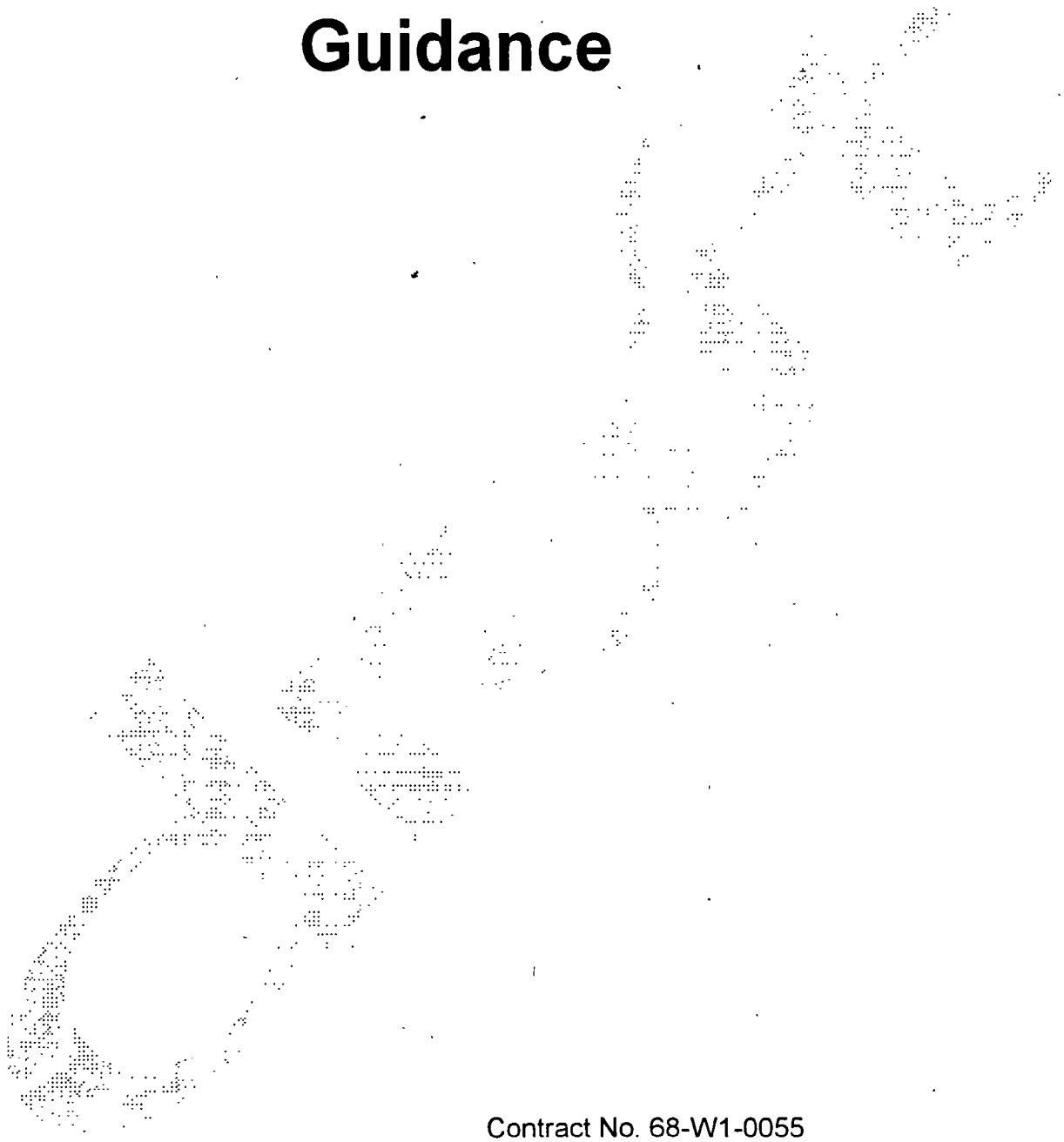
United States
Environmental Protection
Agency

Office of Information
Resources Management

EPA Network InfrastructureYear 2000 Guidance



Contract No. 68-W1-0055
Delivery Order No. 094
Product Control No. SDC-0055-094-DM-6010

August 21, 1997

CONTENTS

EXHIBITS

SECTION 1.0 - EXECUTIVE SUMMARY

Network Infrastructure Year 2000 Guidance 1) provides an overview of the Year 2000 problem within the network environment, 2) reviews network hardware and software components that could be affected by the rollover to the Year 2000 and the resulting problems, and 3) provides guidance on identifying and solving the Year 2000 problem as it affects network components.

Guidance for EPA LAN and WAN Managers

The network infrastructure, including its PC component, is the subject of this Addendum to the *Year 2000 Guidance Document*. The earlier guidance was directed toward solving the Year 2000 problem in application software and data across all platforms, whereas this Addendum focuses on the Year 2000 problem in hardware, firmware, and operating system or utility software and system tools. This guidance is intended to assist Local and Wide Area Network (LAN and WAN) managers and other EPA personnel responsible for EPA LANs and their supporting infrastructure. In addition, system managers will find this document useful when coordinating Year 2000 repair priorities and schedules with LAN managers.

The Problem Facing All Federal Agencies

The Year 2000 problem stems from program code that uses two digits instead of four digits to represent a year value. In code using this shorthand, the year 2000 will be stored as "00," an incomplete value that can cause extensive misinterpretation throughout a network environment. When the following factors are considered, the Year 2000 problem can have a devastating effect on a network

- The network infrastructure comprises myriad components, including microprocessors, embedded software, and firmware. These components contain both obvious and not-so-obvious date functions.

- Many PCs, even recent models, also track the year using only two digits. On January 1, 2000, these PCs will roll from "99" to "00," or, not comprehending the implied "1900," will simply revert to 1980, the "birth" date of DOS.

- Client/server applications are riddled with dates recorded as two-digit, instead of four-digit, years.

Solving the Problem in the Network Environment

The staged approach to solving the Year 2000 problem in the network environment is much the same as for applications and data—plan, inventory, assess, repair, test, and implement. But there are many dissimilarities within the process due to the nature of the network infrastructure. For

example, unlike applications, embedded systems cannot be assessed by reviewing code to identify date occurrences. Therefore, testing will be one of the key ways to identify Year 2000 compliant embedded systems. However, much network equipment cannot be tested. This means that the ability to verify Year 2000 compliance will be limited to researching and evaluating statements issued by a product's vendor or manufacturer.

Critical Activities for Network Year 2000 Projects

It is important to recognize the close connection between the network and application Year 2000 repair efforts. Repairing the Year 2000 problem in EPA's applications and data will be of little use if the platforms used to access them will not function in the Year 2000. As with the Year 2000 application repair effort, there are a significant number of factors that can delay compliance or limit the success of Year 2000 network repair. LAN managers must direct careful attention to completing the following critical activities:

- *Communicating repair priorities between client/server application and network repair efforts.* Delays in repairing the network infrastructure may postpone the repair and testing of mission-critical application systems.

- *Establishing responsibilities for cross-organizational network components.* Because components of the network may reside under different managers, clearly communicating responsibilities for shared components will be essential to success.

- *Sharing vendor compliance information.* Because the network Year 2000 project depends so heavily on vendor compliance statements as an assurance of Year 2000 compliance, sharing this information throughout EPA will save valuable time and resources.

- *Clearly conveying EPA's definition of Year 2000 compliance.* One of the key problems in determining compliance is the various interpretations of the term "Year 2000 compliant."

- *Updating general support system contingency plans for Year 2000-related scenarios.* All LANs require a contingency plan to ensure that the agency functions supported by the system can continue if the system is unavailable. Given the immovable deadline for the Year 2000 project and the interdependencies between Year 2000 projects, contingency planning will be critical for ensuring that the Agency's automated operations are fully supported.

SECTION 2.0 - INTRODUCTION

As a society, we have come to rely heavily on automated equipment, both at work and at home. Much of this equipment contains embedded software and microprocessors which may include date functions. Consider the time and date functions in home VCRs, TVs, thermostats, and microwave ovens. Then there are physical facility date functions in elevators, physical access control systems, and air-conditioning systems that often have a direct bearing on computer system operations and security. Finally, there are PC hardware and software clocks, telephone switches, network routers, and more. Many of these devices have date functions that may fail in the year 2000. What is worse, some network or network-related equipment may have secondary, or even unknown, date functions that could affect the integrity of the equipment in the year 2000.

JANUARY 2000 . . .

Monday, January 3. You sit down at your desk to begin the first work day of the new era, confident you've tested all your PCs and servers, relieved that the Year 2000 compliance effort is completed and work can proceed as usual. You turn on your PC and see the initial prompts. But . . . you can't access your budget planning spreadsheet through the network! You can't open your e-mail! What happened? You begin to realize that, somehow, at least one date function was overlooked during the compliance process. At least the PC works! But if you can't access your network, chances are embedded software or a microprocessor is the culprit.

2.1 THE PROBLEM WITH EMBEDDED SOFTWARE

We already know that application programs that use dates to perform calculations and sort data will produce inaccurate results or crash when the year changes from "1999" to "2000." So too will problems result from embedded software and chips based on two-digit years. Many applications obtain the processing date from the system—if the system date is incorrect, or not what the application expects to find, the application will produce erroneous results. In addition, chips and embedded software may either stop functioning or revert (as do many applications) to assuming the year is "1900."

How can a chip assuming the year is 1900 affect a network? Consider the following scenario. A card reader is used to gain access to a file server room. What happens on Monday, January 3, 2000, when the LAN administrator uses his card to enter the file server room? The system is likely to see the card's date as "1900" and decide that the card, in fact, every card, has expired and no one will be allowed access to the server room!

2.2 DOCUMENT PURPOSE

The purpose of this document is to provide guidance to LAN administrators and other EPA personnel responsible for solving the Year 2000 problem within EPA's LANs and their supporting

infrastructure. A network and its associated infrastructure is often referred to as a general support system. The term "general support system" is defined in the Office of Management and Budget's (OMB) Circular A-130, *Management of Federal Information Resources*, as:

> "an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A [general support] system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO)."

Although the OMB definition of a general support system includes both mainframe and network hardware and software, this Addendum focuses only on the process for resolving the Year 2000 problem within the network environment.

2.3 RELATIONSHIP TO STANDARD YEAR 2000 PROJECT APPROACH

The basic project approach to solving the Year 2000 problem for the LAN infrastructure is much the same as that described in the *Year 2000 Guidance Document*, to include planning; inventory; assessment and triage; and repair, replacement, and testing. But there are important differences. Some of the factors pertinent to the infrastructure environment are as follows:

- Most organizations have large amounts of networked equipment.
- For any given system software (firmware, BIOS, etc.), there are many different versions.
- The equipment may be controlled by many different people, none of whom are experts on that type(s) of equipment.

How is the process different for a network infrastructure? Exhibit 2–1 below highlights network considerations.

Exhibit 2-1. Year 2000 Remediation Process in the Network Infrastructure

Repair Stage	Network Infrastructure Approach
Planning	• Requires close communication among network managers and between network and application system managers/owners, including vendor compliance information sharing. • Requires close coordination of network infrastructure repair with legacy application system repair. • Requires development of vendor coordination procedures to determine product compliance through vendor- or manufacturer-provided information.
Inventory	• Requires that system boundaries be defined. • Must be at a much greater level of detail. Where we were looking at applications and modules of code, now we are looking at operating system versions and releases and PCs, routers, boards, and chips.
Assessment	• Assessment and triage will be less of a physical code review. The triage process will be based both on hardware and software and long-term strategy—is now the time to replace all those 486s? • Assessing the scope of the Year 2000 problem within the LAN infrastructure will require more of a hands-on, compliance testing process to determine if PCs, other hardware components, and system software are compliant. • For untestable devices, or devices for which testing is not feasible, assessing the problem will require researching and monitoring product compliance status as stated by the vendor or manufacturer.
Repair, Testing, and Implementation	• Will often mean obtaining and implementing new physical components or applying patches rather than straight code repair.

2.4 DOCUMENT ORGANIZATION

The Addendum contains seven sections, a bibliography, and Attachments A through D, providing supplementary information. The document is structured as follows:

Section 1.0 **January 2000 . . .** High-level summary of *Network Infrastructure Year 2000 Guidance*.

Section 2.0 **Introduction**. Overview of network infrastructure issues and how this document relates to the *Year 2000 Guidance Document*.

Section 3.0	**Network Infrastructure Components**. A discussion of common components within the EPA network infrastructure that could have a Year 2000 problem, problems specific to these components, and terms you will need to be familiar with when addressing the Year 2000 problem in a network environment.
Section 4.0	**Planning from the Network Perspective**. Key considerations for the network infrastructure planning process.
Section 5.0	**Conducting the Inventory**. Discussion of which components must be included in the inventory, how to identify and document network components, and how to revise the contingency plan.
Section 6.0	**Assessment from the Network Perspective**. Scoping the problem, researching vendor compliance statements, testing PCs and other equipment, and evaluating the assessment results.
Section 7.0	**Repairing, Replacing, or Retiring Network Components**. Conducting the network triage process and defining an approach for addressing the repair, replacement, or retirement of network components.
Bibliography	
Attachment A	Help for Determining Hardware and Software Compliance
Attachment B	Standard EPA Information Technology (IT) Components
Attachment C	Current Year 2000 Websites
Attachment D	Examples of Year 2000 Problems

SECTION 3.0 - NETWORK INFRASTRUCTURE COMPONENTS

Much of the attention focused on the Year 2000 problem is on addressing the issue in application software and data. However, repairing software applications and data will be of little use if the networks that support them have a Year 2000 problem. The components of the network infrastructure, including hardware and its embedded software, must be inventoried and evaluated to ensure that they support processing into and past the Year 2000.

