United States
Environmental Protection
Agency

Office of Solid Waste
and Emergency Response
(5104)

EPA 550-F-99-003
February 1999
www.epa.gov/ceppo

EPA
CEPP

PREVENT YEAR 2000 CHEMICAL EMERGENCIES

The Environmental Protection Agency (EPA) is issuing this Alert as part of its ongoing effort to protect human health and the environment by preventing chemical accidents. Alerts are issued when EPA becomes aware of a significant hazard. It is important that facilities, State Emergency Response Commissions (SERCs), Local Emergency Planning Committees (LEPCs), emergency responders and others review this information and take appropriate steps to minimize risk. The Alert is targeted at the chemical process industry to increase awareness of the potential for chemical safety problems due to upcoming date changes.

CHEMICAL SAFETY ALERT

THE YEAR 2000 (Y2K) PROBLEM

It is 11:59 p.m. on December 31, 1999. The Year 2000 problem (also known as the "millennium bug") could disrupt your chemical process and storage operations. Is your facility prepared? Here are some examples of what could happen.

- A safety system, designed to detect emissions of deadly hydrogen sulfide gas, shut down during a Y2K test on an oil rig in the North Sea.
- At a smelter in New Zealand, all the process controls stopped working at midnight on December 31, 1996, because programmers had failed to take into account that 1996 was a leap year. The loss of process control damaged equipment valued approximately at $600,000.
- A utility company in Hawaii ran tests on its system to see if it would be affected by the Y2K bug. The entire system shut down.

At any size company, the Y2K issue could threaten worker and community safety and health. It could cause complete shutdowns of machinery or safety-related systems or could generate erroneous information (e.g., wrong temperature) which could lead an operator to take unsafe or improper steps. For chemical process industries, the Y2K problem could increase the potential for process shutdowns and accidental chemical releases.

This alert raises awareness about the Y2K problem and offers a strategy to address the problem. However, given that the Year 2000 is approaching soon, facilities should dedicate increasingly more efforts on developing contingency plans to prepare for unanticipated events like those above. Contingency planning is especially important for facilities that have not started or have made little progress in assessing and remediating the Y2K problem.

In addition to administrative and management systems, (payroll, financial records, inventory), the Y2K problem could affect three parts of your facility - your software, your control/process equipment, and critical services provided to you by others such as utilities and feedstock suppliers.

YOUR SOFTWARE

The Y2K dilemma is the result of a standard practice used in software programming. To save memory space and keep costs down, computer programs and microchips were traditionally designed to recognize only the last two digits of a year. This means that when the year 2000 rolls around, computers may not be able to distinguish whether 00 means 1900 or 2000. This could cause computer programs to crash and systems to shut down. For example, if you rely on computer systems to notify you to schedule maintenance or retire equipment, the system may not properly notify you because the computer cannot recognize dates after December 31, 1999. See the "*Dates to Watch*" box for a few other dates that might cause problems.

Your Control/Process Equipment

Even if your operations do not directly use computers, some of your control machinery, process equipment, automation equipment (e.g., valves, pumps), and emergency protection equipment (e.g., fire and gas detectors), may be embedded with computer chips that are date-sensitive. If these chips misunderstand the date change, the equipment could fail or malfunction, causing process upsets that lead to accidents. For example, an automatic valve with an embedded chip could fail in such a way that the valve turns off the feedstock supply. Because Y2K problems can affect so many devices, cascading failures are possible.

Your Service Providers

The Y2K problem can affect manufacturing, electric utilities and energy suppliers, water utilities, telecommunications, transportation, and other sectors that are critical to your facility operations. Disruption of these services can become your problem. For example, a water supply utility could shut down, causing loss of critical cooling water to chemical reactor systems. Most plants also have suppliers that produce raw and in-process materials that are vital to running their processes. Many plants have customers who accept products through "just-in-time" delivery schedules. Failure to receive these materials could result in safety hazards at your plant.

Hazard Awareness and Reduction

The Y2K concern is real, and the solution may not be easy. However, the effort now to identify and fix the problem will reduce the risk of more costly impacts of business disruptions, safety failures, and accidental chemical releases. While many large companies in the chemical industry already have started addressing the Y2K problem, many small businesses are just beginning to realize the impact that the Y2K problem may have on their operations.

