired outcomes of this meeting should be? Which Federal agencies should be present at a meeting such as this?

Answer. When the CSB convened the expert meeting in December, 1998, the majority of expert participants valued the involvement of a broad diversity of stakeholders, including six Federal agencies representing regulatory, research, training, toxicology, emergency response and investigatory functions. The Federal government commands an important role in providing leadership coordination, and direction on the Y2K issue. Government needs to get pertinent and candid information out to the public, demonstrate that organizations are managing against the problem, establish that normal emergency response mechanisms have been reviewed and updated, and share technical information with those that need it.

No individual agency represents the total mandate of the Federal government, nor engages all relevant stakeholders. While the President's Council has assigned responsibility for the chemical sector to the Environmental Protection Agency, to the best of my knowledge with less than 200 days remaining there is no plan to convene a Federal agency summit meeting on chemical safety.

A Federal Summit on Y2K and chemical safety would:

- a. delineate the extent and depth of surveillance efforts of the chemical handling industry in the private and public sectors;
- b. identify best practice and application of independent validation and verification procedures for assuring compliance efforts;
- c. compile individual agency resources and actions devoted towards assessing and improving Y2K compliance for the chemical handling industry;
- d. identify needs and opportunities for cross-sectoral coordination, training and investigation;
- e. identify best practice for emergency planning and response, including ways of identifying facilities with Y2K failure potential prior to sensitive dates;
- f. discuss the feasibility of the executive branch of the federal government requesting Y2K compliance from high hazard chemical handling facilities;

g. delineate coordination needs and opportunities with state and local agencies on chemical safety.

The outcome of a Federal Summit would be a more coordinated Federal plan of action and communication on chemical safety.

The Federal agencies should include

1. the major regulatory agencies—EPA (OIRM, OSWER, OPPTS, OECA) and OSHA (Office of Compliance, Office of Policy),
2. research, training, and public health agencies—NIOSH, NIEHS, ATSDR,
3. Emergency management—FEMA,
4. agencies with facility management functions that include the management of chemical hazards—DOE, DOD, and
5. independent investigatory and safety agencies—CSB, NTSB.

*Question 2.* Your testimony is guardedly optimistic about the larger firms in this industry. However, the Chemical Manufacturer's Association has been running a Y2K-survey on their almost 200 member firms since December last year and as of the end of April, has only gotten a 63% response rate. Searching the web for information, CMA has gotten data on another 7% or so. Should we not be concerned about the 30% (almost 70 companies) that have not participated in their own association's survey on this important matter? Could you recommend incentives that parties in the government or elsewhere could take to improve the response rate?

Answer. Recognizing the need for greater transparency on safety and environmental programs, more than a decade ago, the Chemical Manufacturers Association told the public, "Don't trust us, track us!" and implemented the Responsible Care<sup>1</sup> code of practices to guide its members. Every participating company's chief officer signs the *Responsible Care*<sup>®</sup> Guiding Principles—the foundation of Responsible Care—as a symbol of his or her commitment to continuous health, safety and environmental performance improvement. Responsible Care<sup>®</sup> is an obligation of membership in CMA. In the Y2K technology problem arena, I urge all to be guided by former President Ronald Reagan who is famous for his international safety aphorism: "Trust but verify."

Yes, we should be concerned about the status of non-reporting companies. Recent surveillance efforts by seven associations of smaller and mid-sized enterprises (SMEs) gathered responses from 300 entities from a total population of more than 3000. Obviously, stated commitments among these companies that they will be 100% Y2K ready by the end of the year is important, and their public disclosure efforts are laudatory although individually anonymous even to their trade association. However, the 10% responders from this SME community does not constitute a random sample of the larger population. Therefore, it is unacceptable to project similar commitments of Y2K compliance before the end of the year for the 90% who did not respond. Furthermore, many other chemical handling entities belong to other associations which have not initiated any surveillance program, and other facilities do not belong to a trade association.

In addition, it is also important to recognize the time sensitivity of information in surveys. At a recent meeting organized by the CMA, one Y2K leader critiqued the accuracy of the CMA aggregate data since his company's current status (which was more complete than originally projected) would not be accurately reflected in their data submitted several months ago. While another company representative anticipating imminent completion of a major merger could not project that the current status would reflect the ultimate status of the company 6 months from now. CMA leaders recently expressed uncertainty that the association would be able to commit resources or garner membership support towards a survey update of their members as has been accomplished in other sectors.

Trade associations which have organized surveillance efforts are to be commended for their voluntary efforts which have increased public awareness and prepared their members for communicating their Y2K compliance status. Hopefully such actions enhance the Y2K compliance of their member. None-the-less, it is important to recognize these associations have limited leverage with their due-paying members to extract Y2K data and maintain its currency. When the survey protocol relies upon voluntary submissions it cannot be expected that all will comply, nor can the compliance results from the responders be projected to the non-responders, such as the 30% of the CMA members and the 90% of the associations of SME chemical specialty producers and distributors.

Legitimate interests of concerned media, investors, workforce and communities will continue to seek information regarding the compliance status and future direction of every company and their specific facilities. The capacity to effectively participate in contingency planning requires that all participants have timely access to rel-

<sup>1</sup> <http://www.cmahq.com/cmawebsite.nsf/pages/responsiblecare>

evant information, sufficient technical understanding and expertise, and the resources to participate.

With approximately 6 months remaining before the end of the year there are limited opportunities to provide incentives. The Federal regulatory agencies should issue a joint communication regarding the applicability of the general duty clauses to Y2K failures affecting health, safety and environmental protection. The CSB has urged organizations with greater technical and financial resources to partner with less resourced entities to improve their compliance status and strengthen their contingency planning efforts. In the private sector this includes large corporations working with smaller suppliers and their customers, such as through an enhanced total product stewardship program. In the public sector this includes federal agencies with facility management competencies, such as DOD and DOE, working with smaller municipalities and businesses in their nearby vicinity. These efforts could increase public awareness of the need for expanding Y2K compliance efforts, contingency planning, and communication of progress, vulnerabilities, uncertainty and management strategies.

The CSB has already stated that instituting new regulations to standardize testing or certification is not a reasonable approach. In the remaining time, it is not possible to develop the mechanism and logistics needed for rulemaking, standard development, establishment of reporting procedures and assuring uniform awareness and compliance. Conversely, there is also little benefit in promoting incentives towards compliance by providing relief from existing regulations because of the same logistical constraints.

*Question 3.* You site lack of knowledge and resources as a potential cause of failures among small and medium sized enterprises, and you say that it would take a "massive" effort to alter this situation. Given the limited amount of time that's left and the dangerous scenario surrounding the fact that literally thousands of these smaller companies are located in the middle of residential communities, what recommendation does the CSB make given this volatile combination? Is there time for a "massive" effort?

Answer. No single entity could be assigned the sole responsibility for assuring SME compliance. Local, state and federal agencies, managers, workers, trade associations, professional associations, community organizations, and others have important roles in promoting health, safety and environmental protection. For example, the Washtenaw County and Ann Arbor, MI Local Emergency Planning Committees (LEPCs) have initiated a laudatory effort to increase awareness and accountability for Y2K compliance among more than 800 businesses handling even small amounts of chemicals in their jurisdiction, and will be organizing community conversations regarding chemical safety concerns. The National Institute of Environmental Health Sciences has increased the Y2K awareness of training experts in the HAZWOPER program and will be providing grant supplements to prepare many more workers and emergency responders (see question 2). The EPA, trade associations representing some chemical SMEs and the CSB have worked together to prepare guidance for SMEs. Industrial unions have sent letters to their locals and employers requesting attention to and information regarding Y2K compliance and contingency planning. Each of these examples should serve as models for others to emulate and thereby reduce the risks.

*Question 4.* My understanding of the chemical manufacturing process is that start-up and shut-down are two very critical and sometimes hazardous points of operation. You indicate in your testimony that power outages and other utility failures could be as threatening as internal system failures. Could you describe for us the risks associated with power outage where normal operations are disrupted, and give us your estimate of the existence of alternative power sources or other contingencies that may be in place within the chemical industry in the event of an electrical or power outage?

Answer. No effort was made in the CSB study to assess the potential of power outages from Y2K-related failures. However, potential Y2K-related power outages represent another set of problems for chemical and petroleum facilities. While many chemical and petroleum manufacturing facilities have backup power generators, Y2K failures may include concurrent loss of power, cooling water and other system malfunctions. High demand processes, such as chloralkali or smelting operations would not be able to operate processes on back-up power generators. Plants without auxiliary power backup systems face a threat to parts of their processes that may not shutdown in a fail-safe mode. Batch chemical processes are especially susceptible because the safety of the process is quite often dependent on time-dependent factors such as precisely timed mixing, heating or cooling requirements.

A potential scenario is that widespread power outages may cause shutdowns of many plants, which in turn will require simultaneous startups. Startups of continu-

ously producing chemical plants are infrequent and their durations are short compared with the life cycle of a plant. Marsh and McLennan in their evaluation of large property damages in the petrochemical industry found that process safety incidents occur five times as often during startup as they do during normal operations. Thus, a large number of simultaneous startups may increase the potential of incidents in one or more process plants. In addition, the simultaneous restarts of large power-consuming facilities will impose large demands on the electrical grid.

While occasional power outages are dangerous and difficult to manage, they are not unusual problems for facility managers and workers to confront. With Y2K power outages, problems will be more complex and they will happen simultaneously such as loss of crucial data, facility subsystems, or communications circuits, as well as loss of other external services and multiple simultaneous occurrences. Unpredictable human behavior will make them worse. The same problem may occur in multiple places, and some problems will ripple into other areas threatening health and safety, individual business continuity and supply chain failures.

Consequently the CSB report recognized that many members of the chemical process industry are concerned about the reliability of power supply and are seeking ways to assess the vulnerability of their specific utility. Individual companies and local associations are encouraged to engage in dialogue with their individual power suppliers to find out what they are doing regarding Y2K. Accurate and pertinent information about utility status is essential for contingency planning purposes.

For some managers of facilities that draw high power loads prudent safety practice may determine that the plant be shut down during critical time periods and restarted at a later date. However, such decisions should not be made without communicating these planned actions with their utilities in order to prevent problems on the power grid. As a further complication, cumulatively, small power consumers can impact on power distribution through the nearly simultaneous shut down of many facilities without coordinating with their utility. Utilities can bring up or shutdown generators as demands vary, but they have trouble responding to unexpected changes in load or demand.

Insufficient electrical demand coupled with increased numbers of generators supplying the electric grid could overload the power distribution system, threaten the integrity of equipment, and/or trip breakers. If that happened, then there could be power outages for all the customers on the affected distribution line. The January 11, 1999 report, "Preparing the Electric Power Systems of North America for Transition to the Year 2000—A Status Report and Work Plan—Fourth Quarter 1998", issued a specific recommendation that would affect any advice given for facilities considering shutting down during rollover to Year 2000.<sup>2</sup>

**"Unusual Loading Patterns and Minimum Generation Conditions.** Another priority concern that is emerging from the contingency planning process stems from the need to have additional generating units on line as a precaution against Y2K events. With additional generators on line and the possibility of customer demand being low through the extended holiday period, utilities must consider what is called a \*minimum generation\* condition. When there is too much generation on line in relation to demand, system voltages and frequency can rise. Planning for the rollover into the Year 2000 must trade off the need to have additional reserves to respond to possible generator contingencies with the potential for excessive voltages. Customers should be encouraged during the period not to take unusual steps such as shutting down facilities that would normally operate through the holiday weekend. Extremely low demand or unusual pattern demand can present additional challenges for operation of the electric system."

The response to the utility problem has to be two-pronged, governmental leadership and corporate accountability. The federal government should ensure the integrity of the nation's electrical grid. In addition, state and local governments should make every effort to ensure the integrity of other utilities within their purview. The chemical process facilities should on the other hand design their Y2K compliance activities, particularly the contingency planning activities with the assumption that most utilities will fail, or at the best be under maximum strain.

The CSB recommends that utilities, individually and through their associations, should take the lead in regards to 1. Informing their customers of possible power supply problems, and 2. Ascertaining whether their customers plan to alter their power demands such that utilities might be unable to maintain power distribution. Where utilities find significant planned shutdowns, they should take the initiative to coordinate shutdowns and subsequent start ups.