> "There are somewhat over one billion embedded chips in service around the world. At the low end they are very simple, such as timers with a capability of counting seconds or minutes one by one until it receives a stop or reset signal. At the high end are fully functional "computers-on-a-chip" which perform sophisticated tasks. Even to most of us in the information technology business, these things aren't "real computers" ... no key board, no monitor, no printer ports."
>
> *Embedded Chips and the Year 2000*
> Gary Eubanks, May, 1997

As the deadline for the Year 2000 project draws nearer, more projects are focusing on ensuring the compliance of the hardware and software that supports critical applications and data. Hardware typically used within a network infrastructure include physical devices, such as chips, motherboards, monitors, keyboards, etc. However, network hardware requires software to operate. Embedded software is software that is permanently written into memory, such as the older BIOSs, device drivers, middleware, etc. PCs are a good example of hardware with embedded software. The PC contains a central processing unit (CPU). The CPU, also referred to as a chip, microprocessor, or processor, contains embedded software.

In the Year 2000 network inventory and assessment process, you will need to be familiar with terms such as embedded software, firmware, middleware, chips, circuit boards, CPUs, controllers, etc. The precise definition of these terms varies within Year 2000 literature. Therefore, this section provides an overview of the terms commonly used in dealing with the Year 2000 problem in the network environment, including some of the variations to be found.

3.1 WHAT IS EMBEDDED SOFTWARE?

Several definitions exist for embedded software. The State of Washington defines embedded software as "computer software that resides permanently on some internal memory device in a computer system or other machinery or equipment, that is not removable in the ordinary course of operation, and that is of a type necessary for the routine operation of the computer system or other machinery or equipment. 'Embedded software' may be either canned or custom computer software." [from: http://leginfo.leg.wa.gov/pub/rcw/title_84/chapter_004/rcw_84_04_150]

The Institution of Electrical Engineers in the United Kingdom define it as "devices used to control, monitor or assist the operation of

equipment, machinery or plant." [from http://www.iee.org.uk/2000risk/emb.htm]

ComputerWeekly (United Kingdom) defines embedded systems as follows: "Embedded systems are written in low-level code, typically Assembler, then burned into the chip's ROM memory, so it cannot be altered (unless the chip has programmable memory)." [http://www.computerweekly.co.uk/news/8_5_97/08598503239/H1prob.html]

3.2 WHAT ARE THE POTENTIAL PROBLEMS WITH EMBEDDED SOFTWARE?

As with application software, two-digit year problems in embedded systems have the following characteristics:

- The Year 2000 is stored as "00," but the system assumes that the first two digits of the date are "19."
- The system interprets "00" as less than "99." For network components, this may result in date sequencing problems. For example, the operating system may delete or overwrite files from the Year 2000 because it assumes the files are really "1900." The system may not allow software upgrades for the same reason.
- The year "00" may be rejected as an invalid date.

Example of Non-Compliant BIOS

PC's basic input/output system (BIOS) is an example of the Year 2000 problem in embedded software. The IBM PC AT was designed with a real time clock (RTC) that stores two-digits for the date. This clock is simply a battery-backed up counter that keeps track of the date when the power is shut off. The RTC only uses a two-digit counter for the year. CMOS (complementary metal-oxide semiconductor) was added to PCs to provide century information. This IBM PC AT clock design has been used within the industry until fairly recently.

So what happens on midnight December 31, 1999? The RTC adds a "1" to "99," which results in a year value of "00." When the PC is booted, ROM BIOS obtains a four-digit date from the CMOS RTC. This would seem to produce an accurate solution, but when the year is 1999, the century counter fails to rollover correctly, leaving the century as "19" and the year as "00." When this happens, chips and embedded software may either stop functioning or revert (as do

many applications) to assuming the year is "1900." Compounding the problem is that many applications interact differently with the RTC and the operating system—some obtain the date from the RTC and some from the operating system.

Even New PCs Are Not Immune

Don't think that because your PC is a Pentium that you don't have to worry about a BIOS problem. Recent articles document the prevalence of non-compliant BIOS even in newer PCs. A recent article in Computer Weekly (UK) related the results of a test of 500 PCs containing BIOS chips with a 1997 manufacture date. Of the tested PCs, 47 percent contained BIOS that was not compliant.[1]

Other Computer-Controlled Devices

Many computer-controlled devices within the network infrastructure may be affected by the Year 2000 problem, including routers, hubs, private branch exchanges (PBX), Integrated Voice Response (IVR) units, facsimiles, and heating and air conditioning equipment. Each network has many computer-controlled devices, of which many come from different manufacturers. In addition, many networks use operating system software and utilities, which may come from different vendors. Each of these factors and their interrelationships contributes to the complexity of resolving the Year 2000 problem.

3.3 WHAT IS SYSTEM SOFTWARE?

System software: software supporting applications. System software includes operating systems, utilities, and file and LAN management tools. It is important in the Year 2000 process because every LAN function, including applications, voice and data, telecommunications, and other network services is dependent on the smooth operation of system software.

Exhibit 2-1, based on the definition of system software in the PC Webopædia, illustrates the relationships among the different levels of software and computer hardware.

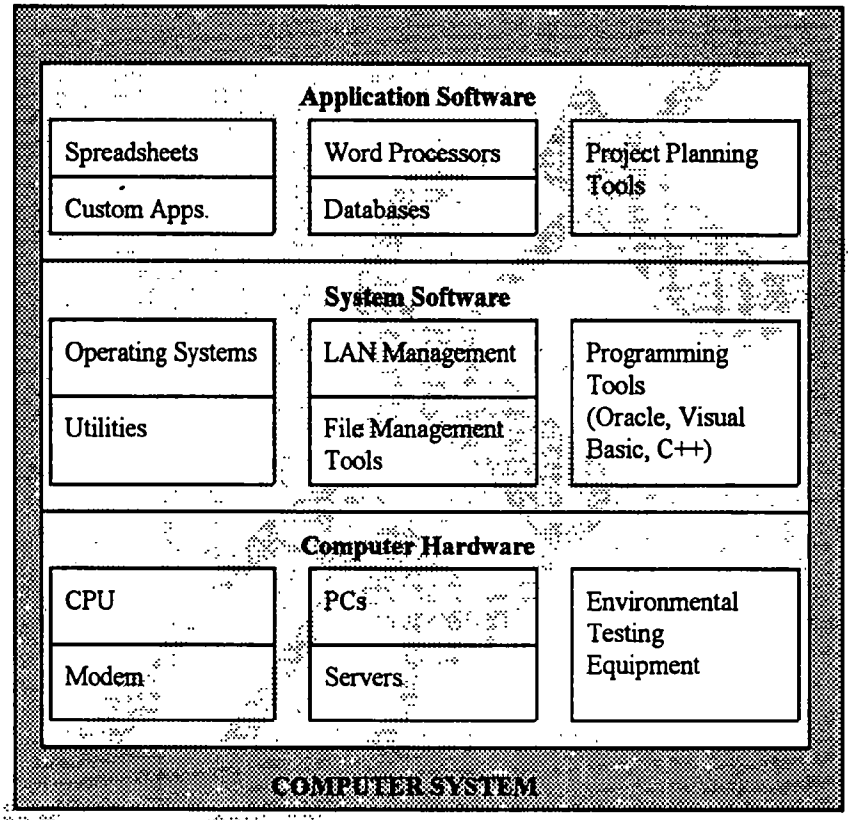
3.4 WHAT ARE THE POTENTIAL PROBLEMS WITH SYSTEM SOFTWARE?

System software based on two-digit year fields can significantly affect the devices and applications running on the network. Examples of the types of problems that may occur include the following:

- The system assumes all dates are in the "1900s." It may be impossible to reset the date or enter a four-digit year, thus

possibly providing applications and network devices with an incorrect date.

Exhibit 3-1. Relationships Between Application and System Software, and Computer Hardware



- The application may receive a garbled date. If the system software makes an incorrect inference about the date, application software may start with an invalid or garbled date. For example, Microsoft's File Manager may show garbled dates for files with timestamps for the years 2000 through 2010. See the Internet article available at http://www.implement.co.uk/milweb81.htm.

- The system software uses a windowing approach. With the deadline looming, many companies are using a windowing approach to resolving the Year 2000 problem. The issue is knowing *what* the date window is (i.e., which years represent 19YY, and which represent 20YY). A problem may arise when interfacing with other systems using other date windowing approaches. See the *Year 2000 Guidance Document*, Section 7.2, for an explanation of date windows.

- The system software uses an incorrect leap year formula. The system software may calculate the day of the week incorrectly because it assumes that the Year 2000 is not a leap year. The software may pass this information to such day-of-week sensitive equipment as thermostats and security access devices.

Who is Responsible?

Who is responsible, or will bear the cost, for fixing hardware and such commercial software such as operating systems? In terms of commercial software, there is much ongoing debate as to who is legally liable for fixing and/or bearing the cost of fixing commercially obtained software. It is unwise to assume that because the software came from a vendor, the vendor is liable for repairing it. The white paper, "Risk Management and the Year 2000," written by Ann Deering, discusses problems with license and maintenance agreements and vendor warranties. The paper is available on the Internet at http://www.adviceinc.com/2000.

Problems with Programming Tools

Programming tools, even those referred to as compliant, may still have problems relating to two-digit years. This is because many tools have the capability to process both two-digit and four-digit years. If programmers are not aware of default-year formats, parameters, or other characteristics of the programming tool, they could inadvertently produce non-compliant code. The Internet is a good source of information on Year 2000 programming tips for software tools such as Oracle, Visual Basic, FoxPro, etc.

3.5 OTHER COMMON TERMS

This subsection provides definitions from PC Webopædia for other terms you may come across in inventorying and researching network components. The URL (Uniform Resource Locator) for PC Webopædia is as follows: http://www.pcwebopaedia.com/.

CPU: "Abbreviation of central processing unit, and pronounced as separate letters. The CPU is the brains of the computer. Sometimes referred to simply as the processor or central processor, the CPU is where most calculations take place. In terms of computing power, the CPU is the most important element of a computer system."

"On large machines, CPUs require one or more printed circuit boards. On personal computers and small workstations, the CPU is housed in a single chip called a microprocessor."

Chip: "A small piece of semiconducting material (usually silicon) on which an integrated circuit is embedded. A typical chip is less than ¼-square inches and can contain millions of electronic components (transistors). Computers consist of many chips placed on electronic boards called printed circuit boards. There are different types of chips. For example, CPU chips (also called microprocessors) contain an entire processing unit, whereas memory chips contain blank memory."

Controller: "A device that controls the transfer of data from a computer to a peripheral device and vice versa. For example, disk drives, display screens, keyboards, and printers all require controllers.

In personal computers, the controllers are often single chips. When you purchase a computer, it comes with all the necessary controllers for standard components, such as the display screen, keyboard, and disk drives. If you attach additional devices, however, you may need to insert new controllers that come on expansion boards."

Firmware: "Software (programs or data) that has been permanently written onto read-only memory (ROM). Firmware is a combination of software and hardware. ROMs and PROMs [programmable read-only memory] that have data or programs recorded on them are firmware."

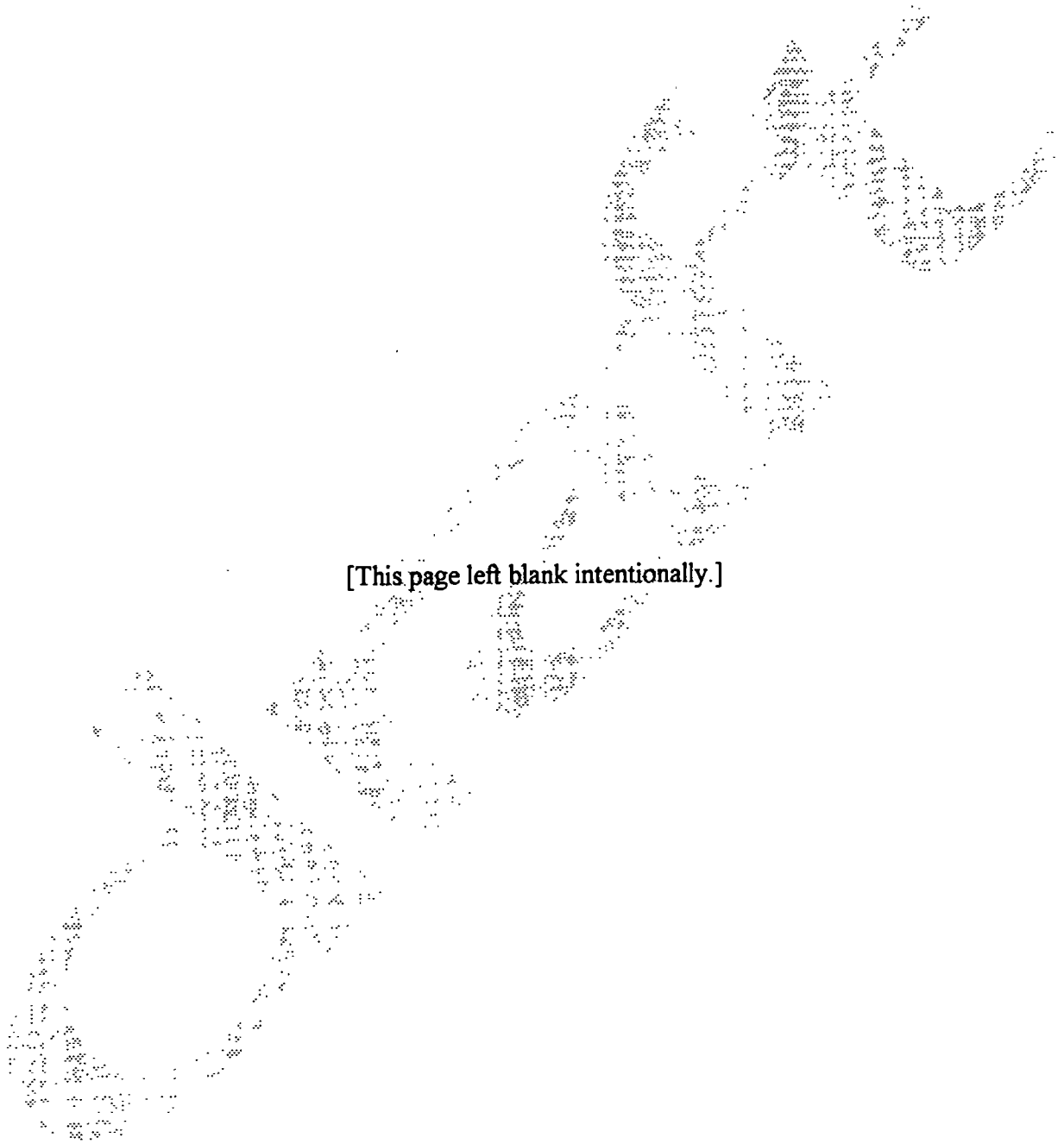
Microprocessor: "A silicon chip that contains a CPU. In the world of personal computers, the terms microprocessor and CPU are used interchangeably. At the heart of all personal computers and most workstations sits a microprocessor. Microprocessors also control the logic of almost all digital devices, from clock radios to fuel-injection systems for automobiles."