Some Dates to Watch

- ✔ **Sept. 9, 1999**: Many computer systems use 9/9/99 as file purge date
- ✔ **Jan. 1, 2000**: Rollover may halt, confuse, or otherwise disrupt many systems and devices
- ✔ **Feb. 29, 2000**: Many systems may not recognize 2000 as a leap year
- ✔ **Oct. 10, 2000**: First time date field uses maximum length
- ✔ **Dec. 31, 2000**: Some systems may not recognize the 366th day

Steps to Address the Problem

There are several steps you can take to identify and address the Y2K problem. Throughout this step process, you should be sure to document what you have done. For additional help in performing these steps, you could contact an appropriate association, trade group, or industry colleague for particular suggestions and best practices for your industry. If you are unable to implement these steps in-house, consider using an outside consultant. There is also a wealth of information on how to follow these steps (See the "*Information Resources*" at end of Alert).

1. Identify and check systems for Y2K compliancy. Each company should check its systems to determine if they are Y2K compliant. Make a list of the date-dependent components of your systems that are likely to be affected by the "millennium bug." (See box on "*Examples of Equipment to Check*"). Focus on software and equipment with embedded chips, and ask yourself if your equipment or systems use or depend on date information, for example, does the system order/retrieve information by date, or perform date-based calculations? Prioritize the items on your list based on their potential for causing health, safety, and environmental concerns and how critical they are to business production. You should review your risk assessments or hazard analyses (e.g., HAZOP) to be certain that Y2K vulnerable equipment and devices are inventoried and addressed. Starting with the most critical equipment, check with your supplier, installer, or manufacturer to determine if the system component is

Y2K compliant (see section on "Information Resources" for some vendor web sites).

2. Remedy problem. If critical equipment can be affected by the Y2K problem, you have several options including repairing, modifying, or replacing the equipment. Where mission-critical systems cannot be assessed, remediated, and corrected, you could consider operating the system in a manual over-ride mode. Staff would need training on new equipment or refresher training on procedures for manual operation. Additional staff may be needed when automated processes are switched to manual.

3. Test systems. Your systems and equipment should be tested to make sure the Y2K malfunction is remedied. Do not forget to test dates other than January 1, 2000 (see the "Dates to Watch" box). Before you test, alert local emergency officials and make sure your employees and community are prepared for any possible failures that may have an adverse effect on health and safety or the environment. (See EPA's new enforcement policy on Y2K testing in section "*It's Your Duty*").

4. Develop and implement contingency plans. Contingency plans are essential in your strategy to address the Y2K problem. Even if you believe your system is Y2K compliant, you should develop a Y2K contingency plan to prepare for unanticipated problems. Your contingency plan should not depend on backup equipment and systems that could also fail because of the Y2K complication (e.g., backup generator, automatic shutdown system). Also, you may need to address staffing and training for meeting Y2K contingency plans and to handle disruptions to transportation infrastructure and telecommunications. Facilities should not overlook the possibility that non-Y2K compliant computers and chips in telecommunications and radio may prevent police, fire, and mutual aid assistance from arriving promptly or at all. Inform local officials concerned with emergency situations when testing equipment, and involve employees in planning for testing and in responding to unexpected system changes. As part of your contingency planning you could:

- Work with and share solutions and lessons learned with your partners, suppliers, neighbor facilities, associations, and customers to ensure that they, too, are addressing the Y2K issue.

EXAMPLES OF EQUIPMENT TO CHECK

- ✔ Controllers
- ✔ Alarms
- ✔ Lighting
- ✔ Robots
- ✔ Air monitoring/leak detection devices
- ✔ Hazard communication databases
- ✔ Underground storage tank monitors
- ✔ Security systems
- ✔ Generators
- ✔ Lab instruments
- ✔ Environmental control systems
- ✔ Controllers for refrigeration, valves, pumps, sensors and analyzers
- ✔ Programmable control systems
- ✔ Safety shutdown systems
- ✔ Fire detection systems
- ✔ Explosion suppression systems
- ✔ Elevators
- ✔ Conveyors
- ✔ Vehicles

- Work with your SERC, LEPC, and other off-site emergency management support to review emergency response procedures and ensure that the procedures and resources available cover possible Y2K consequences.