<sup>2</sup> See with access through Adobe Acrobat Reader, <ftp://ftp.nerc.com/pub/sys/all—updl/docs/y2k/secondfinalreporttodoe.pdf>

*Question 5.* Besides your Board, OSHA, and EPA, are there other Federal agencies in your opinion that should be active in reaching out to the chemical industries on the Y2K problem? If so can you tell us what their activities have been?

Answer. The CSB has not undertaken a comprehensive surveillance of all Federal agency efforts, and recommends that this activity occur through a Federal summit on chemical safety and Y2K. On a more informal basis, many agencies have shared information with the CSB and have engaged in outreach efforts. For example, the National Institute of Occupational Safety and Health (NIOSH) has developed a website devoted to Y2K. I have reviewed technical papers and informational brochures that NIOSH has prepared to educate occupational health professionals, and the academic centers supported in part through NIOSH have provided a forum for me to address the Y2K issue.

In particular I would like to mention and commend the National Institute of Environmental Health Sciences (NIEHS). NIEHS was given major responsibility for initiating a training grants program under the Superfund Amendments and Reauthorization Act of 1986 (SARA). The primary objective of this program is to fund non-profit organizations with a demonstrated track record of providing occupational safety and health education in developing and delivering high quality training to workers who are involved in handling hazardous waste or in responding to emergency releases of hazardous materials. Since the initiation of the Hazardous Waste Worker Training Program in 1987, the NIEHS has developed a strong network of non-profit organizations that are committed to protecting workers and their communities by delivering high-quality, peer-reviewed safety and health curriculum to target populations of hazardous waste workers and emergency responders.

Since last October NIEHS has organized several major discussions of the Y2K risks in hazardous material management and emergency response. Last month they announced the availability of \$100K competitive, supplemental training grants to their existing grantee community. Applications are due in July and awards will be announced in August. Their clearinghouse, which supports informational exchanges among the grantees and others, will be providing key support for curriculum development in order to accelerate the delivery of training programs. This effort is funded through existing resources, and has not benefited from federal Y2K supplemental funding.

*Question 6.* I understand that the purpose of the Chemical Safety Board is generally to improve the safe production, storage and use of chemicals. I also understand that the CSB is neither a regulatory or compliance organization. I applaud the CSB for proactively taking on the Y2K issue before there are Y2K caused accidents to investigate. Are there any specific actions the CSB can take to assist state and local government organizations obtain information about the Y2K readiness of chemical facilities in their jurisdiction for the purpose of assessing the risk to their communities? Are there realistic actions the Executive Branch or Congress can take to facilitate this happening?

Answer. The CSB views the Y2K issue within the larger evolutionary trend of expanding automation and information technologies in the chemical handling sectors. New technology will continue to penetrate the workplace, affecting staffing, management, workers, equipment and interrelationships with suppliers, customers, regulators and the surrounding community. How our nation and businesses manage the Y2K problem will provide important lessons for other new technology issues.

The Year 2000 technology problem threatens to increase the risks of chemical accidents. The potential for catastrophic events, at US chemical process plants, stemming from Year 2000 non-compliance, can be divided into three categories: failures in software or embedded microchips within the process plants, external Y2K-related problems (e.g., power outages), and multiple Y2K-related incidents that may strain emergency response organizations. Therefore, CSB has been motivated to promote a preventative approach by our research, recommendations and outreach efforts.

The CSB currently is staffed with fewer than 30 people, including administrative and support personnel, and funded for FY 1999 at \$6.5M, much of which has been committed to investigating tragic incidents involving chemicals. None-the-less, the CSB will be mailing copies of our Y2K report to governors, heads of territories, protectorates and the District of Columbia and other leaders with suggestions for distributing to relevant agencies and localities. In addition we will continue to work with EPA and trade associations to develop, promote and distribute guidance document for SMEs. The board will continue to address major audiences, communicate with the press, and work with state and local agencies, trade associations, technical organizations, foundations, organized labor and environmental organizations to promote the highest level of vigilance on safety and the year 2000 technology problem.

The CSB reiterates our request that the executive branch should organize high level summit of executive branch agencies and other agencies (See response to ques-

tion 1.). Additional activities could include training OSHA and EPA compliance officers to understand, assess and communicate the importance of Y2K compliance, and assure a common investigative protocol for assessing Y2K technology problems in the etiology of health, safety and environmental failures.

Congress continues to have an important role through its oversight functions which can promote the mobilization and coordination of appropriate Federal agencies. Congress can enhance occupational and environmental health by assuring that liability avoidance for Y2K failures do not include avoidance of responsibility for health, safety and environmental protection.

As stated in the field hearing testimony, if Y2K failures become sufficiently apparent in 1999–2000, policy makers likely will need to consider three major issues: 1. The absence of adequate data regarding Y2K compliance, despite widespread recognition of the problem, deadlines for compliance and consequences, 2. Inadequate application of established principles for managing process safety in facilities, particularly as it relates to automation and information technologies, and 3. Gaps in process safety training, technical assistance, and research, particularly as it applies to small to medium sized facilities and those in low income and minority communities.

---

PREPARED STATEMENT OF JAMIE SCHLECK

**Introductory Comments**

Chairman Bennett and members of the Committee, my name is Jaime Schleck and I am the Executive Vice President of Jame Fine Chemicals Inc. Thank you for inviting me to appear before you today to discuss an issue important to both industry and the public at large. My role here today is to present the impact of the Y2K computer problem on small business chemical manufacturers, and how these companies can prepare for the millennium change. In my testimony I will explain the unique nature of small chemical companies and how this affects Y2K preparations and contingency planning. I will also describe how Jame Fine Chemicals is preparing for the millennium change and identify existing initiatives that assisted us in our Y2K assessment. Finally, I will address what my trade association, the Synthetic Organic Chemical Manufacturers Association, or "SOCMA," is doing to assist its members with Y2K preparation.

Jame Fine Chemicals is a family owned company comprised of 44 employees. The company manufactures various specialty chemicals for use in five distinct industries: pharmaceuticals, cosmetics, dietary supplements, chemiluminescent products and disinfectants.

Jame Fine Chemicals utilizes batch manufacturing techniques. This manufacturing technique is not exclusive to Jame Fine Chemical, as most small chemical manufacturers use batch techniques.

**Batch Manufacturing**

Batch manufacturing provides an efficient, and frequently the only, method to make small quantities of chemicals to meet specific needs and consumer demands for specialized products. Batch processes are distinct from continuous operations in that a continuous operation has a constant raw material feed to each unit operation and continual product withdrawal from each unit operation. A batch process has an intermittent introduction of frequently changing raw materials into the process, varying process conditions imposed on the process within the same vessel and, consequently, an intermittent release of air emissions. Vessels are often idle while waiting for raw materials, waiting for quality control checks, undergoing cleaning, etc.

Due to the unique characteristics of batch manufacturing, the Y2K issue presents a different rubric of automation assessment and contingency planning. The steps and procedures exercised at Jame Fine Chemicals for Y2K compliance are demonstrative of what I believe most small chemical companies have done or are currently doing.

As a general rule, specialty chemicals are much more expensive than traditional commodity chemicals. One can easily make the analogy that specialty chemicals are to commodity chemicals what diamonds are to coal. On a per kilogram basis, the average specialty chemical manufactured by Jame Fine Chemical could be as much as several hundred times more expensive than the most costly commodity chemical. These economics are common throughout the industry. Consequently, the industry is made up of many smaller companies that focus on specific niche products.

Because of the aforementioned economic factors, it rarely pays to automate a process. In terms of profit optimization, the reduction of labor cost and cycle time through automation has a clearly second order effect when compared to yield management and flexibility. Consequently, the cost structure justifies the need for high-



ly skilled labor and a de-centralized manufacturing process (batch processing). These economic factors also provide a strong incentive for companies such as ours to take the necessary measures to ensure that the Y2K issues do not disrupt production.

#### **Jame Fine Chemicals' Y2K Activities**

My company began its Y2K activity in 1997. Our goal was to be completely aware of any Y2K compliance issues by the beginning of 1999, thus providing us a year to make any necessary changes or refinements. Our plan consisted of several steps including assessment, remediation, validation and contingency planning.

##### *Assessment*

Assessment for Jame Fine Chemicals involved the identification of all potentially affected software, hardware, embedded systems, environmental control systems, and other essential systems. Manufacturing controls at most batch plants are quite different than at continuous flow plants. Unlike continuous systems, most batch operations do not rely on computers for manufacturing. Virtually all of the critical inputs and product flows of batch systems are controlled by a trained process operator—a person—not a computer. Process operators are highly skilled laborers who have responsibility for turning valves, making blends, beginning processes, adding and handling of product and—should the situation arise—activating emergency power shut off switches. As a result, there is no risk of chemical overflow due to automation failures.

Computer automation at Jame Fine Chemicals is used for reaction monitoring systems and quality assurance. These systems ensure that the instruments are functioning properly. It is important to distinguish between production automation and monitoring. At Jame Fine Chemicals, there are no process steps that are taken without the input from a human being. We do use several automated monitoring devices to gather data about a particular process, but we do not have batches that run on autopilot.

The process systems at Jame are typical of most batch manufacturers. There are, however, some companies that may have a higher degree of automation in their manufacturing processes. As a general rule, these companies tend to be more sophisticated and have installed their systems within the last several years. Because the batch control systems that have been programmed and subsequently installed within the last five years are amenable to the millennium change, these systems should not pose Y2K related problems. Of course I can not speak to specific programs and companies other than my own.

One area that firms, such as Jame Fine Chemical, must carefully examine is the delivery of raw materials and in utilities, particularly on dates that have been identified as potentially problematic for computer systems that may have Y2K problems (1/1/00; 2/29/00; 10/10/00; 9/9/99). We have identified those processes that could be adversely effected and have taken steps to ensure that they are not active during critical dates.

##### *Implementation*

Once we identified all of our potential Y2K affected systems, we began contacting our vendors and partners for clarification on their Y2K status. We also began physically testing those systems where possible. In cases where data is gathered by automated machinery, we tried changing the dates to see how the systems would react.

Additionally, as part of our Hazard Operation Procedures (HAZOP), we routinely reviewed all of the possible "what if" scenarios for a given process. Whenever a process is introduced or modified, we have a HAZOP meeting to discuss all of the possible scenarios, and we lay out the plan for addressing each circumstance. This process has identified several Y2K scenarios that are now guarded against.

##### *Contingency Planning*

The last step in Jame Fine Chemicals' review of potential Y2K issue was contingency planning. Our contingency plan includes Y2K specific initiatives as well as emergency preparedness plans drawn from other programs and statutes.

Our Y2K specific efforts include the purchase of extra materials from our suppliers. We feel that it will be important for us to increase our raw material "safety stock" by at least 20 percent for the end of the year. This will give us approximately one month of protection for all possible delays. Our purchase orders for most of these materials have already been placed.

The second part of our Y2K specific contingency plan is to have staff on site and on call for December 31, 1999 and January 1, 2000. Rather than shut down, as we normally do, we are committing the resources to ensure that all of our planning and implementation was done appropriately, and to further prevent or respond to any incidents resulting from on or off site Y2K problems.

The third part of our Y2K specific contingency plan is to ensure that no "utility dependent" or "raw material" dependent processes are effected. For example, no util-

ity dependent processes will be running during any of the critical dates (1/1/00; 9/9/99; 2/29/00; 10/10/00). Additionally, no "raw material" dependent processes will be started unless we are sure that we have the proper materials on hand to prevent the process from being interrupted at a critical phase.

The remaining portions of our contingency plan pertain to emergency preparation and community outreach. Since many of the potential, or feared, impacts of Y2K related problems are potentially catastrophic in nature, efforts to prevent, and planning to enable fast response to remediate such events, are already in place. For example, our company has prepared a Risk Management Plan to comply with the Clean Air Act's soon to be implemented RMP regulation. 40 CFR §68. In this plan, we cover such events as loss of power from our utility provider.

#### *Community Outreach Efforts*

Community outreach efforts are also in place through other programs not specific to Y2K. For example, we have always had a good working relationship with our local fire department, Local Emergency Planning Committee (LEPC) and our community. In fact, on April 20, 1999, we conducted an exercise with our on site emergency response team and local fire department. The borough of Bound Brook, NJ has implemented an information system that provides emergency workers with site diagrams and hazard information for local businesses.