Middleware: "Software that connects two otherwise separate applications. For example, there are a number of middleware products that link a database system to a Web server. This allows users to request data from the database using forms displayed on a web browser, and it enables the web server to return dynamic web pages based on the user's requests and profile. The term middleware is used to describe separate products that serve as the glue between

two applications. It is, therefore, distinct from import and export features that may be built into one of the applications."

Endnotes

1. Julia Vowler, "Half of all new PCs fail 2000 Bios test," *ComputerWeekly*, May 22, 1997. Available online at http://www.computerweekly.co.uk/news/22_5_97/08643218486/A.htm



[This page left blank intentionally.]

SECTION 4.0 - PLANNING FROM THE NETWORK PERSPECTIVE

The process of repairing EPA systems and data affected by the Year 2000 problem has begun across the Agency. Critical applications and data must be repaired and tested by the end of 1999. Furthermore, the platforms on which they operate must be repaired, if necessary, well *before* the applications that need them are ready for Year 2000 processing. Careful planning is required if all interdependent systems and platforms are to be ready in time. The intent of this section is to emphasize the importance of planning and identify project planning strategies for the network Year 2000 project.

> "It is generally difficult and expensive to identify and audit embedded systems. The process cannot be automated and is likely to require physical inspection of the hardware distributed widely through the organization. We must accept that risk exists in *any* technology that was ever programmed by a human, examine such technologies for possible failures, and form remediation strategies." [1]

Project planning is often reserved for large software development and maintenance projects. However, given the scale of the Year 2000 problem, even project planning for network Year 2000 projects will be critical. A project plan is necessary because repairing the Year 2000 problem requires strategies for dealing with such unique project issues as network and system interdependencies, untestable embedded systems, equipment with multiple and/or unknown owners, and an unmoveable project deadline. The following paragraphs briefly discuss strategies for ensuring the network Year 2000 project is successful.

Coordinate Network Infrastructure and Application Repair Efforts

It is crucial to ensure that the infrastructure repair effort dovetails with that of the application software. The infrastructure repair involves adjustments to hardware, firmware, etc. that may affect the completion of repair, testing, and implementation of mission-critical legacy application systems. Open lines of communication must be established between network and application system managers to set priorities and coordinate the schedule for repair, testing, and implementation.

Communicate Across Organizations

Various components of the network may reside under different managers with separate management concerns. *When network components, such as servers, cross organizational boundaries, it is essential to know who is taking responsibility for that component's compliance.* Communication of responsibilities and cooperation among network managers and owners will be essential to success.

Organize and Share Vendor Compliance Information

This project requires extensive contact with vendors to identify the compliance of network products, especially those for which testing is impossible or otherwise not feasible. There is a proliferation of Web sites containing hardware and system software compliance status. Communicating is critical—much of the work to identify vendor compliance has already been done. If everyone shares in the knowledge available, current IT resources will go much further. Questions to consider are as follows:

- Which source will you use?
- How was their vendor compliance data gathered?
- Was it obtained verbally or in writing?
- From whom did it come—a sales representative, a vice president, or a technical representative?
- Is a point-of-contact provided?
- Can you trust the data gathered?

Attachment A of this document includes a sample vendor survey from the State of Washington.

Define an Approach for Dealing With Affected Hardware and Software

Develop a strategy for replacing, repairing, or retiring affected hardware and commercial software. Take into account that some vendors haven't even started to address the problem in their software. A large amount of "shareware" for patching PC BIOS's exists on the Web. (However, EPA has strict policies on the use of shareware.) Many sites identify which products are compliant and which are not. Attachment A lists Internet web sites providing product compliance information.

Develop Contingency Plans

Contingency and disaster recovery plans are critical for the Year 2000 repair process. Consider the possible events that may occur during assessment and repair as well as in the Year 2000 operational environment. These include the following:

- Some vendors have not started to address the problem in their software. Is the network dependent on system software that is not yet compliant?

- Tests have shown several cases of equipment from the same manufacturer with internal components (CPUs) from different

manufacturers. One was Year 2000 compliant; the other was not.

The plan must address the network, including telecommunications, and the applications and data running on the network. The network must have a disaster recovery plan that ensures the ability to restore operations for mission-critical functions. A common problem in developing contingency plans is overlooking system resources belonging to, or managed by, other organizations. To be effective, the plan must address all resources needed to support mission-critical functions.

Test the plans, even if it's only on paper. In addition, ensure that master copies of software are available if needed (if the license expires due to setting the date forward). Ensure that applications and data can be restored from backups.

Verify Change Control Procedures

Ensure that a change control process exists. Are change control procedures in place? Are they adequate to support the volume of changes?

Complete Test Plans

Assume any and all components are guilty until proven innocent! Where possible, test even if a component is noted as compliant. Plan tests carefully to ensure the test will not impact system operations. Check individual software packages, such as Lotus Notes or Excel, to identify windowing parameters that may be incompatible.

Define Year 2000 Compliance

Define Year 2000 compliance terms in purchase agreements with vendors. With the acquisition of replacement hardware and software, use Year 2000-compliant language in all acquisitions and make sure you and the vendor have a mutual understanding of "compliant."

Endnotes

1. Testimony of Bruce H. Hall, Research Director, Applications Development Methods and Management, Before the Subcommittee on Technology and The Subcommittee on Government Management, Information and Technology, March 20, 1997. Available at http://www.house.gov/science/hall_3-20.html

[This page left blank intentionally.]

SECTION 5.0 - INVENTORY

The Year 2000 problem mandates a thorough inventory process. The purpose of the inventory is to provide a list of systems and their components for input to the assessment stage. Most people and organizations have never had to track, much less document, all of their systems and components. Do you know how many components your system has and where they are? If not, how will you know where to look for a Year 2000 problem?

> "The problem can and does exist in systems you wouldn't immediately think much about. For example, I recently discovered that five of my six Octel voice mail systems must be upgraded for century compliance; otherwise, all messages at the turn of the century will become 100 years old and will instantly be deleted."
>
> Scott Langdoc, "Y2K: Your Worst Hardware and Software Nightmare," April 21, 1997

5.1 IDENTIFYING EQUIPMENT WITH EMBEDDED SOFTWARE

As with applications and data repair, an inventory is needed for the networked infrastructure, but at a much greater level of detail. All equipment that could potentially contain embedded software must be identified. These are some of the many questions that must be answered:

- Does the system support critical applications?
- Is there current documentation that can help you identify system components?
- What hardware is used by the system?
- How do you know if your hardware contains date sensitive circuits? Looking at the device command set and setup instructions may help in identifying whether hardware has a date function.
- What system software runs the hardware?
- Do you have readily accessible product information?
- Is there a purchase agent who maintains hardware software statistics?
- What are the version and release numbers?
- Is that software still supported by the vendor?
- Does the vendor say it is compliant?
- Can it be tested for compliance?
- Has your contingency plan been revised to address the scope of your inventory and the potential number and type of components affected?

Much of the Year 2000 literature recommends using a "guilty until proven innocent" approach rather than the traditional "innocent until

proven guilty." If you think you don't have a problem, but test for it anyway, you'll be ahead of the game when the year 2000 arrives. Just imagine the opposite scenario: you assumed you didn't have a problem, but on January 1, 2000, your system crashes. What then?

5.2 INVENTORY STEPS

The steps to take in conducting an inventory for the network infrastructure are outlined below:

Step 1. Decide upon a strategy for conducting your inventory—by each system within your office, or by common components of all your systems—for example, inventory all PCs, inventory all routers, inventory all printers. Subsection 5.3 provides examples of typical network components.

Step 2. See what information you may already have for the inventory staff to use, such as system documentation or vendor information provided with the product. Subsection 5.3.1 discusses likely sources of inventory information.

Step 3. Decide on categories of information to gather for each component, prepare standard forms and brief instructions, and provide the forms and instructions to the inventory staff. Exhibit 5-1 provides a sample form for an inventory by component that can also be used in the assessment phase.

Step 4. Determine who will conduct the inventory for specific components (i.e., individual PC users might do an initial inventory of their work space with follow-up verification by LAN personnel).

Step 5. Conduct the inventory that will provide detailed information for each system.

Step 6. Document by system the information you have gathered by component. This step could consist of entering data from the forms into a database or spreadsheet under each system.

5.3 INVENTORY COMPONENTS

These subsections discuss the basic components of the network inventory and categories of information to gather. Keep in mind the breadth of components that can have embedded systems with a Year 2000 problem. Examples of these components include the following:

- **Networks**
  - Bridges and routers
  - Network servers
  - Network system software, including operating system software, embedded software, utilities, etc.

- **PCs**
  - PC hardware
  - Operating system
  - Device Drivers
  - User-written programs and utilities

- **Other Equipment**
  - Facsimile machines
  - Telephone switches
  - Data switching equipment
  - Environmental monitoring equipment
  - Laboratory data acquisition systems
  - Backup generators
  - Heating and air conditioning systems
  - Security systems, security cameras, and door locks

5.3.1 Sources of Inventory Information

In the simplest sense, an inventory process consists of physically identifying components, in this case, equipment and software, for tracking or documentation purposes. Whenever possible, it is a good idea to use other sources for equipment and software acquisitions and locations to supplement the physical walkthrough. This will speed up the process and make the information gathered more comprehensive.

Other such sources might include documentation provided with the equipment or software, purchase records, or LAN network diagrams.

EPA's *Information Technology Roadmap Document* is a useful checklist for ensuring that all components are identified. The components in the Roadmap document are listed in the following categories:

- Hardware Platforms
- Servers
- System Software

- Data Management
- Application System Development Support Tools
- Computing Platform Communications
- Security
- System Management

Attachment B contains a more detailed list of these IT components from the Roadmap document.

5.3.2 Categories of Information to Gather

One of the most important pieces of information you will be gathering for network components is model, version and release, and serial number. This information will be critical in differentiating between compliant and non-compliant hardware and system software; identifying available patches or upgrades; and identifying hardware or software that will not be repaired.

The information gathering should include identifying PCs that do not meet EPA's desktop standards and may or may not be worth repairing or upgrading before the year 2000. Given the considerable expenditure to make all EPA applications, system software, and hardware Year 2000 compliant, in some cases it may be worth holding onto older equipment that can be upgraded for a reasonable price.

In gathering the information needed for network components, it may be helpful to define boundaries and/or categories. For example, information may be gathered at the component level (i.e., identify and document each router, then PCs, servers, etc). Another boundary may be set at the system level.

The information may be categorized either by component or by system, as follows:

- **By Component**:
  - Product name
  - Vendor/manufacturer
  - Version/release
  - Model and make
  - Serial number

- Location and terms of the license and maintenance agreement

OR,

- **By System**:
  - System name
  - Operating system (and version/release)
  - Component
  - Type
  - Vendor/manufacturer
  - Version/release
  - Model and make
  - Serial number
  - Location and terms of the license and maintenance agreement

Whether you decide to categorize the information by component or by system, be sure to pose the following questions for compliant or non-compliant hardware or software:

- **For compliant hardware or software**:
  - The version, release, serial number, or model number.
  - Was product compliance determined by testing?
  - What is the end date?
  - How does the end date appear (i.e., yyyymmdd, mmddyyyy, yymmdd)?
  - Have the Year-2000-compliant models been tested?

- **For non-compliant hardware or software**:
  - Is the product still supported by the vendor?
  - Is there, or will there be, an upgrade for the product?
  - How can the product be upgraded? (repair? replace?)
  - What is the version you currently have?
  - What is the compliant version?
  - When will the upgrade be available?
  - Who is the upgrade manufacturer/vendor?
  - What will be the name of the upgrade?

- What will the date look like after the upgrade (e.g., 2000/02/29 or 00/02/29, etc.)?
- Has the product been tested for Year 2000 date compliance?
- If so, how was the product tested?
- Will the vendor certify that the product is compliant?
- Will this certification be in writing?
- How does the vendor define compliant?

5.4 HOW TO DOCUMENT

In addition to documenting the information gathered (Subsection 5.2.2), document how the component supports the organization:

- What is its function?
- What will happen if it fails?
  - Will it take down the network?
  - Or just one person?
- Is it used to share data?
  - What data?
  - Share with whom?
- Is it still covered under maintenance? (or does it have to be fixed by EPA?)
- Does it have an event horizon other than the year 2000?
- Will it be gone or replaced before its event horizon?
- Is obtaining the component strategically important?

