

---

# The Year 2000 (Y2K) Problem and the Foreign Military Sales Customer

By

Lieutenant Commander Nels E. Berdahl, SC, USN

Information Systems (IS) professional journals, mainstream print media, and several television programs have carried stories about the potential impact of the Year 2000 on our computer-dependent society. These stories often focus on the mind-boggling expense involved in modifying existing program code so that it will correctly handle the year 2,000 (Y2K). Estimates of the total global cost to fix the "Y2K problem" range from \$300 to \$600 Billion.<sup>1</sup> Normally, an investment of this magnitude results in some improved product, tool, or capability. Managers responsible for the massive information systems project known as the "Y2K problem" are simply hoping that "business as normal" will be the mark of their success.

This article will briefly summarize the Y2K problem confronting the Department of Defense and explore some of the issues facing Foreign Military Sales (FMS) customers who have purchased military hardware from the United States. What should or can they do to minimize both the cost and the operational impact of making information systems and military hardware "Y2K compliant?"

## WHAT NEEDS TO BE CHANGED?

The Y2K problem reflects the pervasive influence of information systems on our way of life. We cannot manage the pace of business activity today without modern information systems. What needs to be checked and possibly corrected? *Any* system that has *any* type of automated input from *any* other system, or involves the calculation of dates. The Department of Defense Year 2000 (Y2K) Management Plan defines the "Y2K problem" as

. . . the term used to describe the potential failure of information technology (IT) prior to, on or after January 1, 2000. This potential exists because of the widespread practice of using two digits, not four, to represent the year in computer databases, software applications, and hardware chips. Difficulties will arise in the Y2K when that year is 00 and our information technology will be unable to differentiate it from the year 1900. The associated, but unrelated, calendar year anomaly that must be included in the Y2K systems repairs is the fact that Y2K is a leap year unlike most other century dates.<sup>2</sup>

The reason for the Y2K problem relates to the way programmers designed date storage and processing back when data storage space was at a premium. Programmers often used just the last two digits of the year. This creates no problem as long as the *first* two digits are "19", but if the first two digits vary, many programs will produce results that are incorrect, because the computer quite sensibly processes or sorts the year "00" or "01" as occurring before the year "99."

---

<sup>1</sup> Garner Group estimate cited in "The Global Impact of Year 2000 Computer Processing Problems on Citizens, Businesses and Governments," URL <<http://www.cssa.co.uk/cssa/new/y2kwits.htm>> (2 Sep 1997).

<sup>2</sup> Department of Defense Year 2000 Management Plan, version 1.0, April 1997, Offices of the Assistant Secretary of Defense (Command, Control, Communications, Intelligence). URL for full text is <<http://www.doncio.navy.mil/y2k/dodmgtpln.doc>> (2 Sep 1997).

---

No “quick fix” or “silver bullet” can be used to solve the Y2K problem. Millions of lines of program code have to be inventoried, examined, altered, validated and tested. The problem increases with dramatic complexity if the original source code is not available or unknown. This special problem of missing source code crops up in many of the programs that are *really old* and written in programming languages for which few people remain proficient. U.S. government agencies, as well as businesses, still use thousands of programs and millions of lines of code, that were written in previous decades.

For traditional information systems, solving the Y2K problem means we have to look at all of the following:

- Hardware—everything from personal computers to mainframes,
- Software applications—like the Training Management System (TMS),
- Commercial Off-The-Shelf (COTS) software—like Microsoft’s Access,
- Contracts for future hardware/software,
- Communications hardware and software, and
- Any aircraft or weapon system using the Global Positioning System (GPS) to provide time information or other system clock inputs.

In addition to what first comes to mind when we think of “Information Technology” (IT) systems, there are several other categories of equipment that our IT systems depend on for communications: routers, bridges, switches, PBXs, etc. Still more devices, not traditionally considered IT, may be controlled by embedded microchips that may be affected by the year 2000. Here’s a sample list of equipment that *could* be affected:<sup>3</sup>

