United States Environmental Protection Agency

Office of Enforcement and Compliance Assurance (2201A)

EPA 300-N-99-010

EPA Enforcement Alert

Volume 2, Number 5 | Office of Regulatory Enforcement | August 1999

Y2K: Is Your Facility Ready?

Regulated Entities Have an Obligation to Prevent Hazardous Releases

The U.S. Environmental Protection Agency (EPA) is encouraging regulated entities to take prompt and proper measures to prevent potential Year 2000 (Y2K) computer failures that may cause releases detrimental to human health and the environment.

A number of federal environmental laws require regulated entities to be designed, operated, and maintained in a manner to prevent hazardous releases into the environment. Due to potential Y2K computer chip and programming problems, date-related failures could occur that may lead to the release of hazardous chemicals or other pollutants into the air, water and land.

This issue of *Enforcement Alert* highlights:

- Several laws that require the prevention of releases to the environment;
- Examples of potential Y2K problems; and
- Recommended steps to avoid potential Y2K, environment or public health problems.

In addition, this issue directs readers' attention to new legislation, H.R. 775, the "Y2K Act," which was signed by President William J. Clinton on July 20. This time-limited legislation is designed to establish certain procedures for civil actions brought for damages relating to Year 2000 computer failures.

Finally in this issue, EPA highlights its new enforcement policy that is intended to encourage regulated entities to perform computer testing for potential Y2K glitches.

What the Law Requires of Regulated Entities

The **Clean Air Act's (CAA)** "General Duty Clause," Section 112(r)(1), requires owners and operators of sta-

Continued on page 2

About Enforcement Alert

"Enforcement Alert" **is published periodically by the Office of Regulatory Enforcement to inform and educate the public and regulated community of important environmental enforcement issues, recent trends and significant enforcement actions.**

This information should help the regulated community anticipate and prevent violations of federal environmental law that could otherwise lead to enforcement action.

See Page 4 for useful EPA Websites and additional resources.

Eric V. Schaeffer
Director, Office of Regulatory Enforcement

Editor: Virginia Bueno
(202) 564-8684
bueno.virginia@epamail.epa.gov

Please email all address and name changes or subscription requests for this newsletter.

Clean Air Act 112(r) Definitions:

Accidental Release: An unanticipated emission of a regulated substance or other extremely hazardous substance (EHS).

Listed Substances: List of chemical substances that pose the greatest risk of causing death, injury, or serious adverse effects to human health and the environment including, but not limited to, the list of extremely hazardous substances (EHS) published under the Emergency Planning and Community Right-to-Know Act (EPCRA).

Stationary Source: Buildings, structures, equipment installations or substance emitting stationary activities that belong to the same industrial group; are located on one or more contiguous properties; are under control of the same person (or persons under common control); and may have an accidental release.

Continued from page 1

tionary sources producing, processing, handling or storing listed substances or extremely hazardous substances ("regulated" substances) to:

- Identify hazards that may result from accidental releases using appropriate hazard assessment techniques;
- Design and maintain a safe facility, taking such steps as are necessary to prevent releases; and
- Minimize the consequences of accidental releases that occur.

This clause applies to any stationary sources that handle any extremely hazardous substance regardless of the quantity on-site.

The Resource Conservation and Recovery Act (RCRA) requires generators and owners and operators of hazardous waste treatment, storage and disposal facilities to maintain and operate their facilities to minimize the possibility of a fire, explosion, or any unplanned sudden or non-sudden release of hazardous waste or hazardous waste constituents to air, soil, or surface water, which could threaten human health or the environment. 40 C.F.R. Sections 262.34(a)(4), 264.31 and 265.31.

All Y2K computer failures that potentially could cause a fire, explosion, or unplanned sudden or non-sudden release to the environment need to be addressed by the hazardous waste generators and treatment, storage and disposal (TSD) facilities.

The Clean Water Act (CWA) states that the discharge of any pollutant without a permit or in violation of a permit is illegal; facilities that discharge to water must maintain compliance with their permits.

The Safe Drinking Water Act (SDWA) sets standards for public water systems to assure safe drinking water for the American public. Water systems must maintain compliance with these standards.