In addition, every manufacturing company that belongs to SOCMA participates in Responsible Care®, and one of the obligations of that program is for companies to have an extensive dialogue with their local communities and rescue personnel. Our company has had open houses and regular meetings with our community where safety issues have been addressed. Our Y2K efforts will be addressed at our next community outreach meeting. Because of Y2K, Jame Fine Chemicals is taking extra steps to ensure the safety of our workers and communities as well as the integrity of our systems and products. Through voluntary initiatives like Responsible Care®, and federal regulations like RMP, the chemical industry is prepared to prevent and/or respond to both on and off site chemical related incidents.

#### *Awareness*

Of course, the first step in implementing a Y2K compatibility plan is awareness. As I stated earlier, Jame Fine Chemicals has been aware of the Y2K issue for several years. Like many other small companies, we received material on the Y2K issue and its potential impact on manufacturing systems from our insurers. The insurance industry has done a great job in spreading the word about potential Y2K challenges to their client companies.

#### **Assistance from Voluntary Programs**

As a chemical manufacturer of pharmaceutical intermediates, we are subject to a wide array of federal and state regulations to ensure safety and environmental protection. In addition to regulation, the chemical industry is also committed to volunteer initiatives that go above and beyond what is required by the government. At Jame Fine Chemical, we found two such initiatives to be quite beneficial to our Y2K efforts. The first is our commitment to the aforementioned Responsible Care® program. Responsible Care® is the industry's self regulating code of management practices that ensure employee health and safety, process safety, community dialogue and other activities. We found that there was a synergy between the operating procedures we regularly perform for Responsible Care® and the systems assessment and community outreach for Y2K compliance. I have included a summary of the Responsible Care® program with my written statement.

In addition to Responsible Care®, Jame Fine Chemical is also cGMP compliant, or more specifically, uses the Food and Drug Administration's (FDA) recommended current Good Manufacturing practices. 21 CFR §210. The purpose of cGMP is to ensure purity and quality of the product manufactured. cGMP calls for controls in every step of the manufacturing process and includes stringent standards of system quality assurance and validation of such systems. If a company is not cGMP compliant, it can not sell chemicals in the U.S. As we progressed in our Y2K activities, we found that our cGMP status was beneficial.

#### **Assistance from Trade Associations**

A great resource for many small companies in the chemical industry is trade association membership. Jame Fine Chemicals is a member of the Synthetic Organic Chemical Manufacturers Association (SOCMA). SOCMA is the leading trade association representing the batch and custom chemical industry. This industry produces over 90 percent of the 50,000 chemicals produced in the U.S. while making a \$60 billion annual contribution to the economy. SOCMA's 300+ member companies are representative of the industry and are typically small businesses with fewer than 75 employees and less than \$40 million in annual sales.

SOCMA has been actively involved with the Y2K issue for quite some time. Over the last couple of years, SOCMA has conducted extensive outreach to apprise its

members of the potential ramifications of Y2K computer issues. Specifically, the association has written numerous articles in its magazine, has had technology experts give presentations at meetings and has dedicated a page on its Internet web site to address the issue and link to numerous sources of information and guidance materials. Most recently, SOCMA has volunteered to work with the Environmental Protection Agency (EPA) to develop a document intended to assist small and medium sized companies with their Y2K assessments and contingency plans.

SOCMA has also participated in a Y2K Readiness Survey in collaboration with six other industry trade groups. The results of the survey show a general awareness and dedication to ensuring Y2K compliance. Eighty-one percent of SOCMA member companies that responded to the survey have Y2K testing initiatives that address health, safety and environmental systems, mission critical functions, and include contingency plans. Of smaller-size companies responding, 84 percent confirmed that they have been working to ensure that their supply chains, which include suppliers, transporters and customers, are Y2K ready. While we cannot say that this is representative of all small companies, we believe that these results demonstrate that many small companies are aware of the Y2K issues and are taking them very seriously.

#### **Conclusion**

Jame Fine Chemicals has dedicated time and resources to ensuring Y2K compliance, thus ensuring the safety of its employees and community neighbors. Our contingency plan involves on site and off site activities and protects our customers from potential shortcomings in the supply chain.

Due to the unique nature of batch manufacturing, the Y2K technology problem does not pose as great a risk in small companies as has been feared. Most batch operations are manually controlled by trained process operators and, as such, do not rely exclusively on automation for manufacturing. Those that are fully automated tend to be newer systems that are already Y2K compliant. In addition, ensuring safety and environmental protection is inherent in the chemical industry through both regulatory and voluntary initiatives. In fact, many of the Y2K related emergency plans have already been implemented as a result of OSHA's Process Safety Management, EPA's upcoming implementation of the Risk Management Planning Rule, and Responsible Care<sup>®</sup>. Our trade association, SOCMA, has done a great job in making companies aware of Y2K and assisting them in their assessments and contingency plans.

In concluding my statement, I would like to make one recommendation to the Committee. We all need to work together and communicate what the Y2K technology problem is and how to address it. In our industry, SOCMA and other chemical trade associations have done a great job in getting the word out to their members and providing assistance. In addition, word has spread to many companies through their insurers, trade press, the general press and from their customers and suppliers. We agree that Y2K issues deserve serious attention and we believe that if we all work together to identify and address potential issues, we will all benefit.

This concludes my statement.

Mr. Chairman, thank you for your invitation to appear before you today. I appreciate yours and the Committee's dedication to this important issue.

I would be glad to entertain questions at this time.

---

## ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

---

American Crop Protection Association  
Chemical Producers & Distributors Association  
Chemical Specialties Manufacturers Association  
International Sanitary Supply Association  
National Association of Chemical Distributors  
RISE (Responsible Industry for a Sound Environment)  
SYNTHETIC ORGANIC CHEMICAL MANUFACTURERS ASSOCIATION

Y2K READINESS DISCLOSURE SURVEY OF  
SMALL AND MID-SIZED CHEMICAL COMPANIES

FOR INCLUSION IN THE COMMITTEE RECORD  
SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM  
UNITED STATES SENATE

JUNE 9, 1999

The American Crop Protection Association (ACPA), Chemical Producers & Distributors Association (CPDA), Chemical Specialties Manufacturers Association (CSMA), International Sanitary Supply Association (ISSA), National Association of Chemical Distributors (NACD), RISE (Responsible Industry for a Sound Environment), and Synthetic Organic Chemical Manufacturers Association (SOCMA) commissioned an independent survey of small and medium-sized entities in the chemical industry to determine their readiness for the Y2K phenomenon. The survey was conducted by Fetzer-Kraus, Inc. of Washington, D.C., to obtain a "snapshot" of where this specialized segment of the chemical industry stands in preparation for Y2K. The survey also was launched to assist the committee, Congress, the administration, and the U.S. Chemical Safety and Hazard Investigation Board (CSB) with obtaining timely and accurate information about the preparedness of this specific segment of chemical manufacturers, formulators, and distributors for the turn of the century and the new millennium. The results of the survey, included in this statement, are based on U.S. companies with individual gross sales of \$75 million or less. In all, more than 300 companies that are mostly small batch chemical manufacturers, formulators, distributors, retailers, or combinations of the above, responded. The survey was conducted from March through May of 1999. The results of this survey of small to medium-sized chemical companies illustrates that they have given and continue to give serious regard for the potential problems of the Y2K issue. These companies have investigated the potential for problems, identified and implemented corrective measures, communicated with communities, and coordinated contingency plans with local emergency response authorities to manage the possibility of single and multiple safeguard failures. The companies were asked to disclose whether or not they had Year 2000 action plans with specific elements. The planning elements and responses are as follows:

## YEAR 2000 ACTION PLAN ELEMENTS

Does your facility plan address the following?

	Yes	No	Not Applicable
Prioritization	93%	3%	4%
Supporting Infrastructure	74%	14%	12%
“Supply Chain” Coordination	82%	13%	5%
Safety, Environmental, and Health Systems	66%	7%	26%
Testing	85%	9%	6%
Internal Communications	79%	12%	9%
External Communications	69%	17%	14%
Contingency Plans	79%	18%	4%

In addition to obtaining a “snapshot” of Y2K compliance for the company sectors, the survey also inquired about the stages of readiness based on planning, inventory/assessment, remediation, validation, Y2K readiness and whether or not the various categories were applicable to their operations. The categories included business information and technology (IT) systems; manufacturing, inventory and distribution IT systems; embedded systems; and the supply chain. The responses are indicated in the following two charts:

## Y2K READINESS STAGES (Part A)

Percentage of SMEs that are Y2K Ready

	Y2K ready	Not Applicable
<b>Business IT Systems</b>	74%	4%
<b>Manufacturing, Inventory, &amp; Distribution IT Systems</b>	67%	14%
<b>Embedded Systems</b>	41%	47%
<b>Supply Chain</b>	47%	12%

#### Y2K READINESS STAGES (Part B)

If not Y2K Ready, percentage of SMEs in each stage of preparedness

	Planning	Inventory/ Assessment	Remediation	Validation
<b>Business IT Systems</b>	17%	8%	50%	25%
<b>Manufacturing, Inventory, &amp; Distribution IT Systems</b>	18%	7%	47%	29%
<b>Embedded Systems</b>	10%	24%	45%	21%
<b>Supply Chain</b>	19%	33%	19%	28%

Additionally, the survey was designed to determine when companies would be ready for the Y2K phenomenon in each of the same categories. The results are as follows:

	Ready*	2 <sup>nd</sup> Quarter-Y2K Ready*3 <sup>rd</sup> Quarter-Y2K Ready*4 <sup>th</sup> Quarter-Y2K	Ready*	Ready*
Business IT Systems	12% - 90%	9% - 99%	1% - 100%	
Manufacturing, Inventory, & Distribution IT Systems	11% - 92%	9% - 100%	-----	
Embedded Systems	5% - 93%	6% - 99%	1% - 100%	
Supply Chain	15% - 74%	19% - 93%	7% - 100%	

*\*The first percentage in each quarter indicates those achieving readiness in the quarter. The second percentage for each quarter represents the percent of companies that already have reached readiness (cumulative for all quarters to that point).*

In addition to co-sponsoring this survey, the associations have continued outreach to member companies and provided requested assistance to solve Y2K problems. Many of the associations' Internet sites provide significant amounts of information about compliance and contingency planning for memberships. Additionally, the trade associations currently are working with the U.S. Environmental Protection Agency (EPA) to develop a document to assist small and medium-sized companies with Y2K assessments and contingency plans.

In March of this year, the committee received a report from the U.S. Chemical Safety and Hazard Investigation Board (CSB). The survey indicated that the CSB report lacked appropriate information from any small and mid-sized enterprises (SMEs). While CSB's report might have proved useful two years ago, its conclusions regarding the readiness of SMEs last March now appear to be based on supposition and not fact. The data from the survey clearly indicates that the small and medium chemical producers have placed considerable emphasis on preparing for Y2K concerns for some time. Additionally, the management of small to medium-sized chemical companies is serious and well-organized with Y2K mitigation and contingency plans.

We believe the Y2K issue should not be given short shrift. It is a concern to our members and we have been responding with due diligence along with them during the past several months. It is our hope and desire that no circumstance will exist that places any member company, community, or persons at a significant risk due to a Y2K-related phenomenon. That is precisely why we have taken prudent and timely steps to avert any possibility of such risks to safety, health, and the environment.

We commend the committee for its work and oversight during the approach of the new millennium. Furthermore, we pledge our support of efforts to maintain productive and accurate communications among government and industry entities to ensure a safe and smooth transition from 1999 to the year 2000.

Organized in 1933, the American Crop Protection Association (ACPA) is the not-for-profit trade organization representing the major manufacturers, formulators and distributors of crop protection and pest control products, including bio-engineered products with crop production and protection characteristics. ACPA member companies produce, sell and distribute virtually all the active compounds used in crop protection chemicals registered for use in the United States.

The Chemical Producers and Distributors Association (CPDA) is a voluntary, non-profit national trade association consisting of nearly 100 member companies engaged in the manufacture, formulation and distribution of agricultural, lawn and garden pesticides as well as their adjuvant and inert ingredients. CPDA's membership accounts for more than \$6 billion worth of chemical-related sales each year.

The Chemical Specialties Manufacturers Association (CSMA) represents several hundred companies—about one-third of which are small businesses—primarily engaged in the formulation and packaging of chemical specialty products. These prod-

ucts include: automotive care products; cleaners and detergents; disinfectants and sanitizers; nonagricultural pesticides; and polishes and floor maintenance products.