|  |                         |
|--|-------------------------|
| Scanning Devices of all types (e.g. Bar Code Scanners)                                   | Pagers                  |
| Security Access Control Systems (e.g. Card Readers)                                      | Parking Lot Gates       |
| Flex-Clocks/Time Recording Systems   | Sprinkler Systems       |
| HVAC Equipment (including thermostats)   | Elevators/Lifts         |
| Planned Maintenance Systems  | Telephone Systems (PBX) |
| Lighting (switching systems)   | Telephone Networks      |
| Facilities Management Systems (AutoCAD)  | Mobile Phones           |
| Postage Franking Machines  | Answering Machines      |
| Electronic Telephone Handsets  | Voice Mail Systems      |
| Global Positioning Systems (GPS)   | Traffic Lights          |
| Sewage Treatment Plant Controls  | Photocopiers            |
| Desk-Top Publishing Systems  | Video Recorders         |
| Image Manipulation Hardware/Software (Photographic)                                      | CCTV Systems            |
| Video Cameras/Camcorders   | Fax Machines            |
| Video/Audio Editing Suites   | Scientific Calculators  |
| Still Camera Datapacks   | ATM Machines            |
| Print Preparation Software   | Microwave Ovens         |
| Electronically Controlled Clocks/Watches   |                         |
| Electronic Time Management Systems (e.g. Personal Electronic Organizers)                 |                         |
| Medical Devices (e.g. Infusion Pumps in Drip Feeds, electronic wheelchairs, pacemakers)  |                         |
| Cars (Engine Management/Service Interval Prediction Systems)                             |                         |
| Process Control Devices (DCS, SCADA, RTU + field devices with embedded micro-processors) |                         |

---

<sup>3</sup> This is one of several good summary pages that can be found on the Navy Supply Corps Systems Command Year 2000 web page. The URL is <<http://www.navsup.navy.mil/y2k/index.html>>.

---

Any device, subsystem component, or interface within/between a system(s) that is not Y2K compliant can potentially corrupt the larger system's data. Thus, the initial screening question is: will this system be needed and operating in the year 2000? This is the basic approach taken by all U.S. government agencies in every business area: can this system be retired before it becomes a problem? If we don't plan on using it in the year 2000, we don't need to fix it.

### *When Does the Y2K Problem Start?*

When is the year 2000 a problem for IT systems? While the standard DISAM instructor answer is "It depends," the reality is "Right now!" Several bank institutions have had to conduct emergency surgery on their Automated Teller Machine (ATM) systems after they refused to recognize credit cards with expiration dates of 00. Life insurance companies have already had to deal with annuity computations that cross the year 2000. Many programmers who worked on systems in the 1960s and 1970s assumed their systems would be replaced by the turn of the century, and thus used a "99" in some date fields to indicate a program or authorization that has no expiration date. Those systems using the "99" convention will be having problems on January 1, 1999, a *full year* before the dreaded "2000 dead-line." Other financial and logistics systems have "fiscal year" fields; the fiscal year 2000 starts October 1, 1999.

## **FMS CUSTOMER CONCERNS**

Now, what about the FMS customer who still relies on a U.S. system that is no longer in active use by the U.S. government? The daunting workload involved in fixing mission critical U.S. systems means few, if any, government resources can be assigned to fix systems not in use by U.S. forces. A new FMS case may be required to obtain the needed support. If an open systems sale case has a line for maintenance support, it may be faster to request Y2K analysis and support through the existing line. Regardless of the choice of contractual vehicles (new or existing FMS case), there will be a cost associated with the work effort unless the Case Manager included Y2K in the pricing of the original Letter of Offer and Acceptance (LOA).

FMS customer concerns and questions can be expected in two main areas: weapon systems and logistics systems. There is a lot of information available in both areas at each military department's Y2K web page. Specific weapon system questions should be sent by normal channels to the Implementing Agency's Case Manager. See the following sidebar for a list of useful Y2K web sites. Finding solutions to meet FMS customer needs will ultimately be a team effort that involves the SAO, the customer country, MILDEP case managers, System Project Offices, DSAA, and a variety of commercial firms.

The average FMS customer faces an even more complex problem than many U. S. military units. Many FMS customers are operating "mixed source" systems. For example, an air-to-air missile purchased under an FMS case and delivered by an aircraft purchased through direct commercial channels with ground control system support and data inputs provided by a third-country system. Data requirements to launch a missile could be coming from the aircraft or ground systems. Who is responsible for ensuring the system as a whole is Y2K compliant? The FMS customer has overall responsibility for the entire system, but what company or agency can totally certify that a given sub-system is Y2K compliant when the external data stream from other systems may be non-compliant? If telemetry data can't be loaded to the missile after January 1, 2000, the system as a whole won't work. Even if the missile, aircraft,

---

and all supporting systems are Y2K compliant, what happens if the computer used at the in-country repair facility produces errors during maintenance and/or testing of components? All it takes is for one link in the chain of parts, sub-systems, procedures, and processes to fail, and the entire system may fail. Variations of this type of dependency scenario exist almost everywhere.