Potential Y2K Problems

Y2K computer problems may occur where embedded computer chips, and older operating system software and application programs may only read the last two digits of a date. As a result, several critical future dates could be misread by the computer. Date-related problems may affect computer clock mechanisms, operating systems, software packages, libraries, tools and application software.

In the **chemical processing and manufacturing industries,** Y2K issues could place workers, communities and the environment at risk. These risks could include unintended, complete shutdowns and malfunctions of automated process machinery (e.g., valves and pumps), control room and telecommunication systems and devices, emergency protection systems and equipment (e.g., fire and gas detectors, evacuation alarms, and fire alarms), and heating and cooling systems. Also, erroneous information caused by Y2K problems may lead process operators to take unsafe and incorrect actions that can result in the accidental release of hazardous substances. If a number of systems are affected by Y2K problems, cascading failures can occur.

In the **drinking water and wastewater sector,** Y2K issues could impact the ability of a Publicly Owned Treatment Works (POTW) to collect and treat sewage, potentially causing backups or overflows of raw sewage and creating a public health emergency. In drinking water systems, Y2K problems could limit drinking water facilities' ability to provide an adequate quantity of water or to produce the quality of water provided under normal operations. This water must meet EPA regulatory requirements.

Potential Computer Failure Dates:

Sept. 9, 1999: Many computer systems use or are programmed to use 9/9/99 as a file purge date.

Jan. 1, 2000: Rollover of the date may halt, confuse or disrupt many systems and devices.

Feb. 29, 2000: Many systems may fail to recognize 2000 as a leap year.

Oct. 10, 2000: First occurrence that requires the use of eight digits. May cause failures.

Dec. 31, 2000: Some systems using Julian dates may not recognize the 366th day of the Leap Year.

Identifying and Fixing Potential Y2K Problems

Year 2000 problems must be promptly identified and corrected before they occur. Doing so now can significantly reduce the risk of safety failures, accidental chemical or pollutant releases, and/or drinking water or wastewater treatment system failures. This effort can also reduce potential liability for violations of federal environmental laws.

EPA recommends that the following steps be taken, at a minimum, to

Continued on page 3

Continued from page 2

identify and remedy the Y2K problem:

1 Identify, check and list every system for date-sensitive logic controls. Focus efforts on software and equipment with embedded chips. Prioritize systems based on the likelihood of causing safety, health, and environmental releases. Review all process hazard analysis to be certain that Y2K dependent control systems, process equipment, and safety devices are inventoried and addressed. Proactive steps such as hiring an expert consultant may be wise if regulated entities are unable to identify and implement Y2K remedies in-house. It also is important that contingency plans be developed that allow for "business as usual." For example, publicly-owned water systems should review and amend their contingency plans to provide safe drinking water in emergency situations.

2 Remedy problems by repairing, modifying or replacing systems, devices or equipment. If vital process control systems and equipment can not be adequately addressed, then consider operating the system in a manual override setting. Retrain personnel if they are unfamiliar with the manual operations. Confirm that employees can shut down the process manually if necessary.

3 Test all embedded software to determine if they will be affected by the Year 2000 date change. Embedded software is software that permanently resides on some internal memory device (e.g., Central Processing Units, Basic Input Output Systems, device drivers, middleware, etc.) in a computer system or other machinery or equipment that is not removable in the ordinary course of operation and is of a type necessary for routine operation. Verify that the updated systems work properly for all potential failure dates.

Due to potential Y2K computer chip and programming problems, date-related failures could occur that may lead to the release of hazardous chemicals or other pollutants into the air, water and land.

4 Establish and train workers on site-specific Y2K contingency plans in order to prepare for unanticipated problems with process control systems. Contingency plans should not be dependent on backup systems and equipment that could also fail because of Y2K problems. Contingency plans should also address how systems can be manually operated. Most importantly, advise employees to alert local emergency officials and the community of possible failures that may inadvertently release hazardous substances.

5 Coordinate contingency planning with critical service providers such as electric and gas utilities, medical and fire emergency response establishments, telecommunications companies, and transportation services. These services may be delayed or not arrive at all because of failures in non-Y2K compliant computers and chips in their systems.

6 If necessary, have extra staff available onsite for a number of hours just before and immediately after critical date changes. Train staff in the contingency plans and in the manual operation of process controls with potential Y2K operational complications.