With more than 4,400 distributor, wholesaler, manufacturer, manufacturer representative, publisher, and associate member companies, the International Sanitary Supply Association (ISSA) is the leading international trade association for the cleaning and maintenance industry.

The National Association of Chemical Distributors (NACD) is an international association of chemical distributor companies that exists to enhance and communicate the professionalism of the chemical distribution industry. NACD's more than 300 members purchase and take title to chemical products from manufacturers. Member companies process, formulate, blend, repackage, warehouse, transport, and market these chemical products exclusively for an industrial customer base of approximately 750,000. All member companies are committed to product stewardship and responsible distribution in every phase of chemical storage, handling, transportation, and disposal through implementation of the Responsible Distribution Process (RDP), a condition of membership since 1991.

RISE (Responsible Industry for a Sound Economy) is the national association representing the manufacturers, formulators, distributors and other industry leaders involved with pesticide products used in turf, ornamental, pest control, aquatic and terrestrial vegetation management and other non-food/fiber applications.

Synthetic Organic Chemical Manufacturers Association (SOCMA) is the leading trade association representing the batch and custom chemical industry. SOCMA's more than 300 member companies make the products and refine the raw materials that make our standard of living possible. From pharmaceuticals to cosmetics, soaps to plastics and all types of industrial and construction products, SOCMA members make materials that save lives, make our food supply safe and abundant, and enable the manufacture of literally thousands of other products.



## Small &amp; Mid-Sized Chemical Companies Y2K Readiness Disclosure Survey

RESULTS OF THE CHEMICAL INDUSTRY SURVEY ON YEAR 2000 READINESS AMONG  
SMALL & MID-SIZED CHEMICAL COMPANIES

## Y2K Readiness Stage

	NOT APPLICABLE VALIDATION	Y2K READY	PLANNING	INVENTORY/ ASSESSMENT
<b>REMEDIAION</b> Business IT Systems		7 4%	147 74%	8 17%
Manufacturing, Inventory, & Distribution IT Systems		27 14%	133 67%	8 18%
Embedded Systems		95 47%	83 41%	3 10%
Supply Chain		20 12%	80 47%	17 19%

## ESTIMATED Y2K READY DATE

%	Y2K		Y2K	
	2 <sup>ND</sup> QUARTER 99	READY	3 <sup>RD</sup> QUARTER 99	READY
QUARTER 99	READY			4 <sup>TH</sup>
Business IT Systems		24 12%	90%	19 9%
Manufacturing, Inventory, & Distribution IT Systems		21 11%	92%	18 9%
Embedded Systems		10 5%	93%	14 6%
Supply Chain		25 15%	74%	33 19%

## Small &amp; Mid-Sized Chemical Companies Y2K Readiness Disclosure Survey

## Year 2000 Action Plan Elements

YES NO

N/A

Prioritization	218 93%	6 3%	10 4%
Supporting Infrastructure	172 74%	32 14%	29 12%
“Supply Chain” Coordination	191 82%	31 13%	12 5%
Safety, Environmental, & Health Systems	154 66%	17 7%	61 26%
Testing	198 85%	20 9%	14 6%
Internal Communications	186 79%	28 12%	20 9%
External Communications	159 69%	40 17%	32 14%
Contingency Plans	174 79%	39 18%	8 4%

## Small &amp; Mid-Sized Chemical Companies Y2K Readiness Disclosure Survey

**Small & Mid-Sized Chemical Companies: (Defined as gross annual sales <= \$75 Million)**

- Surveying dates: Between March 1999 – May 1999
- Total number of small & mid-sized companies responding: 240 (80% of total respondents)
- Total number of responses received: 301 (not including 56 companies responding in statement form; these  
companies indicated complete or

near-readiness)

- **Types of Operations:**
  - Manufacturers**
  - Formulators**
  - Distributors**
  - Retailers**
  - Combination**
  - Other**
  
- **Participating Chemical Industry Trade Associations:**
  - American Crop Protection Association**
  - Chemical Producers & Distributors Association**
  - Chemical Specialties Manufacturers Association**
  - International Sanitary Supplies Association**
  - National Association of Chemical Distributors**
  - RISE (Responsible Industry for a Sound Environment)**
  - Synthetic Organic Chemical Manufacturers Association**

---

PREPARED STATEMENT OF THE CHEMICAL MANUFACTURERS ASSOCIATION

The Chemical Manufacturers Association (CMA) is pleased to update you on our efforts to assist members of the association and allied trade associations in preparing for a wide range of Y2K challenges. CMA is a nonprofit trade association whose member companies represent more than 90% of the productive capacity of basic industrial chemicals in the United States.

CMA has undertaken an aggressive plan to assist our members. This plan includes:

Development of a customer survey instrument that our members are using to gauge the readiness of their customers and suppliers.

Sponsor workshops and meetings of members and allied trade groups to discuss readiness, contingency plans and community assistance. At our May, 1999 Responsible Care® conference we discussed the need for plants to work with their local communities to share contingency plans and assist the communities in developing local Y2K contingency plans. An additional workshop on Y2K readiness is scheduled for June 10, 1999. This workshop is open to members of allied trade associations.

We sponsor a list server and web site location on Y2K where members and the public can share information and benchmark against other member's practices.

We have conducted a readiness survey of our members to determine their readiness for Y2K. We have provided summaries of the results as information is collected. The latest summary, dated May 12, 1999 is included in these comments for the record.

The readiness survey looks at four areas:

- Business Information Technology Systems
- Manufacturing, Inventory & Distribution IT Systems
- Embedded Systems
- Supply Chain Issues

According to the survey of CMA members, nearly 72% of the respondents who provided dates will be ready by the end of June 1999 and an additional 20% by the end of September 1999. All respondents indicated they would be Y2K ready before the end of the year.

The survey results also indicated the readiness of member companies based on size. The survey results are similar for the four different size categories in the survey. Based on this information we conclude that the small to medium sized firms in our membership are no less Y2K ready than the large firms.

**RESULTS OF THE CMA SURVEY ON CHEMICAL INDUSTRY YEAR 2000 READINESS**

**All respondents:**

Size of company or company's domestic chemical operations (in terms of gross annual revenues) reported in this survey:  
 total Number of responses: 123  
 26 : <\$100 Mn      32 : \$100-500 Mn      19 : \$500Mn-1 Bn      34 : \$1-5 Bn      6 : >\$5 Bn

**Y2K Readiness Stage:**

	NOT APPLICABLE		Y2K READY		PLANNING		INVENTORY/ ASSESSMENT		REMEDATION		VALIDATION		ESTIMATED Y2K READY DATE					
	0	0.00%	26	21.14%	1	0.81%	5	4.07%	51	41.46%	27	21.95%	4th Qtr 98	1st Qtr 99	2nd Qtr 99	3rd Qtr 99	4th Qtr 99	After 2000
Business IT Systems	0	0.00%	26	21.14%	1	0.81%	5	4.07%	51	41.46%	27	21.95%	25	30	45	18	3	0
Manufacturing, Inventory, & Distribution IT Systems	3	2.44%	18	14.63%	2	1.63%	7	5.69%	63	43.09%	28	22.76%	22	22	49	24	1	0
Embedded Systems	5	4.07%	15	12.20%	2	1.63%	26	21.14%	52	42.28%	13	10.57%	12	17	52	27	4	0
Supply Chain	4	3.25%	10	8.13%	4	3.25%	51	41.46%	22	17.89%	21	17.07%	7	22	49	31	6	0
													5.7%	17.9%	39.8%	25.2%	4.9%	0.0%

**Year 2000 Action Plan Elements:**

	Yes	No	N/A
Prioritization	120	1	0
Supporting Infrastructure	117	2	2
"Supply Chain" Coordination	119	0	2
Safety, Environmental and Health Systems	116	0	5
Testing	118	1	2
Internal Communications	106	8	3
External Communications	100	17	3
Contingency Plans	112	8	1

**RESULTS OF THE CMA SURVEY ON CHEMICAL INDUSTRY YEAR 2000 READINESS**

**Big Companies: (Defined as gross annual sales greater than \$1bn)**

Size of company or company's domestic chemical operations (in terms of gross annual revenues) reported in this survey:

Number of responses: 40

34 : \$1-5 Billion 6 : >\$5 Billion

**Y2K Readiness Stage:**

	NOT APPLICABLE		Y2K READY		PLANNING		INVENTORY/ ASSESSMENT		REMEDATION		VALIDATION		ESTIMATED Y2K READY DATE					
	0	0.00%	4	10.00%	0	0.00%	0	0.00%	24	8	4	10.0%	1st Qtr '99	2nd Qtr '99	3rd Qtr '99	4th Qtr '99	After '2000	
Business IT Systems	0	0.00%	4	10.00%	0	0.00%	0	0.00%	24	8	4	10.0%	19	19	5	1	0	0
Manufacturing, Inventory & Distribution IT Systems	0	0.00%	1	2.50%	0	0.00%	3	7.50%	25	6	4	10.0%	19	19	9	0	0	0
Embedded Systems	0	0.00%	2	5.00%	0	0.00%	9	22.50%	23	2	1	2.5%	16	22	9	0	0	0
Supply Chain	0	0.00%	1	2.50%	0	0.00%	19	47.50%	9	6	0	0.0%	8	16	14	1	0	0
	0	0.00%	7	17.50%	0	0.00%	31	77.50%	77	20	0	0.0%	20	40	35	2	0	0

**Year 2000 Action Plan Elements:**

	Yes	No	N/A
Prioritization	40	0	0
Supporting Infrastructure	40	0	0
"Supply Chain" Coordination	40	0	0
Safety, Environmental and Health Systems	40	0	0
Testing	40	0	0
Internal Communications	38	1	0
External Communications	37	2	1
Contingency Plans	38	2	0

**RESULTS OF THE CMA SURVEY ON CHEMICAL INDUSTRY YEAR 2000 READINESS**

**Medium Sized Companies: (Defined as gross annual sales from \$100Mn - \$1 Bn)**

Size of company or company's domestic chemical operations (in terms of gross annual revenues) reported in this survey:

Number of responses: 51

32 :\$100-500Mn 19 :\$500Mn-1Bn

**Y2K Readiness Stage:**

	NOT APPLICABLE		Y2K READY		PLANNING		INVENTORY/ ASSESSMENT		REMEDIATION		VALIDATION		ESTIMATED Y2K READY DATE								
	0	0.00%	9	17.65%	0	0.00%	3	5.88%	20	39.22%	14	27.45%	4th Qtr 98	1st Qtr 99	11	18	10	99	4th Qtr 99	After 2000	
Business IT Systems	0	0.00%	9	17.65%	0	0.00%	3	5.88%	20	39.22%	14	27.45%	21.6%	21.6%	11	18	10	99	2.0%	2.0%	0
Manufacturing, Inventory, & Distribution IT Systems	1	1.96%	8	15.69%	0	0.00%	3	5.88%	20	39.22%	16	31.37%	21.6%	11.8%	6	22	10	99	2.0%	2.0%	0
Embedded Systems	3	5.88%	5	9.80%	0	0.00%	13	25.49%	22	43.14%	6	11.76%	11.8%	9.8%	5	22	12	99	5.9%	5.9%	0
Supply Chain	3	5.88%	5	9.80%	2	3.92%	18	35.29%	11	21.57%	10	19.61%	8.8%	11.8%	5	6	21	13	25.5%	5.9%	0

**Year 2000 Action Plan Elements:**

	Yes	No	N/A
Prioritization	49	1	0
Supporting Infrastructure	50	0	0
"Supply Chain" Coordination	49	0	1
Safety, Environmental and Health Systems	49	0	1
Testing	49	1	0
Internal Communications	46	2	1
External Communications	42	7	1
Contingency Plans	46	4	0

**RESULTS OF THE CMA SURVEY ON CHEMICAL INDUSTRY YEAR 2000 READINESS**

**Small Companies: (Defined as gross annual sales less than \$100 Million)**

Size of company or company's domestic chemical operations (in terms of gross annual revenues) reported in this survey:

Number of responses: 26  
26 : <\$100 Million

**Y2K Readiness Stage:**

	NOT APPLICABLE		Y2K READY		PLANNING		INVENTORY/ ASSESSMENT		REMEDATION		VALIDATION		ESTIMATED Y2K READY DATE					
	0	0.00%	13	40.63%	1	3.13%	2	6.25%	7	21.88%	5	15.63%	4th Qtr 98	1st Qtr 99	2nd Qtr 99	3rd Qtr 99	4th Qtr 99	After 2000
Business IT Systems	0	0.00%	13	40.63%	1	3.13%	2	6.25%	7	21.88%	5	15.63%	8	10	8	3	1	0
Manufacturing, Inventory, & Distribution IT Systems	2	6.25%	9	28.13%	2	6.25%	1	3.13%	8	25.00%	6	18.75%	7	7	8	5	0	0
Embedded Systems	2	6.25%	8	25.00%	2	6.25%	4	12.50%	7	21.88%	5	15.63%	5	6	8	6	1	0
Supply Chain	1	3.13%	4	12.50%	2	6.25%	14	43.75%	2	6.25%	5	15.63%	2	8	12	4	2	0
													6.3%	25.0%	37.5%	12.5%	6.3%	0.0%

**Year 2000 Action Plan Elements:**

	Yes	No	N/A
Prioritization	31	0	0
Supporting Infrastructure	27	2	2
"Supply Chain" Coordination	30	0	1
Safety, Environmental and Health Systems	27	0	4
Testing	29	0	2
Internal Communications	22	5	2
External Communications	21	8	1
Contingency Plans	28	2	1

PREPARED STATEMENT OF THE CHLORINE INSTITUTE, INC.