Inventory and Assessment Form

Exhibit 5.1 provides a sample form for an inventory and assessment by component. Using this or a similar form will be of great assistance in documenting your system and keeping the information in one place. In creating a form, include the following considerations:

- Make sure there is a field identifying the system to which a component belongs.

- Recognize that certain components, such as servers, may cross ownership boundaries.

- Note current compliance status if available.

5.5 REVISING THE CONTINGENCY PLAN

The Year 2000 will present some interesting dilemmas for ensuring continuity of support and recovery of processing capabilities should the network be affected by the Year 2000 problem. In the event of such a failure, what will you do? What are the critical processes you support, what happens if those processes fail, and how do you get them back into operation?

Before the assessment and repair processes start, contingency plans must be in place to ensure that the availability and integrity of systems and data are maintained. The assessment process includes testing the system for Year 2000 compliance, which may pose a threat to the integrity of the system and its data. A plan must be in place to ensure that processing and data can be restored if the system, or its applications and data, are adversely affected by the compliance testing process. Preparing and testing contingency, continuity of support, and disaster recovery plans provide an important method for protecting data during assessment, repair, and operations.

Review the contingency and disaster recovery plans in light of the information gathered in the inventory. Are there resources that your system depends on that are managed or owned by other organizations? Does your system have a large amount of system software that could be affected? Does the network include a large amount of hardware that is likely to be non-compliant? Does that network support mission-critical functions?

Disaster Recovery Scenarios

A significant difference from ordinary contingency planning is the kinds of scenarios that need to be examined. Typical contingency and disaster recovery planning considers common threats that may affect the processing environment, such as environmental threats and intentional and unintentional human threats. However, the Year 2000 planning process must consider unique scenarios, such as the range and types of network equipment that could fail simultaneously (including back-up systems or devices) and external factors with potential Year 2000 problems that could impact the network, for

example, telephone switches. Since it is not possible to identify all the things that might go wrong in the testing process, the contingency plan must focus on a range of potential problems. Reviewing the experiences of others in dealing with the Year 2000 problem in the network environment may be a good source of data for determining potential problems. Many lessons learned are posted on the Internet.

The Federal Information Processing Standards Publication (FIPS PUB) 31, *Guidelines for ADP Physical Security and Risk Management*, and EPA's *Information Security Manual* provide instructions for developing contingency plans.

For LANs that provide critical processing support (i.e., that process mission-critical applications and data), a backup processing site may be an option. However, you must first ensure that the backup site itself is Year 2000 compliant.

Exhibit 5-1. Year 2000 Inventory and Assessment Form for EPA System Components

I. INVENTORY

A. Component Description (Complete items 1-7.)

1) Date: _____

2) Component Type: _____

3) Home System: _____

4) Location: _____

5) Component Owner: _____

6) Component Function: _____

7) Year 2000 Compliance Status: _____

B. Product Specifications and Vendor Information (Complete items 8-12.)

8) Product Name: _____

9) Vendor/Manufacturer:

10) Version/Release: _____

Name: _____

Address: _____

11) Serial Number: _____

12) Model and Make: _____

Telephone No. _____

II. ASSESSMENT CHECKLIST (Check yes or no for each question and describe as needed.)

A) Impacts of Failure:	**Yes**	**No**	**Description**
A1) Could malfunction shut down the Network? A2) If yes, describe the impact of the shutdown.	☐	☐	A2)
A3) Could malfunction shut down individual PCs? A4) If yes, describe the effect on overall operations.	☐	☐	A4)
A5) Is the component still under a service warranty?	☐	☐	
A6) Does it have an event horizon other than 2000? A7) If yes, will it be replaced before its event horizon?	☐	☐	A7)
A8) Is obtaining the component strategically important? A9) If so, describe why.	☐	☐	A9)
B) Data Exchange B1) Is the product used to share data? B2) What are the data? B3) Data are shared with what system?	☐	☐	B2) B3)
C) Vendor Support C1) Is the product still supported by the vendor?	☐	☐	
C2) Is there an upgrade? C3) If yes, what version is needed for compliance? C4) What will the date look like after the upgrade?	☐	☐	C3) C4)
C5) Has the product been tested for compliance?	☐	☐	
C6) Will the vendor certify product compliance? C7) If yes, how does the vendor define compliance?	☐	☐	C7)

[This page left blank intentionally.]

SECTION 6.0 - ASSESSMENT FROM THE NETWORK PERSPECTIVE

> The key problem in the assessment process is determining what others mean by Year 2000 compliant hardware and system software—there are no standards for embedded software.

The Year 2000 assessment process focuses on identifying the size and significance of the Year 2000 problem within the network. Although the goal of the assessment process in the network environment is the same as for legacy systems, the steps are likely to be very different. In both cases, the assessment involves locating the problem, identifying solutions, and repairing, replacing, or retiring affected components. The primary difference in the network environment is that this assessment does not include reviewing source code, because you don't have the source code. Assessment will be based primarily on reviewing compliance statements (statements made by vendors as to whether the hardware and software they provide is Year 2000 compliant) and specifications and testing (not to be confused with application software testing). Testing is important—whenever possible, all components must be tested. Hardware and software that cannot be tested must be researched and verified. ***All software and hardware must be assumed guilty until proven innocent.***

Assessing the degree to which the network infrastructure may be affected by the Year 2000 problem consists of the following steps:

- Researching vendor compliance statements.
- Testing compliance.
- Defining an approach for untestable components.
- Completing Year 2000 network triage.

The subsections below provide information on finding and evaluating vendor compliance statements for hardware and software in use at EPA. In addition, an approach for testing the compliance of equipment and its embedded software is discussed. Testing compliance at this stage will be identical to the types of testing required for repaired and upgraded hardware and software.

6.1 RESEARCHING VENDOR COMPLIANCE STATEMENTS

Finding and reviewing vendor compliance statements, or statements from other government Year 2000 project teams, will expedite the assessment process for many systems, especially if the project is divided into groups of similar hardware and software.

During the past year or so, many Year 2000 projects have been surveying vendors to determine if their vendor-supplied products have a Year 2000 problem. This massive survey process has lead government project teams and vendors to post much of this information on the Internet. Refer to Attachment A for a list of current Internet websites providing compliance information; key government-sponsored websites are discussed in the following subsection. Attachment C provides additional sources of Year 2000 information that may be of use in the Year 2000 network assessment process.

6.1.1 Government-Sponsored Web Sites

Several government-sponsored Internet web sites provide Year 2000 compliance information for hardware and software products. To date, these web sites include:

Social Security Administration (SSA). The SSA site lists the compliance status of products in use within the federal government and includes the following information: product name; vendor name and phone number; compliance status (Yes, No, or N/A); compliant version/release and release date; and agencies using the product with a point of contact, version(s) in use, and processing environment. The information at this web site is organized by product name. The URL for this web site is:

http://www.ssa.gov/year2000/y2klist.htm

Department of Defense. The Defense Department sponsors a database containing Year 2000 compliance information on hardware and software products, organized by vendor. The Defense Information Systems Agency (DISA) Commercial Off-the-Shelf (COTS) Software Product Compliance Catalog is available through the following URL:

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

Washington State. This state site maintains a Year 2000 product compliance web site, organized by vendor. The URL for this web site is:

http://www.wa.gov/dis/2000/6_survey.htm

Don't forget EPA. Other EPA offices may have some of the same equipment as you and have already determined the compliance status of these products. EPA is also developing its own Intranet Year 2000 web site which will provide continuous updates on Year 2000 resources and project experience. The EPA Year 2000 web site is expected to be available by the end of calendar year 1997.

Government-Wide Initiative

A current government-wide initiative is a Year 2000 database listing product compliance information provided by vendors, and comments and test results by government agency users. This database will serve as a central repository of Year 2000 compliance information for use by all federal agencies, rather than having each agency develop its own database. The completed database will reside on the General Services Administration's (GSA) web site at http://www.itpolicy.gsa.gov.

6.1.2 Vendor Sites

Many large vendors provide information on the compliance status of their products on their own web sites. Examples include CISCO, IBM, Unisys, and Microsoft. If the information is not present as a link from the home page, it can usually be found by doing a site search.

6.1.3 Contacting Hardware and Software Product Vendors

If compliance information is not currently available for your product, and it is not possible or feasible to test the product for compliance, you will need to contact the vendor. To ensure that all necessary information is gathered through a minimal number of contacts, it's a good idea to develop a questionnaire or survey form listing all the needed information. The Washington State web site contains an example of a Year 2000 survey form used in collecting compliance information. A copy of this survey form is included in Attachment A.

An important component in this survey process is ensuring that the vendor has a clear understanding of what "Year 2000 compliance" means within EPA.

Any form used must, at a minimum, gather the information below.

For compliant products:

- The version, release, or model number.

- Was product compliance determined by testing?
- What is the next date at which date processing problems may arise (sometimes called end date or terminal date)?
- What format is used internally and externally for the date?

For non-compliant products:

- What version/release, model, etc., will be compliant and when will it be available?
- Will the Year 2000 compliance be determined through testing?
- What will the date format in the upgraded product be (i.e., mm/dd/yy, mm/dd/yyyy, yyyy/mm/dd, etc.)?

6.1.4 Are Compliance Statements Proof of Compliance?

The Year 2000 compliance information supplied from these sources must be carefully reviewed and verified where possible. While most vendor statements accurately reflect the Year 2000 compliance status for their product, some may not, primarily due to different interpretations of what "Year 2000 compliance" means. You may not be able to rely on some vendor statements if they are not detailed enough or do not state their definition for Year 2000 compliance.

Consider the following examples from the DISA COTS Year 2000 compliance web site at:

http://www.mitre.org/research/cots/PACKAGE_LIST.html

Example 1.

> Products: M/Exchange, M/TEXT, M/TEXT for Spanish: Versions 3.0+ are Y2K compliant."

Example 2.

> Products: Netopia networking solutions:
> "The industry's first ISDN solutions engineered to provide hundreds of dollars in savings on Internet access per month for small offices has plans to issue a white paper on Y2K issues

soon. To date, the only issues testing has uncovered are inaccuracies in the activity log which will not affect the overall functioning of the program."

Example 3.

3Com(r) networking products:
"3Com certifies that all 3Com products available on or after February 1, 1997 that are date data sensitive will continue performing properly with regard to such date data on and after January 1, 2000, except for those indicated below. If there are current plans to modify these products or product lines, such plans are noted. 3Com is committed to correcting any related problems in currently available products by January 1, 1998. . ."

These examples illustrate the differences in the types of information and level of detail provided in vendor compliance statements. It is likely that organizations will need to use individuals that are experienced with the specific hardware or software in question to evaluate products' Year 2000 compliance statements.

Verify Date Formats

Don't assume just because someone says the product has Year 2000 compliant dates, the dates are in EPA's anticipated format: YYYYMMDD. Microsoft has four-digit years and includes the ability to meet multiple approaches for dates with four-digit years. However, some Microsoft products are shipped with the default date format as MMDDYYYY. In addition, compliance may also mean the use of date windows or century indicators. See the *Year 2000 Guidance Document*, Section 7.2, for an explanation of date windows and century indicators.

Also consider the source of the compliance statements currently available as to who collected the data, who provided the data, and how the data was collected. Was it by telephone or mailed survey, from other users, or directly from the vendor?

6.1.5 Evaluating Results and Sharing Information

At the end of the research process, network components will fall into one of the following three categories:

1. Components verified as Year 2000 compliant through vendor statements. The compliance status of these components should

be verified through testing if possible. Subsection 6.2 discusses compliance testing.

2. Components for which there was no information available from the manufacturer. The compliance status of these components must be determined through testing. See Subsection 6.2.

3. Components that are not yet compliant or will not be made compliant. If components will be made compliant (replaced by the vendor, or a patch provided) prior to the Year 2000, the contingency plan must be updated to address the possibility that the update, etc., may not be ready on time. Components that will not be made compliant must be replaced.

Section 7 discusses an approach for repairing, replacing, or retiring (disposing of) network components that cannot be tested or are not Year 2000 compliant.

Sharing compliance information is critical if all EPA programs and offices are to be ready for the Year 2000. Because so many EPA systems depend on other EPA systems or components of other systems, such as local office networks and central telecommunication systems, system managers who focus solely on their own system may end up being affected on January 1, 2000, by another system that did not complete Year 2000 repairs on time.

6.2 TESTING COMPLIANCE

Compliance testing entails setting the system clock ahead to evaluate the effects of date change to the Year 2000. Where at all possible, test even products the vendor says are compliant!

Network configurations are unique. Each has its own combination of servers, operating system software, devices, interfaces, number of connections, etc. Therefore, this section discusses general issues and a generic process for testing network devices and system software.

6.2.1 Preparing for Testing

Before starting the testing process, remember the following: BACKUPS ARE CRITICAL!! Before compliance testing is started, the system must be fully backed up. *Test* the backup first to ensure that you can retrieve your data and applications from the backup. Does any network software have a product license with an expiration date? Verify that applications will not expire if dates are set forward.

If they will, ensure that the original or back-up disks for the application are available to reload it. Evaluate the impact of setting the date **back**. Consider all connected devices and how a change in date might affect them. When testing PCs, always log out of all networks before beginning.

Test Plan

Develop your test plan. The network's configuration diagram can be extremely useful in identifying possible interactions between hardware and software. Define and document all test scenarios. Include pre- and post-year 2000 dates, including March 31, 2000. Include tests for accurate day-of-week calculations. Carefully document test procedures to ensure that testing is reproducible. The data gathered in the inventory process may be helpful in establishing your test scenarios.