### *Year 2000 Web Sites*

The Y2K problem has an unyielding deadline. This deadline combined with Internet technology has resulted in a lesson in applied information distribution. Government and business web sites specifically geared to the Y2K problem are being updated frequently . . . as new "best practices" are identified and tools are developed. Some useful web sites used to research this article are:

DoD: <<http://www.disa.mil/cio/y2k/cioosd.html>>  
Army: <<http://imabbs.army.mil/army-y2k>>  
Navy: <<http://www.doncio.navy.mil/y2k/>>  
Air Force: <<http://infosphere.safb.af.mil/~xpsm/frmain.htm>>  
GSA: <<http://www.itpolicy.gsa.gov/mks/yr2000/y201toc1.htm>>  
GAO: <<http://www.gao.gov>>  
Business: <<http://www.year2000.com>>

Each site contains useful policy and tool information as well as an extensive index of resources.

Several FMS logistics information systems will need to be changed, even though there are plans to ultimately replace them with the Defense Security Assistance Management System (DSAMS). Some of these systems provide and/or accept information from FMS customers through another system, Supply Tracking and Repairable Return (STARR/PC). STARR/PC, in turn, requires the Defense Automated Addressing Office (DAASO) communications interface package known as DAAS Automated Message Exchange System (DAMES) in order to pass information back and forth. Both the STARR/PC and DAMES managers report that their respective systems are currently year 2000 compliant. For DAMES, this includes both the DOS and Windows versions. Further details on STARR/PC system compliance can be obtained from the United States Air Force Security Assistance Center (AFSAC). The AFSAC STARR/PC Points of Contact are Carol Healey, Susan Weeks, or Mark Minch at 937-257-5760, DSN 787-5760. DAMES questions should be addressed to Robert Durham, DAAS-SF at 937-656-3848, DSN 986-3848.

Even if all the USG applications and commercial off-the-shelf software are Y2K compliant, it doesn't mean the system will actually work after January 1, 2000. Older personal computers (PCs), especially those manufactured prior to 1995, often have problems handling the shift to the year 2000. It's recommended that every PC be tested to see if the system clock will rollover correctly to the year 2000 (see the following sidebar, "Personal Computer Systems Year 2000 Issues"). There have been recent cases reported of people buying a new computer that was erroneously claimed to be Y2K compliant. It is better to test the PC now and make sure that any applications subsequently loaded onto the machine are in compliance. This statement holds true regardless of the customer, organization, or application.

Security Assistance Offices (SAO) use several Security Assistance information systems. Users of the Training Management System (TMS) have already experienced some Y2K

---

problems with “fifth quarter” 1999, e.g., first quarter of fiscal year 2000. The DISAM TMS point of contact, Mr. Tom Dop, says that TMS can and will be made Y2K compliant as soon as the legacy systems feeding Integrated Standardized Training List (ISTL) data are Y2K compliant. Multiply this kind of interaction by over 3,962 DoD systems deemed “mission critical,” and the magnitude of the Y2K problem becomes apparent.

The Security Assistance Automated Resource Management System (SAARMS) uses a “runtime” version of Microsoft Access as the database engine. “SAARMS will have to be updated to reach Y2K compliance,” says DISAM’s Ernie McCallister, but the “work effort will be at DISAM and the SAOs will just have to update a new version of SAARMS after we re-write the program. We’ll meet the deadline.”

If your office or parent organization has developed any “in house” programs using Microsoft (TM) products, it’s a good idea to pay a visit to the Microsoft Y2K home page at <<http://www.microsoft.com/win32dev/guidelns/getready.htm>>. This site has specific information about what versions will be or currently are Y2K compliant.

### HOW DO WE FIX IT?

The Department of Defense management plan lays out a five phase process to be used on the Y2K problem: *Awareness, Assessment, Renovation, Validation, and Implementation*. These phases are being used by virtually every United States Government agency working on the problem.

The *Awareness* phase runs throughout the entire process, and this article is an example of trying to get the word out to all concerned.