- Make sure employees are trained and prepared to shut down the process manually, if necessary.

- Consider scheduling downtime and maintenance over the end of 1999 and beginning of 2000. During shutdowns, systems can be isolated and Y2K tested. However, before you schedule downtime, recognize that startups and shutdowns have their own risks which must be balanced against the potential risks from Y2K problems. Also, if you are a large power user, notify your utility if you plan to have a shutdown. Utilities could have operating problems if power demands unexpectedly drop, particularly if many facilities shut down.

- Have a full staff available for a number of hours just before and after critical date changes for unanticipated emergencies.

- Consider conducting an exercise using a Y2K scenario to improve emergency response capabilities. One community, Lubbock, Texas, already has successfully conducted such an exercise and learned a number of important lessons, including the need to prevent emergency communications failure.

Remember, in terms of contingency planning, facilities should take advantage of the one positive piece of information that the Y2K problem offers us: the ability to know when it will occur.

IT'S YOUR DUTY

Under the General Duty Clause of the Clean Air Act (CAA section 112(r)(1)), owners and operators of facilities with hazardous substances have a general duty to prevent and mitigate accidental releases, including those caused by Y2K failures. Also, under EPA's Risk Management Program (RMP) Rules (CAA section 112(r)(7)), accidental release scenarios related to Y2K problems (e.g., loss of utilities, interruption of raw material deliveries, failure of monitoring devices) would be reasonable alternative scenarios to consider. The public may view any Y2K-related operating problems that occur in January 2000 as a test of the quality and reliability of your RMP. In addition, EPA has initiated an enforcement policy designed to encourage prompt testing of computer-related equipment to ensure that environmental compliance is not impaired by the Y2K computer bug. Under this policy, EPA intends to waive 100% of the civil penalties and recommend against criminal prosecution for environmental violations caused by tests designed to identify and eliminate the Y2K-related malfunctions. This policy is limited and subject to certain conditions. (See complete policy on EPA's Year 2000 web site listed in "*Information Resources*.")

The Occupational Safety and Health Act (OSHA) has a similar General Duty Clause (section 5(a)(1)) for protection of employees from hazardous situations involving the use of highly hazardous substances. Also, OSHA's Process Safety Management (PSM) Standard is intended to prevent or minimize injury to employees from accidents (including those caused by Y2K problems) involving highly hazardous chemicals.

INFORMATION RESOURCES

Below are some resources that will help you to get started to address the Y2K problem at your facility. Future updates of this resource list can be found at the EPA CEPPO Website below.

Environmental Protection Agency (EPA)
Provides information on EPA's efforts to address the Year 2000 problem. This includes EPA's Y2K enforcement policy, and under the heading "Environmental Y2K Sectors," the Office of Water guidance for wastewater systems (including a checklist of basic systems) and the Office of Solid Waste flyer on waste management and the Y2K problem.

http://www.epa.gov/year2000/

EPA's Office of Solid Waste and Emergency Response Y2K information.

http://clu-in.com/y2k.htm

EPA's Chemical Emergency Preparedness and Prevention Office (CEPPO) has this Y2K alert and updates.

http://www.epa.gov/ceppo

Occupational Safety and Health Administration (OSHA)
The OSHA web site has a bulletin on Y2K.

http://www.osha.gov/Y2knews.pdf

Chemical Safety and Hazard Investigation Board (CSB)
The CSB has sponsored a conference and report on the Y2K problem and the potential for accidental chemical releases. Relevant Year 2000 sites can be found on the CSB Web site by clicking on Chem Links and then searching on "Year 2000."

http://www.chemsafety.gov

U.S. Small Business Administration (SBA)
This web site offers information specific to helping small businesses address the Y2K problem. It provides a list of questions to help identify date-sensitive equipment. SBA also has an extensive list of links to major corporations that post their Y2K status online.

http://www.sba.gov/y2k/
Hotline: 1-800-U-ASK-SBA (1-800-827-5722)