For example, consider the data gathered from the following questions:

- Is the date two-digits or four-digits?
- Is the date incremented using a counter from a base date (e.g., days from January 1980)?
- How does the product calculate the leap year? Does it follow all three leap year rules—divisible by 4, except if it is a new century, in which case it must also be divisible by 400?

If necessary, create test data. Data may be needed if you are going to test the effect on a database of setting the system date forward. Include test scenarios that have data in 1900 and 2000 (in the same set).

6.2.2 Coordinated Testing

Even if the hardware and system software are determined to be Year 2000 compliant, the test process is not over. Tests must still be completed for all applications, COTS, and custom software operating on the network.

Because many applications obtain dates from the operating system's clock, the format used for the date or the windows used for converting dates from two- to four-digit years may have problems when the entire environment is tested together.

6.2.3 Testing PCs

Testing the compliance of PCs is probably one of the easier tasks in the Year 2000 compliance testing process. Test all PCs, even new ones and those from the same vendor. This is important because even new PCs and PCs from the same vendor/ manufacturer have been reported as having BIOS problems. These problems are primarily due to the use of BIOSs from different manufacturers in the same model PC. If you think you don't have to test your PC, consider the following information from the May 22, 1997 edition of Computer Weekly:

> "In a test of 500 PCs containing Bios chips with a 1997 manufacture date, the company found that 235 (47%) were not year 2000 compliant. A separate test found that a massive 93% of pre-1997 Bios chips did not comply." [1]

The State of Utah provides a detailed list of steps to follow in determining PC compliance.

Exhibit 6-1. Is Your PC Year 2000 Compliant?

Test for Compliance by Completing this Form: Source: State of Utah Y2K Home Page	
1.	Exit windows.
2.	At the DOS prompt type logout and press enter to logoff the file server.
3.	At the DOS prompt type date and press enter.
4.	Enter the new date as 12-31-99 and press enter.
5.	At the DOS prompt type time and press enter.
6.	Enter the new time as 11:58p (or 23:59) and press enter.
7.	Turn off your PC (do not just press Ctrl-Alt-Del or press Reset button, turn off machine)
8.	Wait at least one minute and then turn your PC on.
9.	If your computer automatically comes up and asks for your login ID and password just press enter so it will bypass logging into the file server.

Test for Compliance by Completing this Form: Source: State of Utah Y2K Home Page	
10.	Exit windows (if it boots up automatically).
11.	At DOS prompt type date and press enter.
12.	If the date that is shown is anything other than 01-01-2000 then your PC is not Year 2000 compliant.
13.	Also, because year 2000 is a leap year, at the DOS prompt type date and press enter and then type 02-29-2000 and press enter. Type date again and press enter. If you get any date other than 02-29-2000 then your PC is not year 2000 compliant.
14.	At DOS prompt follow steps 3 through 6 to change your date and time back to the current date and time.
15.	Reboot your computer to resume working.

6.2.4 Testing Other Network Devices and System Software

Testing networks may be much more difficult than testing PCs. Servers are the foundation of the network—it may not be possible to take the server off-line and test it. What happens to ongoing work if the server cannot be restored?

For these reasons, testing servers may require the construction of an *identical* processing environment in which to test the compliance of network hardware and operating system software. Components within these identical network environments can be swapped out and verified as compliant.

6.2.5 Problems Identified in Testing Network Components

Experience in testing network components has shown that testing will not be straightforward and will require personnel experienced in the network environment. The most common problem reported is expiration of software licenses—illustrating the importance of backups!

Year 2000 web sites include information about testing experiences that illustrate the need to carefully investigate test results. Interoperability among network components may be one of the

problems that show up during the testing process. In one case, tests in the network environment initially implied that the network was not affected by the Year 2000 problem, but upon further research, the test staff have found areas in which the interconnected network components had a Year 2000 problem. Attachment D provides examples of this and other problems identified during Year 2000 compliance testing.

6.3 EVALUATING ASSESSMENT RESULTS

The outcome of the vendor compliance research and testing process is a list of the networks and network components that were:

- Tested and compliant.
- Tested and failed.
- Untestable, with vendors stating that the product is compliant.
- Untestable, without vendor compliance statements or with vendor stating that it is not complaint.

Based on an understanding of the value of the information and functions that the network supports, you must determine which components are important enough to warrant the resources needed for their repair or replacement.

Endnotes

1. Julia Vowler, "Half of all new PCs fail 2000 Bios test," *ComputerWeekly*, May 22, 1997. Available online at http://www.computerweekly.co.uk/news/22_5_97/08643218486/A.htm

SECTION 7.0 - REPAIRING, REPLACING, OR RETIRING COMPONENTS

The Year 2000 problem must be fixed in critical networks just as in critical legacy application systems. The rapidly approaching deadline and decreasing resources require that affected network components be evaluated and prioritized for repair. This process is very similar to the process described in the *Year 2000 Guidance Document* for completing a system triage for application systems.

> "While a replacement of chips in PCs may seem a simple task, when you multiply this requirement by the number of PCs that exist throughout the Air Force and the manpower this swap-out will require, the picture changes. . . ."[1]

This section discusses the triage process in the network environment: identifying which network systems, components, and/or software will be repaired, replaced, retired, or continued in use with a manageable defect.

7.1 THE NETWORK TRIAGE PROCESS

The concept of conducting a triage for networks is much the same as the process followed in the medical community—determine which systems are in the worst shape, determine if they will still work if repaired, and repair them first. This section discusses setting priorities for repairing or replacing network components to ensure that the most important networks are functional in the Year 2000.

Two factors affect the ability to repair network components. These include the following:

- The amount of **time required vs. time remaining** to fix, test, and implement the changes.
- The number of **knowledgeable staff members** available to make the changes.

Evaluating the components affected by the Year 2000 problem in light of the deadline and current staff will ensure the best use of Year 2000 resources. Note: In this context, affected network components include those in the following categories:

- Failed compliance test.
- Untestable; statement is available from the vendor verifying compliance.
- Untestable; no vendor compliance statement available.

- Vendor states that component will not be made compliant.

- Vendor states that component will be made compliant in the future.

7.2 NETWORK COMPONENT CATEGORIES

Place network components in the following categories.

- *Network components that will be replaced.*

  PCs are an example of equipment that may be placed in this category. Identify PCs that do not conform to EPA's desktop standards that may not be worth repairing/upgrading before the Year 2000. However, replacing all outdated PCs may require considerable resources. In some cases, it may still be worth holding onto older equipment that can be upgraded for a reasonable price rather than doing a wholesale replacement of older PCs and other equipment.

- *Network components that are repairable.*

  Some network components may be repairable either through a patch or upgrade. This is an area in which the cost will be uncertain. In some cases, vendors and manufacturers are providing the repair at no cost, in others, you will bear the cost of the repair.

- *Network components that cannot or will not be repaired.*

  Older network components are likely to fall into this category. If the component cannot be repaired, it will have to be replaced or retired (disposed of).

- *Components whose Year 2000 compliance status is unknown.*

  You must give careful consideration to this final category. Developing emergency procedures to handle the failure of this component is wise; however, consider the importance of the overall system. If the failure of the component or resulting processing problems will cost more in terms of time, money, or system availability than the replacement cost, then the component should certainly be replaced.

7.3 REPAIR, REPLACE, OR RETIRE?

Use a risk-based approach in determining which components will be repaired, replaced, or retired. A risk-based approach includes evaluating the risk and likelihood of failure against the cost to fix or replace the component. Failure of network components or resulting processing problems may have a significant cost in terms of down-time, money, availability of the system or data, and impact on a program or the public.

Support for Critical Processes or Applications

In making the decision to repair, replace, or retire network components, include an evaluation of the processes and applications supported. However, information as to the importance of the network or the applications and data it supports may not be available to system managers. In such cases, obtain input from network users and application and data owners to make the repair, replace, or retire decision.

Other Factors to Consider

Other factors may also come into play in determining which components should be repaired or replaced and the order in which they will be repaired. Consider the following factors:

- *Time to repair or replace.* Is there enough time to fix or replace the component and complete testing?
- *System use.* Does the network/component support a large number of users and functions?
- *Interconnectivity.* Will the loss of the network/component have an affect on other systems or organizations?
- *Long-term strategy.* Does the network/component represent a long-term technology solution for an office or region?

Based on a consideration of the risks and the above factors, prepare a prioritized list of components to be repaired or replaced.

7.4 RESOLVING THE PROBLEM

The following is a list of possible approaches for resolving the Year 2000 problem. Choosing an approach must be based on the importance of the network/component versus the total cost to repair or replace.

- Conduct further research to identify other hardware or software users and their experience and plans for the product.

- Repair the component. If the upgrade or patch is available at reasonable cost **and** in a timely manner, the component can be repaired. Some non-compliant products may have fixes or upgrades in process but the date that these will be available is not set. What happens if a compliant version of the product is not available in time for testing?

- Replace the component. Critical components must be replaced. In other cases, consider replacement if it is cost-effective or if no other option is available.

- Retire or dispose of the component. Non-critical components may not require repair or replacement. Such components would not be of high priority and would not have a significant impact on other networks, components, or organizations.

- Continue to use the component if it has a manageable defect. When identifying this type of component, you must be certain that the Year 2000 problem it contains is isolated and manageable. That is to say, even with a Year 2000 date problem, the component can continue to function without affecting network performance.

  For example, the component could be an obsolete hub that issues a datestamp to a diagnostic database but takes no further action. Work-arounds for this type of component could be as follows:

  - Ignore the incorrect date in the diagnostic software, knowing that it is confined to the hub.

  - Disable Simple Network Management Protocol (SNMP) functionality for the hub so that it will not transmit either an inaccurate date or an error message to the diagnostic database.

Endnotes

1. "Y2K Issue," Internet. Available at: http://infosphere.safb.af.mil/~jwid/fadl/world/isswrld.htm

BIBLIOGRAPHY

2K-Times. Eubanks, Gary. *Embedded Chips and the Year 2000* (May 1997). Online. Internet. August 20, 1997. Available: http://www.2k-times.com/y2k-a152.htm

ADVice, inc. Deering, Ann. *Risk Management and the Year2000: A White Paper* (April 6, 1997). Online. Internet. August 20, 1997. Available: http://www.adviceinc.com/2000/2000-WP.html

Bellcore Year 2000. Bellcore White Papers. *The Year 2000 Approaches...Is Your Network Ready?* (January 1997). Online. Internet. August 20, 1997. Available: http://www.bellcore.com/feature/jan97/y2kwp2.htm

Compaq Computer Corporation. *Service Advisory 1092B - Year 2000 Support* (February 1997). Online. Internet. August 20, 1997. Available: http://www.compaq.com/support/techzone/solutions/sa1092b.html

The Computer Information Centre (CompInfo), The Year 2000 Date Problem - Support Centre. *Where to Look for Potential Problems in your Organisation! Departmental Systems and Embedded Systems* (August 6, 1997). Online. Internet. August 19, 1997. Available: http://www.compinfo.co.uk/y2k/examples.htm

_____. *Y2K Safe Questions*. (September 9, 1996). Online. Internet. August 20, 1997. Available: http://www.compinfo.co.uk/y2k/disa.htm

_____. Cane, Alan. *Millenium bomb: Threat to global telcoms links* (May 2, 1997). Online. Internet. August 20, 1997. Available: http://www.compinfo.co.uk/y2k/ft-may2.htm

_____. Warren, Peter. *Computer chaos in 2000 may stop cars and fridges* (April 6, 1997). Online. Internet. August 20, 1997. Available: http://www.compinfo.co.uk/y2k/consumr1.htm

@ComputerWeekly. Vowler, Julia. *Half of all new PCs fail 2000 Bios test* (May 22, 1997). Online. Internet. August 20, 1997. Available: http://www.computerweekly.co.uk/news/22_5_97/08643218486/A.html

Dallas/Fort Worth Data Chapter of the Data Administration Management Association (DFWDAMA). Reuben, Charles P. *Do PCs have a Year 2000 Problem?? Don't Bother to Ask This I.T. Director (not a DAMA member) Who Just Finished His PC Inventory !!! A Modest White Paper* (February 20, 1997). Online. Internet. August 19, 1997. Available: http://www.dfwdama.com/pcmess.htm

Gartner Group. Testimony of Bruce H. Hall, Research Director, Applications Development Methods and Management, Before the Subcomittee on Government Management, Information and Technology, March 20, 1997. Online. Internet. August 20, 1997. Available: http://www.house.gov/science/hall_3-20.html

Gartner Group @vantage, Management Edge: Year 2000. "Beyond IT Systems: The Year 2000 Touches Everything," an excerpt from *The Year 2000 Crisis: An Enormous Challenge that Must be Addressed* (March 12, 1997). Available: http://www.atvantage.com/atvhome/wsj/ggdoc2.htm

Giga Information Group. Statement of Hearing Testimony, Subcommittee on Technology and Subcommittee on Government Management, Information and Technology. Topic: *Year 2000 Risks: What Are the Consequences of Technology Failure?* (March 20, 1997). Presented by Ann K. Coffou, Managing Director, Giga Year 2000 Relevance Service. Online. Internet. August 20, 1997. Available: http://www.house.gov/science/couffou_3-20.html

Government Executive, Information Technology. Corbin, Lisa. *How to Become Year 2000 Compliant* (May 1996). Online. Internet. August 19, 1997. Available: http://www.govexec.com/tech/articles/0596s1s2.htm

Greenwich Mean Time 2000, Time Bomb. *Implications of Y2k for the PC User and some examples of how your PC may be affected.* Online. Internet. August 21, 1997. Available: http://www.gmt-2000.com/gmt-2000/homepage_frameset.html