The Chlorine Institute, Inc. is pleased to provide these comments for the record of the Committee's hearing on the Y2K readiness of the chemical industry in Trenton, New Jersey on May 10, 1999.

The Chlorine Institute, Inc., founded in 1924, is a 235-member, not-for-profit trade association of chlor-alkali producers worldwide, as well as packages, distributors, users, and suppliers. The Institute's mission is the promotion of safety and the protection of human health and the environment in the manufacture, distribution and use of chlorine, sodium hydroxide, potassium hydroxide and sodium hypochlorite, plus the distribution and use of hydrogen chloride. The Institute's North

American Producer members account for more than 98 percent of the total chlorine production capacity of the U.S., Canada, and Mexico.

The Institute has been conducting a readiness survey of its members that produce, repackage and distribute, and use chlorine. (Repackaging chlorine most often involves the transfer of liquified chlorine gas from a 90-ton rail car or pipeline to either 100 lb. or 150 lb. cylinders or one-ton containers.) The survey form is attached to these comments. Earlier results were presented verbally to the staff of the committee. The following data and assessments are based on the survey results to date. The information received is very encouraging as to the Y2K readiness of the members of the Institute.

#### **North American Chlor-Alkali Producers**

The Institute's membership includes 24 North American companies that produce chlorine and its co-products sodium hydroxide or potassium hydroxide (alkalis). Information has been received from 23 companies. Of those, twenty companies responded directly to the Institute and three to the CMA survey. All companies responding indicated they were fully engaged in addressing the Y2K concerns and would be Y2K ready by the end of the year. The results indicate the majority will be Y2K ready in the third-quarter of 1999.

Chlor-alkali production at the vast majority of plants is dependent on electricity supplied by local utilities. Plants have contingency plans to deal with an interruption of power without the loss of containment of the product.

#### **U.S. and Canadian Repackagers of Chlorine**

The Institute's membership includes 21 repackagers of chlorine (19 U.S. and 2 Canadian). Nineteen companies responded to the Institute's survey. All of these members would be considered small (the majority) to medium size companies.

All of the companies responding indicated they would be Y2K ready by year-end. The majority indicated they would be Y2K ready by October 1999.

These companies are the source of chlorine for the vast majority of water and waste water treating facilities using liquified chlorine gas as a disinfectant. Some water utilities receive their chlorine by rail tank cars or tank trucks. The repackaging of liquified chlorine gas does not depend on computer driven or dependent systems. Therefore, there would not be accidental releases of chlorine due to a Y2K problem. Also, as long as the repackaging companies have a source of liquified chlorine gas and electrical power, they will be able to keep the water utilities supplied. Several members have volunteered that they have back up generators to maintain operations should there be an electrical failure. Others are planning to keep their inventories higher than usual so they can supply customer requests for increased quantities of chlorine prior to year-end 1999. Inventory buildup is limited by the number of containers available to fill. The Institute believes that many local or state authorities require utilities to have sufficient chlorine in inventory in case of a disruption of supply.

#### **Chlorine Users**

The Institute has chlorine user members in four categories (by use): general chemical processes, bleach makers, swimming pool applicators, and water utilities. The following are the survey results from general chemical processes and bleach makers.

##### *General Chemical Processes*

Of the 15 Chlorine Institute members in the general chemical processes category, responses were received from nine companies, six directly to the Chlorine Institute and three to CMA. All responders indicated they would be Y2K ready by year end. All the direct responders to the Chlorine Institute indicated they would be Y2K ready by September 1999. The nine responders represent a mix of large (mostly), medium and small companies.

##### *Bleach (Sodium Hypochlorite) Makers*

There are nine Chlorine Institute members in the category of bleach makers. Five companies responded to the survey and all will be Y2K ready by July 1, 1999. These companies receive chlorine and sodium hydroxide and combine the two in a process that results in a water solution of sodium hypochlorite, i.e., bleach. Bleach has many applications, most of which fall into disinfection processes, including water and waste water treatment. With one exception, these members are small (mostly) or medium size companies. Some of the repackaging companies also produce bleach.

As an additional input to the questions of readiness of U.S. bleach makers, a major manufacturer of sodium hypochlorite continuous processing systems was contacted (a member of the Institute) to determine the readiness of their equipment in the field. The company has informed its customers that their equipment is Y2K compliant.

Bleach manufacturers not using continuous processing equipment produce their product in a batch process which involves little or no dependence on computer based process control.



As with the other members mentioned thus far, bleach makers are dependent on an electrical supply for operating their processes. It is anticipated that an interruption of the electrical supply will not result in chlorine or sodium hypochlorite releases. The process of making bleach essentially is one of the methods used to deal with chlorine during a disruption in the chlorine production process.

The Institute does not have sufficient information to generalize on what steps are being taken by bleach makers to ensure a supply of sodium hypochlorite to water utilities, beyond the inventory capabilities of both production sites and user sites. Some producers have indicated that they have stand-by electrical generating capabilities.

### Survey Of Members Y2K Preparedness

Please complete the following simple form and return to Michelle Terry by March 23, 1999 (or sooner).

Please answer each question by checking the appropriate box following each question, and complete the survey by providing the name of the person completing the survey and the identity of the member company.

- Question 1. Have you determined whether your company's chlorine, NaOCl or HCl production, distribution, or using facilities have potential Y2K problems related to safety or environmental protection? (Note: When answering this question, consider not only on-site issues, but potential adverse effects caused by suppliers on customers whose operations may be affected by the Y2K problem.)

Yes       No

- Question 2. If the answer to Question 1 is yes, have you begun an in-depth assessment of your chemical related operations for Y2K problems?

Yes       No

- Question 3. If the answer to Question 2 is yes, when do you expect to complete the assessment?

Completed     January     February     March     April  
 May             June         July         August     September  
 October         November    December

- Question 4. If you have not started working on the Y2K problem, indicate when you intend to begin.

\_\_\_\_\_       Not determined  
(Date)

- Question 5. What is your target date to have all necessary systems in place to address any or all Y2K problems?

\_\_\_\_\_       Not determined  
(Date)

\_\_\_\_\_  
Person Completing Survey and Company

\_\_\_\_\_  
Date

PREPARED STATEMENT OF AUDREY R. GOTSCH, DRPH

The New Jersey/New York Hazardous Materials Worker Training Center has been conducting training for personnel responding to hazardous materials incidents since 1987. The Center based at the Environmental and Occupational Health Sciences Institute, UMDNJ/Rutgers University, has trained over 165,000 people, including over 135,000 directly responsible for reacting to chemical emergencies. This training has enabled emergency personnel to respond appropriately and effectively

when faced with a hazardous materials incident. Preparation, both in the classroom and during simulated emergency situations, is how emergency responders learn to protect the people that live in our communities. They are the essential personnel needed to abate the hazards when faced with catastrophic incidents. As Y2K approaches, communities should be concerned about how much and what types of training are suitable for emergency response personnel.

The significance of Y2K comes as a result of computer chips being designed with only two digits rather than four to specify the year. Time sensitive processing may result in systems shutting down or incorrect calculations being generated in year 2000. Nationally, numerous areas may be affected. Utilities, banks, public hospitals, municipal transit systems and communications systems that link police, fire, and other emergency and security operations are just some of the areas that could be affected. Many of them are evaluating their contingency plans taking into consideration safety, utility continuity, supply reliability and customer needs. However, in the event of emergency situations that may arise from power outages and utility failures, emergency response personnel will be needed to quickly respond.

Y2K issues may effect emergency responders in several ways. They may be limited by power outages, reduced ability to communicate due to failures in telephone, radio, computer systems, and multiple incidents. Failures in public utilities or communications systems will reduce or eliminate ways to call for emergency assistance. However, maybe more importantly, multiple incidents will put enormous pressure on emergency responders, and their resources. Emergency responders will be over extended, mutual aid may not be available, and response to an incident will not occur in a timely manner.

Planning for the potential catastrophic incidents related to the issue of Y2K requires emergency planning and responsive intercommunication. These skills are enhanced through training and education efforts developed to address the challenges of Y2K related issues. Knowledge is key for the emergency response community in order to deal with any casualties that may come. Public agencies and the private sector already support training and education for chemical workers and Hazardous Materials (HAZMAT) emergency responders through programs which can tailor training modules to specific targeted groups of responders at the operations, awareness, technician and specialist levels.

In the chemical and manufacturing industries, the potential exists for a number of disastrous events to stem from Y2K Non-Compliance. First, failures in software or embedded microchips within the process plants may cause process excursions or control problems resulting in accidents. Second, external Y2K-related problems, such as power outages may lead to a variety of problems. For example, rapid shut-downs may result in the triggering of fire suppression systems, causing loss of water pressure for actual fires, and disarming such systems. Third, multiple Y2K-related incidents may exceed the capacity of emergency response organizations to respond.

A fact sheet distributed by the Superfund Labor Health and Safety Task Force, reported that during the five year period between January 1993 through December 1997, OSHA inspected 2,852 facilities with 1,580 citations written for no emergency response plan being available. There were 1,305 citations written for plans not containing all necessary elements and 1,229 citations written for training not addressing emergency planning and coordination. There were 70 inspections at Treatment Storage and Disposal facilities in the last five years resulting in 122 citations being written, 80% involved emergency response training and planning. Consequently, proper training and strategies to implement various guidelines, checklists and software must be provided for emergency responders, local governmental agencies, chemical and manufacturing industries that focus on environmental health and emergency response.

Training issues must be addressed, not just as a one-time effort. We must insure that our emergency response and operations personnel are fully oriented and qualified to implement alternative strategies and operational activities. Only with preparation through comprehensive training will all emergency personnel obtain the critical skills necessary to take appropriate action and prevent an incident before it occurs.

Thank you for the opportunity to share our concern with you.

---

#### Overview of Responsible Care®

Responsible Care® is the chemical industry's initiative for continuously improving health, safety, and environmental quality. Conceived in 1984 by the Canadian Chemical Producers' Association, the initiative was brought to the United States by the Chemical Manufacturers Association (CMA) in 1988 and by SOCMA in 1990.

With more than twenty U.S. Responsible Care® Partner Associations and the spread of Responsible Care® to over 40 countries, it has truly become an industry-wide global initiative.

The following provides an overview of SOCMA's Responsible Care® initiative.

#### **The Responsible Care® Initiative**

Responsible Care® is a continuous improvement initiative built around a set of ten Guiding Principles (see page 2.5) and six Codes of Management Practices (see page 2.6) that put the Guiding Principles into action. The six codes, in order of their implementation are: 1) Community Awareness and Emergency Response (CAER), 2) Process Safety, 3) Employee Health and Safety, 4) Pollution Prevention, 5) Distribution, and 6) Product Stewardship.

Other elements of Responsible Care® include: 1) a self-evaluation process that determines how well companies are applying the Codes which helps evaluate industry performance, 2) mutual assistance, and 3) performance improvement measurements.