7 Conduct Y2K computer failure scenarios to learn valuable lessons that can be used to improve emergency response, prevent communication failures, and diagnose and correct equipment malfunctions.

Contact Sounjay K. Gairola, Office of Regulatory Enforcement, RCRA Enforcement Division, (202)564-4003, Email: gairola.sounjay@epamail.epa.gov or Leslie Oif, RCRA Enforcement Division, (202)564-2291; Email: oif.leslie@epamail.epa.gov.

President Signs 'Y2K Act'; EPA's Y2K Enforcement Policy'

On July 20, President Clinton signed into law "The Y2K Act," which is intended to ensure that Y2K problems do not disrupt commerce or create unnecessary caseloads in the courts. Most provisions do not apply to government enforcement actions.

The Y2K Act establishes a "Y2K upset defense" for some federal law violations and provides civil penalty immunity for small businesses for some first-time violations. The Y2K upset defense and the civil penalty immunity expire after June 30, 2000 and Dec. 31, 2000, respectively. In addition, relief is not available under either provision if the violation causes actual or imminent harm.

The **Y2K upset defense** applies to any temporary violations of federally enforceable monitoring and reporting

Continued on page 4

United States
Environmental Protection Agency
Office of Regulatory Enforcement
2201A
Washington, D.C. 20460

Official Business
Penalty for Private Use $300

Bulk Rate
Postage and Fees Paid
EPA
Permit No. G-35

Continued from page 3

violations by any business (regardless of its size) that are directly related to a Y2K failure.

Among other qualifying conditions, the violations cannot result from lack of reasonable preventive maintenance or preparedness for a Y2K failure or be caused by operational error or negligence.

The **small business civil penalty immunity** provisions provide relief to businesses with less than 50 full-time employees.

Available only for small businesses that have not committed the same violation in the previous three years, the violation must have been caused by a Y2K failure and the business must have taken steps to prevent and remediate the failure. Among other qualifying conditions, the business must undertake reasonable and prompt measures to correct the violation.

The full text of the Y2K Act can be found at **http://thomas.loc.gov** and key in "H.R. 775."

In November 1998, EPA issued a "Y2K Enforcement Policy" that is designed to encourage the expeditious testing of computer associated hardware and software that may be potentially vulnerable to Y2K problems. The policy was published in the Federal Register on March 10, 1999.

Under this policy, EPA intends to waive 100 percent of the civil penalties and recommend against criminal prosecution for environmental violations resulting from Y2K testing designed to identify and eliminate Y2K-related malfunctions. To receive the policy's benefits (e.g., waiver of penalties due to testing), regulated entities must address specific criteria and conditions identified in the policy.

To the extent that the Y2K Act provides greater relief than EPA's Y2K Enforcement Policy, the Act takes precedence and will apply. In at least one circumstance, however, EPA's policy may be applicable where the Y2K Act does not apply (e.g., where an entity that is not a small business violates an underlying substantive requirement and not just a monitoring or reporting requirement, EPA's policy may provide greater relief).

Contact Gary Jonesi, Office of Regulatory Enforcement, (202) 564-4002 or E-mail: jonesi.gary@epamail.epa.gov.

Useful Websites

RCRA Enforcement Division: http://www.epa.gov/oeca/ore/red/

EPA's Office of Water Home Page: http://www.epa.gov/ow

Chemical Emergency Preparedness and Prevention Office: http://www.epa.gov/swercepp/y2k.htm

EPA's Year 2000 website: http://www.epa.gov/year2000

EPA's Y2K Enforcement Policy: http://www.epa.gov/fedrgstr/EPA-GENERAL/1999/March/Day-10/g5958.htm

President's Council on Y2K Conversion: http://www.y2k.gov/text/index.htm (the Council is responsible for coordinating the Federal Government's effort to address Y2K issues and readiness).

U.S. Small Business Administration: http://www.sba.gov/y2k (provides information to help small businesses get Y2K ready).

EPA's Small Business Gateway: http://www.epa.gov/

U.S. Chemical Safety and Hazard Investigation Board (CSB): http://www.chemsafety.gov (offers Y2K help to small and medium businesses)

EPA's Audit Policy Website: http://www.epa.gov/oeca/auditpol.htm