HQ Air Force Communications Agency. *Y2K Issues.* Online. Internet. August 20, 1997. Available: http://infosphere.safblaf.mil/~jwid/fadl/world/isswrld.htm

Institution of Electrical Engineers. *Microprocessors and Microcontrollers: Possible Actions* (July 7, 1997). Online. Internet. August 20, 1997. Available: http://www.iee.org.uk/2000risk/actmod2.htm

_____. *The Millennium Problem in Embedded Systems* (August 6, 1997). Online. Internet. August 20, 1997. Available: http://www.iee.org.uk/2000risk/

Internet Engineering Task Force, Year 2000 Working Group. "The Internet and the Millenium Problem (Year 2000) Working Draft" (July 1997). Ed. Phillip J. Nesser II. Online. Internet. August 19, 1997. Available: http://www.ietf.org/ids.by.wg/2000.html

Micro Firmware Technical Support. *The "Year 2000 Problem" on PC Systems* (February 26, 1997). Online. Internet. August 20, 1997. Available: http://www.firmware.com/pb4ts/year2000.htm

Network Business Services Internet Marketing. The Good, the Bad, and the Ugly. *NBS's Own Year 2000 Investigations* [*Real Time Clock Test Results*] (June 19, 1996). Online. Internet. August 19, 1997. Available: http://www.nim.com.au/year2000/ye02001.htm#ye02002

Novell Project 2000. *Novell's Project 2000 White Paper* (May 1997). Online. Internet. August 19, 1997. Available: http://www.novell.com/p2000/wpaper

PCWeek Online, Corner Office. Langdoc, Scott. "Y2K: Your Worst Hardware and Software Nightmare" (April 21, 1977) Online. Internet. August 20, 1997. Available: http://www8.zdnet.com/pcweek/opinion/0421/21corner.html

The RighTime Company [utilities, diagnostics, and fixes] (August 6, 1997). Online. Internet. August 20, 1997. Available: http://www.rightime.com/

Royal Greenwich Observatory. *Information Leaflet No. 52: The Year AD 2000* (May 23, 1996). Online. Internet. August 19, 1997. Available: http://www.compinfo.co.uk/y2k/greenwch.htm

Sandy Bay Software, Inc. *PC Webopaedia* (1996). Online. Internet. August 20, 1997. Available: http://pcwebopaedia.com

U.S. Environmental Protection Agency. Office of Administration and Resources Management, Enterprise Technology Services Division. Cavanaugh, Kevin. *Year 2000 and Agency Personal Computers: An Initial Look at Problem Identification and Steps for Resolution*. Research Triangle Park, NC: June 2, 1997.

_____. _____. _____. *Information Technology Architecture Road Map*. Publication No. 612/002A. Research Triangle Park, NC: August 31, 1995.

The Year 2000 Information Center. Huntress, John. *The Year 2000 and Embedded Systems: For Most Businesses, This Does Not Have to be a Major Problem*. Online. Internet. August 20, 1997. Available: http:www.year2000.com/archive/embedded.html

WebWeek, Infrastructure. Fryer, Bronyn. "Net Is Not Immune to Year 2000 Concerns, Study Says." Reprinted from *Web Week*, Volume 3, Issue 15, May 19, 1997. Online. Internet. August 20, 1997. Available: http://www.webweek.com/970519/infrastructure/immune.html

ZDNet. The ZDNet News Channel. Kerstetter, Jim "Oracle Apps aren't ready as year 2000 draws near." Reprinted from *PC Week*, November 4, 1996. Online. Internet. August 20, 1997. Available: http://www5.zdnet.com/zdnn/content/pcwk/1344/pcwk0104.html

ATTACHMENT A

HELP FOR DETERMINING HARDWARE AND SOFTWARE COMPLIANCE

- State of Washington Year 2000 Project: Survey Letters for Process Control Software and Desktop Hardware
- State of Washington Year 2000 Project: Sample Process Control Software Manufacturer's Survey Response
- Websites Containing Product Year 2000 Compliance Information

August 21, 1997

Washington State Process Control Survey Letter

Dear Sir:

The State of Washington, Department of Information Services (DIS) is researching the impact that the Year 2000 and beyond will have on computer hardware products. Your hardware products have been identified as being used by Washington State agencies. Models include portables, desk-top, LAN /WAN Servers, and Mid-Range in every conceivable configuration.

We know that the BIOS in many models will not roll over to the year 2000 and that in some instances the CMOS itself must be replaced in order to effect the change. Please provide us with a list of all hardware products manufactured by your company that contains a BIOS and is Year 2000 compliant. For hardware that is Year 2000 compliant, please answer the following questions:

1 What is the end date?

2. How does the end date appear? i.e., yymmdd or ccyymmdd, etc.

3. Have your Year 2000 compliant models been tested for compliance?

For State of Washington purposes, year 2000 compatibility must include, but not be limited to, date and century recognition before and after 1/1/2000, and date data interface values that reflect the century. In addition, leap year calculations must be accommodated and must not result in erroneous results or system failures.

We will assume that any hardware product not listed on your Year 2000 compliant list, is non-compliant. For non-compliant products that have been manufactured by your company, please answer the following questions:

1. Can the non-compliant product be upgraded?

2. By which method can the product be upgraded - software (Flash BIOS) or replacement of the BIOS chip itself?

3. When will the upgrade be available?

4. Who will manufacture the software upgrade and by what name will it be sold?

5 How will the date visually appear after the upgrade? i.e., 2001/12/31 or 01/12/31, etc.

6. Is your product tested for Year 2000 date compliance?

7. Do you have recommendations or other information that will help us further identify affected products (serial numbers, BIOS versions, model numbers, etc.)?

We would appreciate a written response to this letter. DIS plans to incorporate your response in a planning document that will be published to state of Washington Information Technology Managers. Because the state of Washington operates on two-year budget cycles, there is for us some urgency in determining future expense associated with this issue.

Your response will be published on the World Wide Web at http://www.wa.gov/dis/2000/y2000.htm (Year 2000 Project Information Resource Center). Should your company have the information available on the web, we will point our Homepage to your Y2K statement.

Washington State Desktop Hardware Survey Letter

Dear Sir:

The State of Washington, Department of Information Services (DIS) is researching the impact that the Year 2000 and beyond will have on computer hardware products. Your hardware products have been identified as being used by Washington State agencies. Models include portables, desk-top, LAN /WAN Servers, and Mid-Range in every conceivable configuration.

We know that the BIOS in many models will not roll over to the year 2000 and that in some instances the CMOS itself must be replaced in order to effect the change. Please provide us with a list of all hardware products manufactured by your company that contains a BIOS and is Year 2000 compliant. For hardware that is Year 2000 compliant, please answer the following questions:

1. What is the end date?

2. How does the end date appear? i.e., yymmdd or ccyymmdd, etc.

3. Have your Year 2000 compliant models been tested for compliance?

For State of Washington purposes, year 2000 compatibility must include, but not be limited to, date and century recognition before and after 1/1/2000, and date data interface values that reflect the century. In addition, leap year calculations must be accommodated and must not result in erroneous results or system failures.

We will assume that any hardware product not listed on your Year 2000 compliant list, is non-compliant. For non-compliant products that have been manufactured by your company, please answer the following questions:

1. Can the non-compliant product be upgraded?

2. By which method can the product be upgraded - software (Flash BIOS) or replacement of the BIOS chip itself?

3. When will the upgrade be available?

4. Who will manufacture the software upgrade and by what name will it be sold?

5. How will the date visually appear after the upgrade? i.e., 2001/12/31 or 01/12/31, etc.

6. Is your product tested for Year 2000 date compliance?

7. Do you have recommendations or other information that will help us further identify affected products (serial numbers, BIOS versions, model numbers, etc.)?

We would appreciate a written response to this letter. DIS plans to incorporate your response in a planning document that will be published to state of Washington Information Technology Managers Because the state of Washington operates on two-year budget cycles, there is for us some urgency in determining future expense associated with this issue.

Your response will be published on the World Wide Web at http://www.wa.gov/dis/2000/y2000 htm (Year 2000 Project Information Resource Center). Should your company have the information available on the web, we will point our Homepage to your Y2K statement.

SAMPLE PROCESS CONTROL SOFTWARE MANUFACTURER'S SURVEY RESPONSES

This attachment provides three samples of the survey results published by the State of Washington in response to their Process Control Software Manufacturer's Survey.

Sample Process Control Software Manufacturer's Survey Response

3Com Corporation

"Is Your Network Ready for the Next Millennium?

There's no need to worry about your network's future. Since 3Com certifies most of its products as compliant with Year 2000 requirements, you can stride confidently into the next millennium with 3Com networking solutions.

The information contained in this document was provided by the various 3Com product divisions and is current as of February 25, 1997.

I. Current Products

3Com certifies that all currently sold 3Com® products that are date data sensitive will continue performing properly with regard to such date data on and after January 1, 2000, except for those indicated in the tables below. If there are current plans to modify these products or product lines, such plans are noted. . . . [continues]"

From a link to the vendor's web site:
http://www.3com.com/0files/products/bguide/yr2000.html

Sample Process Control Software Manufacturer's Survey Response

ADC Kentrox

"October 9, 1996

In our commitment to proactively provide our customers pertinent information, we are providing the following information regarding the impact of the clock change for the year 2000 on their communication systems.

We hope this information, which outlines our product compliance, will be helpful to you. If you have any additional questions, please call our Applications Support team at (800) 733-5511 or (503) 643-1681, or send e-mail to support@kentrox.com. Thank you for your business.

Year 2000 Conformance
The criteria listed below was used to verify proper operation of ADC Kentrox products at the crossover from the year 1999 to the year 2000.

All future products and new releases of current products will be verified to the conformance criteria by the ADC Kentrox Engineering Quality Department.

Year 2000 Conformance Criteria

1. When the product's time and date are manually set to 23:59 December 31, 1999, the product's time and date will automatically increment to 00:00 January 1, 2000.

2. When the product's time and date are manually set to 23:59 December 31, 2000, the product's time and date will automatically increment to 00:00 January 1, 2001.

3. When the product's time and date are manually set to 23:59 February 28, 2000, the product's time and date will automatically increment to 00:00 February 29, 2000.

4. When the product's time and date are manually set to 13:00 January 1, 2000, it may then be manually set to 14:00 February 29, 2000.

5. Product increments time and date correctly through the year 2050.

6. Product recognizes leap years through the year 2050.

Product List

The following table lists the conformance of ADC Kentrox products. . . . [continues]"

From a link to the vendor's web site:
http://www.kentrox.com/support/special/2000prod.html

Sample Process Control Software Manufacturer's Survey Response

Hypercom Network Systems

"Hypercom Network Systems
2851 West Kathleen Road
Phoenix, AR 85023

Phone: (602) 866 5399
Fax: (602) 548 2166

Charles W. Splittorff
Western Regional Manager

May 22, 1996

"Thank you for the opportunity to respond to your concerns over year 2000.

All of the Hybrid Routers from Hypercom are year 2000 ready now.

The Hypercom Routers handle Data (specializing in legacy traffic), Voice and Video without the expense of ATM. We are committed to ATM for your future directions, but currently offer the full spectrum of service on much lower cost media widely available in today's market. If your current needs demand ATM, then we can supply that as well.

Please let me know how Hypercom may be of further service to you as you plan for future projects. We are able to offer you the best combination of services and function for your legacy protocol requirements.""

Sample Process Control Software Manufacturer's Survey Response

Intelligent Controls, Inc. (CTC)

AXxess 100/200: The year 2000

PRODUCT: AXxess 100/200
VERSION: All Versions
SUBJECT: AXxess 100/200: The year 2000

SUMMARY
This document covers operation of ICI's system controllers when the year 2000 arrives.

BACKGROUND
Problems occur when the year 2000 arrives because routines which must compare two dates will fail if two digit years are used and one date is before and one after 2000. For example, the year 01 will test as being before the year 99 whereas 2001 will test as after 1999. Tests which look for equality rather than before or after, such as "is today 01/01/00" will work correctly.

AXxess 200
The Windows based, AXxess 200 program has been designed from the ground up to use four digit years in all situations where dates are used. It has been tested under a variety of simulations and no problems have been found when installed on the newer computers.

. . .

AXxess 100 and PC AccPak
The DOS based AXxess 100 and older PC AccPak programs use two digit years throughout. These programs run on a weekly schedule for most access control events. This includes not only commands such as door unlocking but control of card validity as well. The actual date is only used in controlling these events to determine if a day is a holiday which will work correctly.

Dates are also used for starting and expiring access cards. However, these tests also use the equality test and hence will work correctly with the two digit year.

The main problems, however, will occur when running reports on the audit trail. The audit trail is stored using the two digit date format. The date-time stamp has the form yymmdd hhmmss. For example, 991231 235959 will test as being after 000101 000000 which is actually one second later. If reports are run on the audit trail that contains dates before and after 2000, the report may not run if a starting date and time are specified. The report will run correctly if no start date is specified. .[continues]"

From a link to the vendor's web site:
http://www.intelligentcontrols.com/KB00010.htm

WEBSITES CONTAINING PRODUCT YEAR 2000 COMPLIANCE INFORMATION

The following table lists sources of information for verifying Year 2000 compliance of commercial hardware and software. The sources listed include web sites sponsored by Federal agencies and sites sponsored by private companies and organizations.

The information listed below is current as of August 1997. Please note that Internet addresses are subject to change.