Responsible Care® establishes the following value-added goals: 1) improved chemical processes, 2) improved customer relations and service, 3) waste reduction, 4) minimization of accident and incidents, 5) safety handling, transportation, and storage, and 6) increased internal communications and heightened public awareness.

#### **Benefits of Implementing Responsible Care®**

Enhanced environmental, health, and safety performance is the most obvious benefit of implementing Responsible Care®. However, there are other outcomes to the process. Enhanced operating performance is another very beneficial result of implementing the program: it is a value-added investment program.

There is a real input of time, effort, and funds into the start of the process—however, there are measurable financial, as well as operating benefits that can be gained by fully implementing the program. The following are just some of the potential value-added benefits:

- building ties with the local community, government agencies, and other manufacturers,
- reducing the frequency and consequences of worker incidents,
- increasing customer service and satisfaction,
- minimizing disruptions and shutdowns from accidents and worker incidents,
- reducing in worker compensation costs,
- increasing emergency response preparedness, both on and off-site,
- reducing emissions and waste disposal costs, and
- efficient use of labor and equipment resources due to an integrated approach to process design, construction, operation and maintenance.

#### **SOCMA's Participation**

Helping its members to achieve enhanced performance is one of SOCMA's primary goals. The Association has adopted the chemical industry's Responsible Care® initiative as its primary performance improvement program. Using this approach, SOCMA's members have been able to formalize their ongoing, continuous performance improvement efforts.

Since becoming a Partner in Responsible Care® in 1990, SOCMA members have been dedicated to environmental, health, and safety performance improvement. SOCMA's members have voted to require a commitment to the Responsible Care® Guiding Principles and implementation of the six Codes of Management Practices as a condition of Active Membership. (SOCMA's membership category for U.S. chemical manufacturers).

Implementation of the six Codes has been on a phased-in basis according to the following schedule:

CAER.....	1990
Process Safety.....	1993
Employee Health & Safety.....	1996
Pollution Prevention.....	1997
Distribution.....	1998
Product Stewardship.....	1999

Preparing and submitting annual self-evaluations for each Code is a requirement for Active Membership in SOCMA. Copies of each Code self-evaluation are included in this manual for your convenience. The initial self-evaluation for each Code is due in the year following Code activation, and annually thereafter.

#### **Responsible Care® Guiding Principles**

1. To recognize and respond to community concerns about chemicals and our operations.
2. To develop and produce chemicals that can be manufactured, transported, used and disposed of safely.
3. To make health, safety, and environmental considerations a priority in our planning for all existing and new products and processes.

4. To report promptly to officials, employees, customers and the public, information on chemical-related health or environmental hazards and to recommend protective measures.

5. To counsel customers on the safe use, transportation and disposal of chemical products.

6. To operate our plants and facilities in a manner that protects the environment and the health and safety of our employees and the public.

7. To extend knowledge by conducting or supporting research on health, safety, and environmental effects of our products, processes and waste materials.

8. To work with others to resolve problems created by past handling and disposal of hazardous substances.

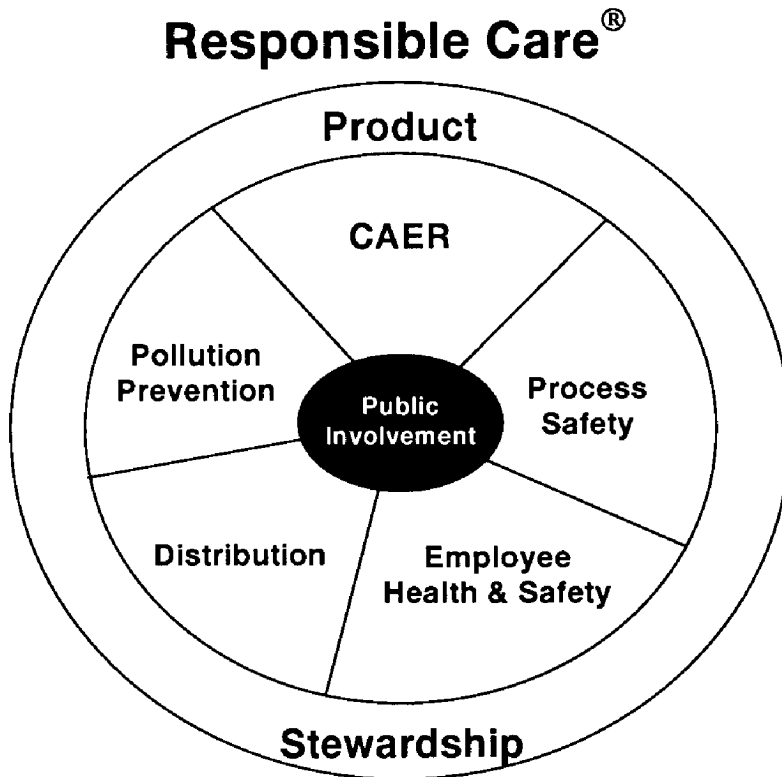
9. To participate with government and others in creating responsible laws, regulations, and standards to safeguard the community, workplace and environment.

10. To promote the principles and practices of Responsible Care<sup>®</sup> by sharing experiences and offering assistance to others who produce, handle, use, transport or dispose of chemicals.

#### The Codes of Management Practices

#### Community Awareness and Emergency Response (CAER)

The CAER Code is intended to foster community awareness and to reduce potential harm to employees and the public in an emergency. Meeting the CAER Code requires a continuing dialogue among facility managers and their plant neighbors, employees, emergency responders, interested groups, teachers, and other individuals and organizations in the community. The Code calls for a continual assessment of public attitudes toward facilities and requires each facility to evaluate its outreach program regularly. Further, companies must share all relevant information with emergency management agencies and other public facilities so that all planning is coordinated. These plans must be tested annually. Companies must also plan to help communities recover from any environmental, health, or safety incidents.



**Process Safety**

The Process Safety Code is designed to help prevent fires, explosions, and accidental chemical releases. Companies must conduct safety reviews of all new and modified facilities before start-up, maintenance and inspection programs must be documented, and layered protection systems must be put in place to prevent equipment failures or human errors from becoming incidents. The Code calls for all employees to be trained in safety practices, and plants are required to share their safety knowledge with other facilities, as well as with the government and the community. It requires input from community officials and organizations, and requires that safety programs include contractor employees.

#### **Employee Health and Safety**

The goal of the Employee Health and Safety Code is to protect and promote the health and safety of people working at or visiting member company work sites. The Code addresses management of occupational health and safety programs, identifying and assessing hazards, maintaining employee health, preventing unsafe acts and conditions, and communicating safe work practices and hazards to employees, contractors, and visitors.

#### **Pollution Prevention**

The Pollution Prevention Code is designed to improve the industry's performance by seeking 1) ongoing, long-term reductions of all pollutants released to the environment; 2) steady reduction in the amount of wastes generated by member companies; and 3) proper management of remaining wastes. There is a high priority given to employee and community input in these processes, using the mechanisms established in the CAER Code. The Code also calls for companies to promote the pollution prevention concepts with customers, suppliers, other companies, and the government.

#### **Distribution**

The objective of the Distribution Code is to reduce employee, environmental, and public risks from the shipment of chemicals. This applies to the storage, handling, transfer, and repackaging of chemicals in transit. The Distribution Code fosters greater cooperation among manufacturers, suppliers, carriers, and customers to prevent incidents and to respond quickly in the case of a transportation emergency. The Code calls for companies to evaluate the risks in the chemical distribution systems and the methods they have in place to minimize those risks; meet or exceed all regulations and industry standards for chemical distribution; and review the performance of employees, distributors, carriers, and contractors to ensure they meet requirements.

#### **Product Stewardship**

The purpose of the Product Stewardship Code is to make health, safety, and environmental protection an integral part of designing, manufacturing, distributing, and using products, and of recycling and disposing waste materials. Implementing the Code will affect nearly every segment of a company, including research and development, manufacturing, distribution, and sales and marketing. The Code mandates the sharing of health, safety, and environmental information about the use, storage, and disposal of products with customers, suppliers, distributors, and contractors.

---

PREPARED STATEMENT OF GEARY W. SIKICH

#### **ABOUT THE AUTHOR:**

Geary W. Sikich is the author of, "It Can't Happen Here: All Hazards Crisis Management Planning", published by PennWell Books. His second book, "Emergency Management Planning Handbook", is published by McGraw Hill. He is a Principal with Logical Management Systems, Corp. (LMS) based in Munster, Indiana. Mr. Sikich has over 20 years experience in management consulting in a variety of fields. He consults on a regular basis with companies worldwide on crisis management issues. As a Senior Executive, Mr. Sikich is experienced in human resource development, strategic planning, competitive intelligence and crisis management planning in diverse industries. A key player in developing business solutions for clients worldwide.

- Designed world class training system; acclaimed, duplicated worldwide.
- Developed & conducted workshops, seminars & conferences worldwide.
- Directed critical infrastructure vulnerability assessments.
- Designed competitive intelligence systems for executive decision-makers.
- Created business continuity management systems for public/private sector clients.
- Guided combined teams to validate numerous clients crisis management programs.

Internationally recognized speaker, writer and conference leader. Publications include two books on crisis management and numerous articles appearing in various print media. Symposium leader for international conferences and workshops; frequently interviewed for television and other media. Results oriented leader adept at increasing revenue, identifying problems, defining solutions and implementing new processes and procedures. A skillful negotiator, communicator, motivator.

**M.A.-Management**, Central Michigan University (**completed courses toward degree**)

**M.Ed.-Counseling and Guidance**, University of Texas; 1981

**B.S.-Criminology**, Indiana State University; 1973

Who's Who in Executives and Professionals 1997-1998

Life Member, Association of Former Intelligence Officers

Member, American Society for Industrial Security

Member, Union League Club of Chicago

Statement of: Geary w. Sikich

Principal

Logical Management Systems, Corp.

**To: US Senate Special Committee on the Year 2000 Technology Problem Background**

At the request of members of the US Senate Special Committee on the Year 2000 Technology Problem, I have prepared the following statement. I specialize in crisis management, business continuity management planning, training and issues analysis for companies and organizations. I have become involved in the assessment of Year 2000 related issues for clients, the preparation of Year 2000 contingency plans and providing advisory services regarding the adequacy of Year 2000 preparedness activities for clients and Year 2000 workshop attendees at conferences that I have been engaged to speak at.

The following is a brief synopsis of recent speaking engagements concerning the Year 2000 issue:

Critical Elements: Year 2000...; East West Corporate Corridor Association, 1998.

How to Prepare Your Year 2000 Crisis Management Team, International Quality & Productivity Center, 1999.

Integrating Contingency Planning into Your Y2K Business Continuity Strategy, Institute for Gas Technology, 1999.

Year 2000 Background and Critical Issues, Institute of Gas Technology, 1999.

Year 2000 Contingency Planning, Institute of Gas Technology, 1999.

Understanding the Y2K Business Continuity Planning Process, International Quality & Productivity Center, 1999.

Business Continuity Plans: Crisis Management for a Smooth Transition into the Next Millennium, International Quality & Productivity Center, 1999.

Auditing Your Year 2000 Contingency Plan, International Quality & Productivity Center, 1999.

Managing the Rollover Weekend, Drilling Your Year 2000 Emergency Management Plan, International Quality & Productivity Center, 1999.

Year 2000 How Will It Work, East West Corporate Corridor Association, 1999.

Managing Crisis at the Speed of Light, Disaster Recovery Journal Conference, 1999.

Critical Elements, Year 2000, The 21st Century... Are You Prepared, The Airport Mobility Network Group, Resource Library, 1999.

All Hazards Crisis Management Planning, Airport Professional, Issue 8, 1999, The Airport Mobility Network Group.

Y2K Expert Testimony: Who will be the Experts, Institute of Gas Technology, 1999.

Crisis Management Planning Guidelines: Y2K, American Society for Industrial Security, 1999.

I have authored "It Can't Happen Here: All Hazards Crisis Management Planning", published by PennWell Books in 1993, "Emergency Management Planning Handbook", published by McGraw Hill in 1995, and now available in a Spanish Language edition, published by McGraw Hill in 1997.

Logical Management Systems, Corp. provides consulting services to clients in the Financial, Energy, Telecommunications, Security, Healthcare, Chemical, Manufacturing, Utilities, Public and Private Sector.