General Accounting Office
Guide: "Year 2000 Computing Crisis: Business Continuity and Contingency Planning" has general principles for use by businesses as well as government agencies.

http://www.gao.gov/special.pubs/bcpguide.pdf

National Institute of Occupational Safety & Health (NIOSH)
NIOSH has Y2K case studies, a web forum, vendor list, and an equipment manufacturer directory.

http://www.cdc.gov/niosh/y2k/y2k-hmpg.html

Health & Safety Executive (UK)
The British Health and Safety Executive web site offers several reports on the Y2K problem. Of particular interest to the chemical industry is "Health and Safety and the Year 2000 Problem - Guidance on Year 2000 Issues As They Affect Safety-Related Control Systems" and "Contingency Planning for a Safe Year 2000."

http://www.open.gov.uk/hse/dst/2000indx.htm

National Fire Data Center
A basic system check that can help you determine if your organization's computer system is Y2K compliant is available on this website.

http://www.usfa.fema.gov/y2k/y2kcom.htm

Electronic Systems Center of the Air Force Materiel Command (site maintained by Mitre Corporation)
The site provides information on Y2K certification, compliance, solutions, testing and evaluations, contingency plans, cost estimation, tools and services.

http://www.mitre.org/technology/y2k

National Institute of Standards and Technology
The site has links to free software tests, self-help tools and product compliance status databases for use in Y2K assessment, testing, contingency planning and remediation. Information is provided for smaller manufacturers through the Manufacturing Extension Partnership, a nationwide network of centers providing technical and business assistance to smaller manufacturers. Small manufacturing firms can call 1-800-MEP-4MFG.

http://www.nist.gov/y2k

President's Council on Year 2000 Conversion-Product Compliance Information
The site has a list of computer manufacturers' Y2K sites.

http://www.y2k.gov/java/product_compliance.html

Mary Kay O'Connor Process Safety Center
The site has links to compliance status of some manufacturers' control systems. Click on Y2K information.

http://process-safety.tamu.edu/y2k/y2k.htm

Chemical Manufacturers Association (CMA) Survey
CMA has developed a standard survey form for the use of its members. This survey package is designed to help companies assess Y2K efforts of critical suppliers and customers and minimize the risk of service interruption. The survey (posted on 12/14/98) can be found in the "What's New" section of the CMA website.

http://www.cmahq.com

Case Study of One Chemical Manufacturer's Approach to Y2K Problem

http://www.dell.com/smallbiz/y2k/studies.htm#merisol

American Petroleum Institute
The site provides industry activities, company status reports, Y2K database, and technical links.

http://www.api.org/ecity/y2k/index.html

Year 2000
The site has a list of Year2000 vendors and consultants.

http://www.year2000.com

National Bulletin Board for Year 2000
Provides tools for analysis, conversion, and testing for Y2K problems.

http://it2000.com/solutions/index.html

Y2K Freeware and Shareware

http://www.aphis.usda.gov/y2k/wares.html

Year 2000 Embedded Systems Vendors, Associations, and Manufacturers

http://ourworld.compuserve.com/homepages/roleigh_martin/y2k_com.htm

Some PC Test Results for Y2K Problems

http://www.hqisec.army.mil/y2kweb/y2kresults.html

http://www.nim.com.au/year2000/ye02001.htm

FOR MORE INFORMATION...

CONTACT THE EMERGENCY PLANNING AND COMMUNITY RIGHT-TO-KNOW HOTLINE

800 424-9346 OR (703) 412-9810
TDD (800) 553-7672

MONDAY-FRIDAY, 9 AM TO 6 PM, EASTERN TIME

◆◆◆

TO OBTAIN COPIES OF THIS PUBLICATION, CONTACT NATIONAL SERVICE CENTER FOR ENVIRONMENTAL PUBLICATIONS (NSCEP) PHONE: 800-490-9198 FAX: 513-489-8695
http://www.epa.gov/ncepihom

VISIT THE CEPPO HOME PAGE ON THE WORLD WIDE WEB AT:

http://www.epa.gov/ceppo

United State Environmental
Protection Agency
(5104)
Washington, DC 20460

Official Business
Penalty for Private Use
$300