Websites Containing Year 2000 Compliance Information	
Source	**Internet Address**
Social Security Administration	http://www.ssa.gov/year2000/y2klist.htm Information is in alphabetical order by product name. The list often includes a URL to the vendor site.
Defense Department sponsored data base (Provided by the Electronic Systems Center and the MITRE Corporation)	http://www.mitre.org/research/y2k/ Organized 1) by type of software or hardware, and 2) by vendor. Also includes the source of the compliance information and, for many products, a link to vendor home site and/or the vendor phone number.
Washington State Year 2000 Project - Hardware and Software Compliance Surveys	http://www.wa.gov/dis/2000/6_survey.htm Lists hardware and software manufacturers and either survey results or a link to their Year 2000 compliance statements.
Audit Serve, Inc.	http://www.auditserve.com/yr2000/yr2ktrk.html Organized 1) by type of software or hardware, and 2) by vendor. Contains a brief statement as to the product's compliance status or notes a specific Year 2000 problem.
University of Florida	http://www.is.ufl.edu/bawb052h.htm Includes a list of vendors and links to their hardware/software compliance statements.

Websites Containing Year 2000 Compliance Information	
Source	**Internet Address**
International Product Information web site	http://britnet.ftech.net/bin/y2k.pl?SEARCH (Note: This site is also available through http://www.weblaw.co.uk/y2k.htm. Products can be displayed by category or by company. The site can also be searched by product or company name.
CIC The Computer Information Centre (CompInfo)	http://www.compinfo.co.uk/y2k/manufpos.htm Contains a list of hardware and software manufacturers with links to their compliance statements.

August 21, 1997

ATTACHMENT B

STANDARD EPA INFORMATION TECHNOLOGY (IT) COMPONENTS

Standard EPA IT Components[1]

Hardware Platforms

- Desktop devices
  - PC DOS; PC/Windows 3.1
  - PC Win95
- PC 32-bit Operating System (OS2)
- Workstations; Scientific Visualization (Silicon Graphics)
- Unix based workstations (Scientific Open System Workstation)

Servers

- Lan Servers (Intel-based)
  - Network Operating System (NOS)
  - Agency LAN Services (ALS)
  - Relational Database Management System (RDBMS)
  - Applications Servers (Notes)
  - X.400 Gateways
  - Communication servers
- Mainframe
- E-mail Server (DEC VAX)
- Unix Server Data General platform
- DEC/VAX; VAX Scientific Cluster
- Open System Server (Unix)

System Software

- Operating System
  - DOS
  - OS/2
  - DG/US Sun Solaris
  - IRIX
  - Netware
  - MVS/ESA
  - VMS
- Network Operating System
  - Netware
  - Pathworks
  - Unix/NFS

[1]Derived from the *EPA Information Technology Architecture Roadmap*, EPA/OARM, 612/002A, August 31, 1995.

- User Interface
  - Win 3.1 Automaxx
  - MOTIF
  - Open Look
  - TSO/ISPF

Data Management

- File Structure
  - DOS
  - USF (Universal File System)
  - Netware
  - VSAM; ISAM; BDAM
  - RMS
  - NFS/UFS
  - RMS/DECNet
  - NFS
- Navigational DBMS (Phase Out)
  - dBASE
  - xBASE/Focus
  - ADABASE; S2K; Focus
- Navigational DBMS Access to Mainframe
  - Natural Conn
  - SAS Access
- Navigational Front-End to Mainframe
  - Natural; Focus; Easytrieve
- Data Warehouse
  - Oracle
  - DB2
- Relational DBMS
  - Oracle
  - DB2
- Relational DB Comm Access
  - SQL Net
  - SQL Connect
- DBMS Transaction Processing Monitor
  - (TBD)
  - CICS (mainframe)
- Directory (Encyclopedia)
  - IRDS
  - X.500
  - WAIS
- Dictionary
  - Oracle

- Predict
- DB2

Application System Development Support Tools

- 3GL
- 4GL
- Case
- SQL Development Tools
- Object Oriented Development

- Code Management
  - SCCS/RFCS
  - Librarian
  - ENDEVOR
  - USM
  - DECSET
- Development Libraries (Subroutine Libraries)

Computing Platform Communications

- SPX/IPX Communications
  - Netware
  - Netbios
- Asynch Communications
  - XTALK
  - Kermit
  - Nasi
  - In OS
  - Telnet
  - NACS
  - PSI
  - ANET
  - DEC LAT/FAX
  - SLIP; PPP
- TCP/IP Communication
  - LAN WP; WG
  - Pathworks
  - DG; Sun
  - Silicon Graphics
  - TGV-MNET
  - OS
- SNA Communications
  - LAN WS; Dynacom
  - TN3270; x3270
  - SNA/SAA

  - VTAM
  - SNA GW/CT
- DECNET Communications
  - Pathworks
  - DECNET
- X.25 Communications
  - PSI
  - DECNET

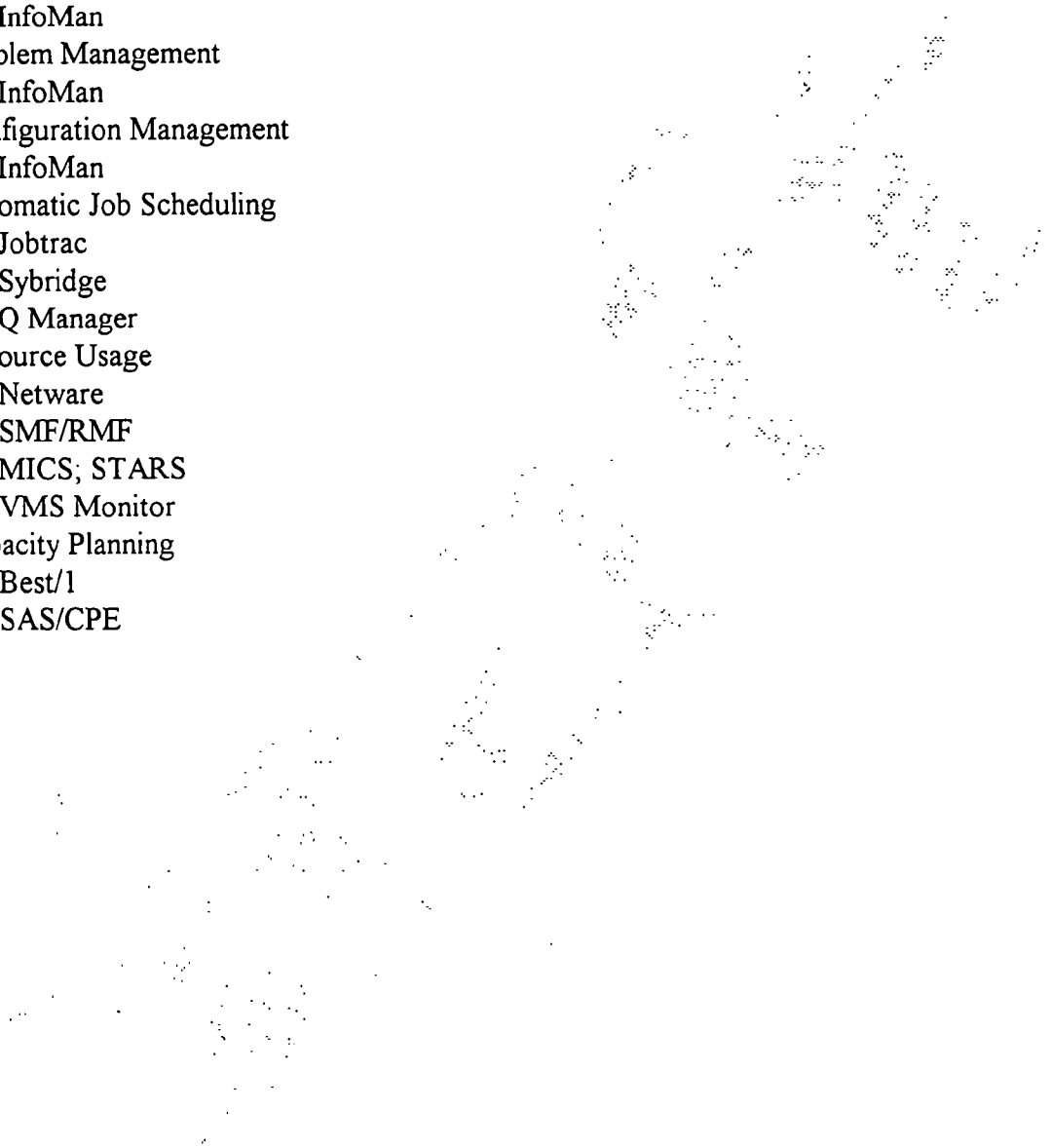
Security

- Control
  - Netware
  - RACEF
  - RMS
  - Hitman
  - DG/UX
- Virus Protection
  - LAN Protect; McAfee
- Monitoring/Auditing
  - LAN Auditor
  - Secure MAX
  - Security ToolKit
  - BINDVIEW; Seems
  - CA/Exam; RACEF

System Management

- Software Distribution
  - AM PM/NIDS
  - OS/EYE*Node
- Backup
  - In OS
  - SMS Compatible
  - Legato Networker
  - Maynard
  - HSM/SMS
  - FDR; ASM2
  - VMS Backup
- Fault Protection/Alerts Monitoring
  - OpenView
  - NMS
  - LAN Manager
  - Netview
  - Omegamon; TMON

  - DECmcc
  - OS/EYE*Node
  - SNMP-MIB2
- Change Management
  - InfoMan
- Problem Management
  - InfoMan
- Configuration Management
  - InfoMan
- Automatic Job Scheduling
  - Jobtrac
  - Sybridge
  - Q Manager
- Resource Usage
  - Netware
  - SMF/RMF
  - MICS; STARS
  - VMS Monitor
- Capacity Planning
  - Best/1
  - SAS/CPE



ATTACHMENT C

CURRENT YEAR 2000 WEBSITES

Current Year 2000 Websites

The following table lists current Year 2000 websites providing information that may be of assistance to network Year 2000 projects. See Appendix D of the *Year 2000 Guidance Document* for a list of websites and documents providing general information for Year 2000 projects. The sources listed below include web sites sponsored by Federal agencies and sites sponsored by private companies and organizations.

These sites are provided for general information. Inclusion in this list does not constitute endorsement or certification by EPA.

The information listed below is current as of August 1997. Please note that Internet addresses are subject to change.

GENERAL YEAR 2000 INFORMATION	
2k-Times ™	http://www.2k-times.com/y2k.htm
Home of the Millennium Bug, sponsored by Durham Systems Management, Ltd.	http://www.year2000.co.uk/
IT 2000 The National Bulletin Board for the Year 2000	http://it2000.com/index.html
The Millennium Problem in Embedded Systems, Institution of Electrical Engineers, United Kingdom (UK)	http://www.iee.org.uk/2000risk/
Texas Tech University Health Sciences Center	http://www.ttuhsc.edu/pages/year2000/ttuy2k.htm
Y2K Cinderella Project	http://www.cinderella.co.za/cinder.html
y2k Home Page	http://www.y2k.com/

GENERAL YEAR 2000 INFORMATION, Continued	
The Year 2000 Information Center™, sponsored by Peter de Jager and Tenagra Corporation	http://www.year2000.com
Year 2000 Information Directory, CIO Council Subcommittee on Year 2000 & General Services Administration Office of Governmentwide Policy	http://www.itpolicy.gsa.gov/mks/yr2000/y201toc1.htm
PC-SPECIFIC INFORMATION SITES	
BIOS Information Guide	http://www.sysopt.com/bios.html
Greenwich Mean Time	http://www.gmt-2000.com/
The Good, the Bad, and the Ugly - Geoff May of Network Business Services	http://www.nim.com.au/year2000/ye02001.htm#ye02002
National Software Testing Laboratories (NSTL)	http://www.nstl.com/
RighTime Company	http://www.rightime.com/
Small Computer Program, Information Systems Management Activity (ISMA), U.S. Army	http://scp.hqisec.army.mil/y2k.html
Test and Evaluation Report - Procedures for Testing PCs	http://tecnet0.jcte.jcs.mil.9000/tdocs/teinfo/appendd.htm

YEAR 2000 HARDWARE AND SOFTWARE SURVEY FORMS	
Air Force Year 2000 Compliance Checklist	http://www.mitre.org/research/cots/COMPLIANCE_CHECKLIST.html
IT Product Questionnaire from Computing Services and Software Association (UK)	http://britnet.ftech.net/bin/y2k.pl?NEW
Texas A & M University Computing and Information Services, Year 2000 Team, Year 2000 Survey	http://www.tamu.edu/cis/teams/yr2k/survey.html
Washington State Year 2000 Project, Hardware and Software Compliance Surveys	http://www.wa.gov/dis/2000/survey/process/procltr.htm and http://www.wa.gov/dis/2000/survey/dt_soft/ssurvey.htm
Y2K Safe Questions, Department of Defense	http://www.mitre.org/research/cots/Y2K_QUESTIONS.html
PROGRAMMING TOOLS	
"Oracle and SQL," Millennium Times Europe, Issue 7, February 10, 1997	http://www.implement.co.uk/milweb82.htm#If We Run Oracle
"Oracle Rdb and the Year 2000, Will Your Applications Become Useless in the Twenty-First Century? Rdb Makes That Unlikely." Jan Smith, Oracle Magazine, August 23, 1996	http://www.oramag.com/columns/ian2000.html

PROGRAMMING TOOLS, Continued	
"What is the Year 2000 Problem and How Does It Affect VB [Visual Basic]?" Class Solutions, Ltd.	http://www.class-solutions.com/whatis.htm
Year 2000 Issues in PC Database Packages	http://shaw.iol.ie/~pobeirne/y2kxbase.htm
MISCELLANEOUS SITES	
PC Webopaedia, Internet Encyclopedia	http://pcwebopaedia.com/
Sample YEAR 2000 Test Conditions	http://www.year2000.ca.gov/Relevant/TestScenarios.asp
State Web Sites StateSearch: Links to State Y2K Sites	http://www.nasire.org/ss/ST2000.html
VENDOR/MANUFACTURER SITES	
Sun Microsystems Year 2000 Information Site	http://www.sun.com/y2000/index.html
Unisys	http://www.unisys com/marketplace/year2000/
Digital Equipment Corporation	http://www.software.digital.com/year2000/
Hewlett-Packard	http://hpcc920.external.hp.com/wcso-support/30VinYear.html

ATTACHMENT D

EXAMPLES OF YEAR 2000 PROBLEMS

EXAMPLES OF YEAR 2000 PROBLEMS

The following list provides examples of Year 2000 problems identified in software and/or hardware. The information listed below is current as of August 1997. Please note that Internet addresses are subject to change.