**Objective**

The objective of this Statement for Record is to heighten the awareness of individuals, communities and industries regarding the potential vulnerabilities facing the Chemical industry sector as a result of potential Year 2000 systems failures.

#### **Statement**

I am pleased to present the following statement regarding Year 2000 contingency preparedness issues facing the chemical industry. Portions of this statement have been discussed verbally with members of the Senate Year 2000 Technology Problem Committee staff. This statement summarizes my experiences in dealing with the potential issues faced by the industry in preparing for the Year 2000 transition.

The Chemical Industry has recognized the potential for significant disruption of operations as a result of the Year 2000 date change. Many companies have sought to develop contingency plans and reduce vulnerability to the Year 2000 issues. The plans that have been developed have focused on critical areas such as, potentially affected operations, management/response organization, plan validation, training and documentation.

Having conducted evaluations for clients focusing on regulatory issues, such as, Risk Management Planning, Hazardous Waste Operations and Emergency Response, Oil Pollution Act and other regulatory driven initiatives, I have found that six (6) areas of analysis are of concern with regard to the Year 2000 issue:

1. Organizational Readiness
2. Threat Assessment Review
3. Year Contingency Plan Analysis
4. Documentation and Record-keeping
5. Training and Plan Validation
6. Critical Infrastructure Dependencies

#### **Organizational Readiness**

The involvement of the all levels of management within a company in the Year 2000 contingency planning and emergency preparedness program is essential to its success. To this end many companies are achieving their goal of organizational awareness. Such involvement includes leadership in the development of the program and the direction of program activities.

The methods of demonstrating leadership in Year 2000 contingency planning and emergency preparedness program include, but should not be limited to:

- setting priorities
- developing policy statements
- setting standards
- determining program objectives and direction
- ensuring that safety related issues are a part of the audit and appraisals process
- establishing reporting relationships at the senior management/officer level for the Year 2000 contingency planning and emergency management/response staff
- conducting assessment tours and inspections
- participation in special Year 2000 contingency planning meetings
- reviewing program Year 2000 contingency planning audits
- ensuring that proper involvement and response to recommendations, at all levels within the company
- presenting and attending Year 2000 awareness meetings with all employees to ensure their level of understanding, concerns are heard, addressed and demonstrate commitment to a successful program.

Specific Leadership and Administration issues include:

#### **Year 2000 Contingency Preparedness Policy Development**

A corporate policy statement addressing Year 2000 contingency planning should be developed by all affected entities. This policy should provide a statement of policy regarding Year 2000 contingency planning and the limits of the contingency planning effort. The following is an example of a policy statement that could be used for Year 2000 Contingency Planning.

[COMPANY NAME] Year 2000 Contingency Planning and Management philosophy is based on three precepts: Prevention, Preparedness and Proactive Response. Effective response and management of incidents are essential to [COMPANY NAME]'s business philosophy because we want to minimize the impact of any event on shareholder value. We are committed to this goal through a proactive incident management effort focused on protecting our people, operations and assets.



Response to incidents affecting [COMPANY NAME] operations will be coordinated by the Year 2000 Contingency Management Team supported by Business Continuity Plans, Staff and Technology applications. We will comply with applicable laws and regulations in the implementation of our crisis response and management effort.

#### **Senior and Middle Management Participation**

The level of participation by Senior and Middle Management, is essential for the success of any Year 2000 Contingency preparedness program. One critical aspect to assure the involvement by senior and middle management will be the development of the Year 2000 policy statement and the development and presentation of Year 2000 contingency plan training and awareness materials. It is important to get the "word out" to all levels of management within companies. To this end, the Year 2000 contingency plans and the plan validation programs established by many companies will provide the basis for integrating awareness throughout the companies. Information flyers should also be developed to educate the employees, suppliers and customers on the Year 2000 issues and the activities the company has undertaken to address Year 2000 contingencies.

#### **Management Guidelines**

Management guidelines (protocols) should be developed to assist management implement the Year 2000 contingency plans. In addition, guidelines and protocols for answering customer concerns, media requests and SEC disclosure requirements should also be considered for development.

#### **Management Audits**

Review and approval of the Year 2000 contingency plans and supporting materials is of critical importance to the assuring the ability to respond to Year 2000 identified contingencies. Once the Year 2000 contingency plans have been developed and validated they must be assessed for commitments, evaluated for appropriateness and kept up-to-date. This can be accomplished by reviewing actual responses, through the training and plan validation process (drills and exercises) and by preparing and conducting a detailed audit of the Year 2000 contingency planning system. A suggested evaluation program, outlined below, should be designed to assess the Year 2000 contingency plans and the ability of personnel to complete sequences of critical tasks, under emergency conditions, using available resources as outlined in the Year 2000 contingency plans and associated materials. The audit approach should be based on analysis and evaluation of:

1. Program Administration (Plans and Supporting Materials)
2. Year 2000 Contingency Management/Response Organization
3. Year 2000 Contingency Management/Response Training and Retraining
4. Emergency Facilities and Equipment
5. Plan Implementing Procedures
6. Coordination with External Entities
7. Plan Validation: Drills and Exercises
8. Communications
9. Hazard, Vulnerability, Risk and Issues Evaluation

The ultimate benefits to be gained from implementing the evaluation program are in terms of integrating the Year 2000 contingency planning effort into the day to day operations, related programs (internal/external) and the assurance of adequate management planning and preparedness for the employees and the general public. In order to accomplish this task, a periodic evaluation of all operations should be undertaken. An approach for the audit should generally be to conduct:

##### **1. Personnel Interviews:**

The personnel interviews should consist of answering Year 2000 awareness questions related to the operational area they represent, interviews regarding the knowledge of the extent of potential hazards, general information on emergency preparedness, identification of potentially hazardous situations, record keeping and training.

##### **2. Overview of Written Plans, Policies, Procedures, etc.:**

The overview should consist of a comparison of any written plans, policies, procedures, etc. for consistency with applicable regulatory and non-regulatory guidance.

##### **3. Site/Facility Analysis:**

Site/facility analysis should consist of a periodic walk through assessments of operating locations to accomplish the following:

- A. Identify equipment and processes that could be affected by Year 2000 failures.

B. Identify potential areas of vulnerability (internal/external).

C. Familiarization with the general area conditions.

The ultimate benefits to be gained from this type of evaluation are in terms of identifying areas in need of attention, establishing a list of commitments that have to be met and documenting current efforts. The questions developed for this evaluation program should be assessed on a periodic basis to ensure they are kept up-to-date.

In planning the Year 2000 contingency plan audit, four elements should be taken into consideration:

1. What goals did the Year 2000 contingency program set?
2. What goals did company set for emergency management and response activities?
3. What goals does the Year 2000 contingency audit have?
4. What actions will be taken to resolve Year 2000 contingency audit identified deficiencies?

#### **Year 2000 Reference Library**

Companies should establish a Year 2000 reference library should by formal protocol if necessary. The protocol should define the accepted and approved sources of information for Year 2000 information. A clearinghouse should be established to disseminate Year 2000 information throughout the company. This will reduce the amount of potentially conflicting sources of information and establish a basis for the Year 2000 contingency planning effort. Suggested sources are the Securities and Exchange Commission (SEC). Other sources should be reviewed by management and legal advisors to determine the acceptability and adequacy of the information presented.

#### **Assignment of Responsibility and Planning Efforts**

Responsibility for Year 2000 contingency planning should be assigned to a designated department and/or specific individual. In this way accountability for coordinating the planning effort, continuity of plans and consistency within an organization's planning effort and resultant plans can be assured. This can serve to reduce the potential confusion resulting from the simultaneity of events occurring during the Year 2000 transition period. Year 2000 Contingency Plan operating procedures and emergency related mutual aid agreements should be considered for development to support internal plans.

#### **Threat Assessment Review**

Many companies have developed risk assessment methodologies based upon identification of threats, estimation of the probability of the threat occurring, establishment of forewarning of threat occurrence, determination of the duration of the effect, impact and establishment of preventative measures that can be planned and implemented. This methodology has produced many databases replete with information regarding functions that may be affected, key contacts within the companies and the determination of steps to be taken to diminish the potential impact of the identified threat.

While many companies have produced a valuable tool for assessing internal risk and the determination of potential threats to operations, consideration should be given to developing an assessment of potential scenarios that involve external situations that can impact on the company and its ability to conduct normal business operations.

One threat that has been considered by many companies from an internal perspective is embedded systems. However, the failure of external embedded systems, for example at a wellhead or within a pipeline distribution system, while not controlled by the company could have a significant impact on operations. External factors, that present a potential cascading effect, should be taken into consideration as the Year 2000 contingency plans are developed.

Embedded systems failures can trigger technological disasters which can impede and immobilize efforts to address critical infrastructure disruptions. Infrastructure disruptions in and of themselves be expected to tax emergency response capabilities to the limit. It is estimated that there may be from 10 to 25 billion embedded systems in existence. It is known that some small percentage of these are data sensitive. Of these, a small but significant percentage are not Year 2000 compliant. Estimates range from 0.2% to over 1%. That could mean that from 20 million to 250 million embedded systems failures could occur owing to the Year 2000 related non-compliance problems (source: The Gartner Group).

These include small failures that could have major impacts. Malfunctions could occur in all manner of equipment, devices, appliances and systems found in homes,

hospitals, buildings, plants, facilities and systems. Malfunctions could occur as well in everything from subway systems to water purification plants, waste water disposal plants, oil and gas pipelines, oil refineries, oil tankers, off-shore platforms, chemical plants, manufacturing plants, coal-fired plants, nuclear power plants, hazardous materials storage facilities, laboratories, defense facilities (biological & chemical warfare facilities) and weapons systems of all kinds.

Under Executive Order 13010, certain national infrastructures have been identified and designated as so vital, that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. A report by the President's Commission on Critical Infrastructure Protection (PCCIP), indicates a significant dilemma facing the United States today is the growing interdependence of critical infrastructures. For example, water, sewage and public utilities are commonly found linked together within a city's control system. The report of the PCCIP states in its introduction:

**“The United States is in the midst of a tremendous cultural change—a change that affects every aspect of our lives. The cyber dimension promotes accelerating reliance on our infrastructures and offers access to them from all over the world, blurring traditional boundaries and jurisdictions. National defense is not just about government anymore, and economic security is not just about business. The critical infrastructures are central to our national defense and our economic power, and we must lay the foundations for their future security on a new form of cooperation between the private sector and the federal government.”**

The Critical Infrastructures studied consist of:

- Electric and Gas Power Supplies
- Gas and Oil
- Telecommunications
- Banking and Finance
- Transportation
- Water Supply Systems
- Emergency Services
- Continuity of Government

The Commission divided its work into five “sectors” based on the common characteristics of the included industries. The sectors are:

- Information and Communications
- Banking and Finance
- Energy (Including Electrical Power, Oil and Gas)
- Physical Distribution
- Vital Human Services

Of concern in the assessment of threat issues for companies should be the potential for a government intervention, based on a threat to national security. Under this scenario, a company could have its assets commandeered by the government and be dictated to regarding the distribution of products to users. While this issue is of concern, a strong effort on the industry's part to establish coordination, information exchange and an understanding of expectations, agenda and focus of various entities may serve to assist the industry in the management of this Year 2000 issue.

In addition to the above threat analysis activities companies should determine the time critical, time sensitive and time dependent issues that will affect them during the Year 2000 transition period. Examples are:

<b>Time Critical</b>
<b>0 - 3 Days</b>
Loss of Critical Infrastructures Telecommunications/Information Systems Transportation (air, land, water) Utilities (gas, electric, water) Energy Supply Critical Services Access Denial Degradation/Loss of Critical Operations
Loss/Degradation of Operational Capability Loss of Electrical Supply Sources Loss of Telecommunications/Information Sources Loss/Degradation of Buildings/Occupancy Disruption of Transportation Disruption of Water Supply Disruption of Emergency Services

<b>Time Sensitive</b>	<b>Time Dependent</b>
<b>4 - 7 Days</b>	<b>8+ Days</b>
Finance Vendor/Supplier Business Applications Human Resources & Staffing Legal Oversight/Documentation  Transition to Recovery Organization Recovery Operations Humanitarian Assistance Infrastructure Restoration Information Recovery & Synchronization Resumption of Critical Business Functions Full Function Restoration Permanent Restoration	Government Relations Corporate Relations Corporate Image Banking & Finance  Assigned Relocation Sites Communication Systems Requirements Operations Systems Requirements Personnel Requirements Documentation of Facilities Recovery Assessment of Operations Requirements Building Documents/Records Required in an Emergency Public Sector Contacts Forms and Supplies Associated Plans and Information Insurance and Risk Management Plan Treasury Contingency Cash Plan Controller's System for Tracking Recovery Expenses Vendor/Supplier/Consultant List Floor space Alternatives outside Main Office Records Planning, Storage & Retrieval

Further investigation of external issues relating to Year 2000 threats, risks and issues on the part of the industry is warranted in order to evaluate exposures to external factors that pose a threat to disrupt operations. This can be accomplished through various government organizations and other Year 2000 working groups sponsored by industry.