Example 1 - Network Interoperability Problems

The following reference includes three examples of network Year 2000 problems. The problems were identified during Year 2000 compliance testing.

Bellcore White Papers, *The Year 2000 Approaches...Is Your Network Ready?*

"Our experience has shown that while suppliers may find the majority of problems in their own equipment, they often do not have the resources necessary to verify that their equipment will interoperate with that of other suppliers' once the year 2000 change occurs. . . .

Bichlien went on to give several real-life examples to illustrate the point. One carrier was using a particular supplier's Network Elements (NEs) to implement a bi-directional fiber ring network. These systems were managed by an element manager and several Operations Support Systems (OSSs). As part of Bellcore's sample test of the NE's Year-2000 compliance, the element manager's system clock was set to 12/31/99, 11:59 p.m. After this change, the following behavior was observed.

The system first responded to the date change with an acknowledgment of "Fri Dec 31 23:59:00 EST 1999". A short time later it responded to a query for the date with: "Sat Jan 1 00:01:59 EST 2000". Thus, at first glance, it appeared that everything was working correctly. However, further testing uncovered a variety of problems. Here is a brief list:

- Using the date command to set any date beyond 1999 resulted in the system clock being reset back to a date that was pre-1975! That is, once the year 2000 was reached, it was not possible to set the element manager's system date to the correct date!

- Whenever the element manager received an alarm from an NE, it checked the date of the alarm and compared it with its internal system date. It was also observed that, once the year 2000 was reached, any attempt to correct the system date meant that no further alarms from the NEs would ever be displayed!

- The element manager application was licensed from the supplier for a specified length of time. In the process of doing these tests, once the system date was erroneously reset by the system to the pre-1975 date, the element manager's database locked out any further transactions and displayed an error message saying that the right-to-use license had expired!

Example 1 - Network Interoperability Problems

As another example, another type of NE was tested by again setting the system date to 12/31/99, 11:59 p.m. After this change, the system date was observed to correctly roll over to "Sat Jan 1 00:00:01 EST 2000". Additional tests confirmed that 2/28/2 000 correctly rolled over to 2/29/2000, and 2/29/2000 in turn correctly rolled over to 3/1/2000. Again, at first glance, it appeared that everything was working fine. However, further testing revealed that when a bulk recent change request was initiated , the system responded with an error message indicating that "only future release dates are valid for use with this command." That is, the NE software module that processed the input message was apparently interpreting an internal two-digit year "00" as the year 1900, rather than as the year 2000, and it refused to process the request because it was a date in the past!

As a third example, another type of transport NE from several different suppliers were tested in a similar fashion. Again the dates indicating the change in century, and the recognition of the leap year appeared to be working correctly. While it was not universally true of all the suppliers' products, with NEs from some suppliers, it was impossible to make any changes in the system date once the date rolled over to the year 2000!"

Available at:
http://www.bellcore.com/FEATURE/JAN97/y2kwp2.htm

Example 2 - Year 2000 Problem with PC Application

The following excerpt discusses a Year 2000 problem in a spreadsheet application.

Patrick O'Beirne, MD, Systems Modelling Ltd., "Year 2000 Problems with the PC," May 1997, *Irish Computer*.

"If you enter 03/02/01 into an MS Excel cell, it uses the default date format of Windows (see above) to decide how to display the date. You will need to expand the default column width to display the full date. You may be surprised at the result - different versions of Excel have different assumptions about two-digit years. In Excel 5, figure below 20 are assumed to be 20xx century. In Excel 97, it goes up to 30 before assuming that you meant 19xx. One bank user got upset doing long term projections by typing in dates and did not notice that it took 1/1/21 to mean 1921 and gave wrong results in his calculation. You won't find this in the printed documentation - look for it on the MS Web site www.microsoft.com."

Example 3 - Problems in MS Access

Discusses Year 2000 problems and issues specific to PC database packages.

Patrick O'Beirne, MD, Systems Modelling Ltd., *Year 2000 Issues in PC Database Packages.*

"MS Access will interpret a two-digit year differently depending on whether you have OLEAUT32.DLL installed on your system. That DLL is installed by MS Internet Explorer 3.0.

The default input mask doesn't recognize any date past 1999. If you use a short date format and input "00", the default goes to 1900. To correct this, goto Design View, click on Input Mask, and type 99/99/9999 or whatever format you want. That _is_ tedious to have to do for every control. You might wish to consult the Microsoft KnowledgeBase PSS ID Number: Q132067 Article last modified on 05-27-1996 PSS database name: ACCESS 2.00 WINDOWS. This article describes two methods that you can use on a field formatted for the Short Date data type so that it displays a year later than 1999."

Available at:
http://shaw.iol.ie/~pobeirne/y2kxbase.htm

Example 4 - Year 2000 Problem in Manufacturing Process Control Systems

The following excerpt provides an example of the effect of a leap-year problem in a manufacturing process control system.

Patrick O'Beirne, Systems Modelling Ltd., *The Millennium Problem.*

"ONE PLANT'S £500,000 PROBLEM

At midnight on New Year's Eve 1996 at Tiwai Point in South Island, New Zealand, all the smelting potline process control computers stopped working instantly, simultaneously, and without warning. The Bell Bay plant in Tasmania shut down two hours later - midnight local time. Both smelters used the same computer program, which was written by Comalco computer staff. New Zealand Aluminium Smelters general manager David Brewer said : "The failure was traced to a faulty computer software program, which failed to account for 1996 being a leap year. The computer was not programmed to handle the 366th day of the year. Each of the 660 process control computers hung up simultaneously at midnight. The glitch was fixed and normal production restored by mid-afternoon. However, by then, the damage had been done. Without temperature regulation, four cells overheated and will have to be replaced at a cost of more than NZ$1 million." (Source: NZPA [New Zealand Press Assoc.])"

Available at:
http://shaw.iol.ie/~pobeirne/ieismelt.htm

Example 5 - Default Date Formats

The following discussion includes examples of problems resulting from the use of default date formats.

Mike Sapsard, "Dates Exist at Four Levels," *Millennium Times Europe*, Issue 7, February 10, 1997.

"The reasons for John Hyde only seeing the date as 01/01/:0 were threefold. Because his system had the short date format set to only two digits the century was not shown, and the decade appears to be read from the file system as a hexadecimal character, which File Manager then displays as the equivalent ANSI character. When I created and saved a file called fred.txt it showed up identically in both Win 3.11 and Win 95 (across the network) versions of File Manager, as here. In this case the date was shown as 01/01/19:5.

Saving a file in 2011 gave a File Manager save date of 03/02/;1, or 03/02/19;1 with the earlier colon being replaced by a semi-colon. Further experimentation showed that the 'Beyond Year 2000' marker comes from the ANSI character set from 58 to 67. 0 to 9 correspond to 48 to 57, so the series is just continued for the new characters, with the 19 for the century left unchanged. The latest year to which the system date could be changed was 2099, precisely as reported in the extract from the Microsoft web page in MTE issue 4. In Win 95 and Explorer the date is shown correctly beyond year 2000. . ."

". . . An illustration of this interdependence occurred recently when I was upgrading a Borland Delphi application that uses the Interbase database. In this application dates of various transactions must be recorded. In the original software a mask was used to ensure that dates could only be entered in dd/mm/yy format. When I changed the mask to dd/mm/yyyy format the display showed 27/01/__97, with two blanks in front of the two year digits. With a little adjustment of the parameters for the mask I obtained 27/01/97__ with two trailing blanks. Why could I not obtain the full year?

After a little thought I looked in Settings /Control Panel /Regional Settings /Date and found the answer. Only it isn't the complete answer. The component that I was using looked up the date in the Short date style mentioned above. It appears that I will have to write a custom component to ensure full Year 2000 compliance regardless of any settings in the operating system made by the user. This is where some more thought is required by the operating system and programming language vendors before they release their Year 2000 compliant products. Even File Manager and Explorer are only applications, hence their behaviour."

Available at:
http://www implement.co.uk/milweb81.htm

Example 6 - E-mail Problems

The extract below discusses a possible Year 2000 problem in E-mail protocols.

Bronwyn Fryer, "Net Is Not Immune to Year 2000 Concerns, Study Says," *Web Week,* Volume 3, Issue 15, May 19, 1997.

"Peter de Jager, a leading Year 2000 expert in Toronto, said his organization has detected a minor problem with e-mail sorting using Qualcomm's Eudora. For example, incoming e-mail that is time-stamped with year digits of "00" sometimes is moved to the top of the In-box list, rather than to the bottom, where new messages are generally seen. "We don't yet know whether that problem is in the e-mail protocols or in Eudora," he said."

Available at:
http://www.webweek.com/970519/infrastructure/immune.html

Example 7 - File Manager Year 2000 Problem

The following article discussing the Year 2000 problem in Microsoft's File Manager software is from the Microsoft Knowledge Base.

"File Manager Shows Garbled Date for Year 2000 or Later

Last reviewed: November 23, 1994
Article ID: Q85557

The information in this article applies to:

Microsoft Windows operating system versions 3.1, 3.11

SYMPTOMS

Microsoft Windows File Manager displays an incorrect date if the file is created with a date of 01-01-2000 or later.

STATUS

Microsoft has confirmed this to be a problem in File Manager version 3.1. We are researching this problem and will post new information here as it becomes available."

Available at:
http://www.microsoft.com/kb/articles/q85/5/57.htm

Example 8 - Microsoft Access Year 2000 Problem

The following article discussing the Year 2000 problem in Microsoft Access is from the Microsoft Knowledge Base.

"ACC: Years 00-29 Default to Year 2000 When Typed as M/D/YY

Last reviewed: July 1, 1997
Article ID: Q155669

The information in this article applies to:
Microsoft Access versions 7.0, 97

SYMPTOMS

Novice: Requires knowledge of the user interface on single-user computers.
When you type a date in the format M/D/YY where YY is a number from 00 through 29, Microsoft Access defaults to the years 2000 through 2029.

CAUSE

You have a newer version of Oleaut32.dll, which may have been installed by Microsoft Internet Explorer version 3.0 or Microsoft Windows NT version 4.0.

RESOLUTION

Type all four digits for the year when you enter a date.

MORE INFORMATION

Microsoft Access 7.0 and 97 both use Oleaut32.dll to determine what century to use for dates when you do not specify the full year. The file can incorrectly calculated the date if it is the file supplied with Microsoft Internet Explorer version 3.0 or Microsoft Windows NT version 4.0."

Available at:
http://www.microsoft.com/kb/articles/q155/6/69.htm

Example 9 - Year 2000 BIOS Problem

The following excerpt discusses the BIOS problem and provides an example of several BIOSs that have a problem other than the standard BIOS flaw.

Patrick O'Beirne, MD, Systems Modelling Ltd., "Year 2000 Hardware Compliance," June 1997, *Irish Computer.*

"The date in MS operating systems from DOS through to Windows 95 is kept internally as a count of days since 1980-01-01, the operating systems' "day zero", not 1980-01-04. January 4, 1980 is the result of an algorithm that produces unexpected results when its input is outside of the anticipated range. If, when DOS boots, it reads an out-of-range date from the CMOS RTC, as 1900 is, the date conversion algorithm (to days-since-1980/01/01) calculates an erroneous 1980-01-04; that's what the DOS date will become after rebooting the system after the year 2000 transition if the CMOS RTC exhibits the standard flaw.

A few specific BIOSs cause behavior other than the standard flaw. Importantly, the Award v4.50 series BIOS might not allow any date after 1999 and the Award v4.51PG BIOS - currently common among Pentium- and 486-based machines reports 2096 under some circumstances. These BIOSs can not be corrected by software; they must be upgraded.

OS/2 uses windowing of the CMOS RTC two-digit year to infer century. NT appears to store the century in the registry. Both of these operating systems ignore the content of the century byte in the CMOS RTC and will fail to update it when it should change to 20. Consequently, even though the OS/2 and NT system dates will be fine after the 2000 transition, the CMOS RTC century will still be 19. This leads the machine into the classic RTC problem if Windows or DOS are booted after the change; since 1900 is an invalid year to DOS and Windows, it will be interpreted as January 4, 1980. This erroneous DOS date can usually be corrected by simply setting the date to what it should be; DOS will (via the BIOS) set the CMOS RTC century correctly so subsequent boots will yield the correct date."

Available at:
http://homepages.iol.ie/~pobeirne/complhw.htm

Example 10 - Problems on the Web

The following article discusses a Year 2000 problem with JavaScript.

Walter R. Houser, "The Web is not immune to year 2000 date foul-ups," *Government Computer News,* April 14, 1997.

"JavaScript 1.1, released with Netscape 3.x, and subsequently included in Netscape Communicator, has a schizophrenic getYear function that will return either a two-digit or four-digit year. For dates prior to 1/1/1900, it returns a four-digit year. For dates between and including 1/1/1900 and 12/31/1999, the 20th century, it returns a two-digit year. For dates after and including 1/1/2000, it returns a four-digit year."