#### **Year 2000 Contingency Plan Analysis**

An evaluation of Year 2000 contingency plans should be conducted to determine the viability of the documents and the ability of the companies to implement the plans. Assessment should focus on:

- levels of planning for incident response
- integration of incident management and response activities
- life safety issues
- systematic shutdown of facilities
- continuation of vital operations
- identification of emergency use equipment needs
- identification and protection of vital records
- establishment and coordination with organizations and agencies that would provide assistance in the event of an incident
- programs for reentry and recovery of operations

Assess should also consider:

#### **Administration**

How is the Year 2000 contingency preparedness program administered and who is responsible for coordinating the planning efforts.

#### **Year 2000 Contingency Plans and Supporting Information**

What plans have been prepared and how will they be validated. Are the Year 2000 contingency plans integrated with the existing plans established under regulatory agencies guidelines. Plans should establish a standard format so as to ensure the integration of departmental efforts.

#### **Year 2000 Contingency Plan Implementing Procedures**

Year 2000 Contingency Plans should be augmented by the development of supporting procedures to aid in the implementation of the plans. Contingency Plan Implementing Procedures (CPIPs) should contain specific detailed instruction and guidance for response to Year 2000 related contingencies. The CPIPs

should assign responsibilities to personnel, and include flowcharts and checklists where appropriate to improve contingency management and response.

A suggested format and definition of terms is provided below:

**1.0 PURPOSE** - A statement that defines the basic purpose of the procedures, such as: **“This Management Practice provides guidance and instruction for personnel assigned to plant site locations”**.

**2.0 SCOPE** - This section describes the specific issues addressed in the procedure and lists the individuals, by position description, who generally will implement the procedure.

**3.0 REFERENCES** - References to other supporting documents, technical information and other sources of information are listed in this section of the procedure.

**4.0 DEFINITIONS** - With the paucity of acronyms, abbreviations and foreshortened wordings it is advisable to define any new or unusual terminology. This section of the procedure also clarifies any terms as to their meaning.

**5.0 RESPONSIBILITIES** - A listing of responsibilities, general information, initial actions and subsequent actions is provided to assist the individual implement the procedure.

**6.0 PROCEDURE** - This section contains information pertinent to the accomplishment of the function or task prescribed in the procedure.

**7.0 FLOWCHART** - Any supporting flowcharts, diagrams or other pictorial representation of steps in the procedure.

**8.0 APPROVAL** - This section contains the signatures of approval authorities for the procedure.

The Year 2000 Contingency Plans should introduce concepts which are expanded upon and supported by Appendices and Contingency Plan Implementing Procedures. CIPs, however, will be the tools used to implement the plans. They can be grouped into four general categories, as discussed below.

#### **ADMINISTRATIVE CATEGORY**

Administrative procedures consist of management guidelines. These procedures provide guidance and prescribe the manner in which plan maintenance activities such as, monthly calibration tests or communications tests are to be accomplished.

#### **INCIDENT CLASSIFICATION CATEGORY**

Incident Classification CIPs provide step-by-step immediate action procedures for the identification and classification of the severity of an incident, they should:

- Determine the severity of the incident
- Determine the extent of activation of the Emergency Organization
- Determine the notification requirements
- Determine the protective action recommendations to be given to the offsite authorities

#### **INCIDENT MANAGEMENT/RESPONSE ORGANIZATION**

Duties of the individuals assigned to the Incident Management/Response Organization are described in these procedures. Duties of various personnel who play management or response roles in during an incident are delineated in these procedures.

#### **INCIDENT OPERATIONS**

Incident Operations procedures provide guidelines for conducting operations focused on incident mitigation. Step-by-step instructions to direct specific personnel activities during an emergency are presented.

#### **REENTRY & RECOVERY**

Reentry and Recovery procedures include step-by-step task oriented sequences for personnel responsible for business recovery and resumption activities. These procedures assure that appropriate Recovery Organization personnel and equipment are available when reentry and recovery operations commence.

#### **Training and Proficiency Demonstrations (Drills and Exercises)**

Validation of the Year 2000 contingency plans is of critical importance. To this end a program for the training of personnel should be developed, as should a program of plan validation (drills & exercises). The details for the training and validation program should be documented in a separate section of the Year 2000 contingency plans.

**Communications**

Communication protocols should be developed in support of the Year 2000 contingency plans. An assessment of communications interfaces (technology and human) should be accomplished. The critical nature of communications to a company's operations, is readily apparent. The dependency on the telecommunications system to provide operational and administrative support has been recognized by many companies and evaluations of communications dependencies are being undertaken. Backup systems, such as radio and cellular telephones are under investigation. It should be noted that the general proliferation of telephones in the United States for the home, office, voice and data have had an impact on available telephone numbers, that could cause the system to run out of numbers. This remains one of the critical nodes in the Year 2000 contingency planning process. Protocols should be developed for communication activities, such as: incident notification (for internal and external resources), communicating during incidents and alternate communication methods and equipment.

**Emergency Facilities and Equipment**

Many companies maintain a Command Center for incident related operations. An analysis of the adequacy of Command Centers should be accomplished to determine the vulnerability of equipment to Year 2000 failure/degradation. In addition, it is strongly recommended that the Year 2000 contingency plans include options for alternate Command Center locations should the primary Command Center become unusable.

**Coordination with External Groups and Agencies**

It is highly recommended that the companies in the chemical industry become involved in coordination with external groups, companies and governmental agencies to facilitate the Year 2000 expectations of these entities, as well as, determine what support will be available to them in the transition period should Year 2000 incidents cause a degradation of infrastructures critical to the safe operation of the company.

**Public Information**

A critical element of the Year 2000 contingency preparedness program is the education of the public as to the potential impacts of Year 2000 on company operations. Consideration should be given to preparing a public information flyer describing the company's efforts to address the Year 2000 issue.

**Record Keeping**

In order to facilitate Year 2000 contingency planning requirements, a record of all initiatives should be retained. These records will serve to document the accomplishments, requirements, commitments and reports relating to various Year 2000 contingency planning program requirements. The identification of commitments in the areas of Year 2000 compliance requirements, incident preparedness, training and plan validation is important. The establishment of a defined information management and commitment tracking system structure will ensure that documentation will be available when needed.

Senior management must be kept well informed about Year 2000 initiatives. Information must be shared and managed effectively. Information management is also critical during an incident. The need for an interactive system to provide information on materials, personnel, capabilities and processes is essential.

It is advisable to have a system (and adequate back-up systems) in place that serves to identify, catalog, set priorities and track issues and commitments relating to Year 2000 contingency planning commitments, incident management and response activities.

Comprehensive evaluations or audits to verify that the incident management capability, as well as, physical facilities are in compliance with standards prescribed in codes, industry or consensus standards and regulations is necessary. Year 2000 contingency planning activities can be grouped into eleven categories representing the contingency management and response program. A database can be prepared that identifies, tracks and documents commitments within these eleven categories. The following subsections provide a discussion of each of the eleven subject categories in greater detail.

**PLANS:**

All commitments stated in the Year 2000 contingency plans would be listed under this subject category. Commitments that have been identified from project files should also be cited as they apply under this subject category.

**FACILITIES:**

All commitments relating to the Emergency Facilities (Command Center, News Center, etc.) should be cited under this category. Generally, these commitments should be focused upon the design, construction and habitability aspects as well as the incident response functions of each facility.

**EQUIPMENT:**

All commitments regarding emergency use equipment have been input under this subject category. Equipment commitments primarily deal with the stocking, inventory, operability, operability checks, manufacturer information, and the replenishment of expended or expired equipment and supplies.

**COMMUNICATIONS:**

Commitments concerned with communications hardware, lines of communications, notification systems, communications systems tests and system availability are cited in this subject category.

**TRAINING:**

All commitments to provide training for the Incident Management/Response Organization, other identified emergency responders and various offsite response organizations are listed under this heading.

**PROFICIENCY DEMONSTRATIONS: DRILLS/EXERCISES:**

All commitments for drills, exercises, tabletop, scenario development and critiques are presented under this subject heading.

**ORGANIZATION:**

Commitments concerned with the Incident Management/Response Organization, its composition, personnel qualifications and staffing are cited in this category. Additionally, non-company emergency organizations may be represented in this category as well as commitments by the operating subsidiaries that impact these organizations.

**ADMINISTRATION:**

Commitments focusing on the continuity operations and maintenance of the incident management/response capability is provided under this heading.

**PUBLIC INFORMATION:**

The focus of the Public Information category is on the prompt notification, public awareness, public education and news media commitments.

**OFFSITE COORDINATION:**

Commitments made to interface and/or support various response organizations (State, County, Local, Federal and Private) are cited when it was determined that they had a direct impact on emergency management/response capability.

A computerized commitment tracking and information management system, can be designed to monitor the status of Year 2000 contingency planning commitments. The computerized system can provide a user friendly structure which allows the company the ability to track commitments, perform data entry and perform routine database maintenance. Additionally, the commitment tracking system provides a "tickler" that allows for the prompt scheduling and completion of Year 2000 requirements and other periodic commitments.

A suggested database structure would consist of a categorical breakdown of commitments as follows:

*Item No:* A chronological numeric listing of the commitments is maintained in the database file. In this manner, the number of records contained in the database is easily ascertained by the user. Additionally, recurring items have been provided a unique identifier to assist in identification and sorting.

*Responsibility:* Identification of the specific individual responsible for completion of the action item/commitment or the individual with overall authority for ensuring completion of the commitment.

*Com-Date:* Lists the Month, Day, Year that the commitment is anticipated to be completed.

*Status:* Open, Closed or Recurring are used to identify the status of a commitment/action item.

**Training and Plan Validation**

Effective management of an incident requires a high degree of competence in the areas of emergency management and response activities. For the experienced manager, this learning involves the application of fundamental management principals to the recognition, evaluation and control of all incident exposures. For the less ex-



perienced manager, it requires reinforcing and expanding their knowledge of basic management techniques and integrating incident management practices into those techniques. Year 2000 incident management training should provide the knowledge each manager needs to be effective in dealing with the response to Year 2000 related issues, as well as, business resumption issues.

The establishment of a comprehensive Year 2000 contingency plan training program can ensure that all staff receive the requisite training. All personnel and visitors, including those individuals working on a temporary basis or in a training status, should receive an orientation on the Year 2000 Contingency Plans, to orient them of their expected actions and to ensure their safety in the event of an incident.

Suggested training modules may include, but are not limited to:

**Year 2000 Contingency Plan Overview**

This training should be provided to all personnel. The objectives of the training include familiarization of the student with the background for Year 2000 contingency planning, the specific Year 2000 contingency plan, Year 2000 contingency plan activation and implementation; emergency communications skills, record-keeping requirements and an overview of the concept of operations.

**Incident Management/Response Organization**

As appropriate personnel assigned to the Incident Management/Response Organization should be provided training in their assigned functions.

In order to fully assess the effectiveness of the training provided to personnel a program of periodic drills and exercises should be designed and implemented in accordance with the aforementioned Year 2000 policy guidance. The establishment of a comprehensive drill and exercise program can provide a system to effectively evaluate the ability of personnel to implement the Year 2000 contingency plans.

**Conclusion**

The structure of the Year 2000 contingency plan should provide a flexible framework, addressing a variety of situations. It is important that companies in the chemical industry strive to ensure consistency in the development of their plans.

This statement and the recommendations contained herein are provided based on my experience in addressing crisis management, emergency response and business continuity planning issues for a variety of industries. I feel that the observations and recommendations presented herein, serve to summarize my perceptions regarding the current efforts to address contingency planning for the Year 2000. It is the option of industry management to avail themselves of the observations and implement these recommendations as they feel necessary.