The military departments have nearly completed the *Assessment* phase—what systems need to be changed and what will it cost? The May 1997 cost estimate to correct 3,962 “Mission Critical” DoD Information Systems was \$2.8 billion, and this cost estimate is expected to increase as managers get a better handle on the scope of the problem.<sup>4</sup> The deadline for corrective action is fixed, and qualified personnel resources are scarce. In May, 1997, the U.S. government identified 7,649 mission critical systems, and this doesn’t include the Social Security Administration’s 29,139 information system “modules.” Then there are state government systems, business Electronic Data Interface (EDI) systems, communications systems, etc.

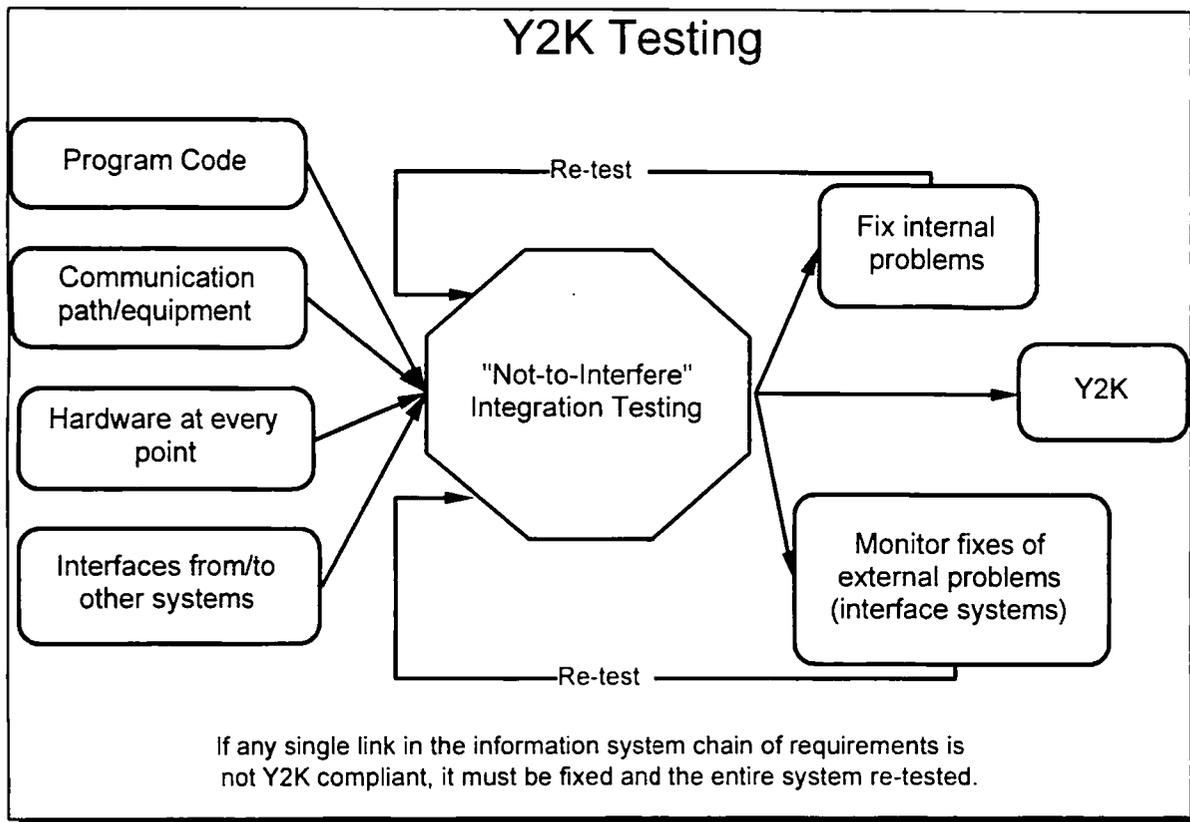
The *Renovation* phase consists of systems replacement, retirement, or conducting repairs to ensure Y2K compliance. DoD has 582 systems that are already Y2K compliant. Another 473 systems are to be replaced, 487 systems are to be retired, 2,752 systems need to be repaired, and a decision has yet to be made on 141 other systems.

*Validation and Implementation* phases will consume up to 50 percent of the time needed to correct the problems. The length of validation testing is due in part to the complexity of the data interchanges between systems. The problem is complicated further because not every system will be updated simultaneously. So the implementation plan must be designed to deploy in a computing environment that is “mixed” (some systems Y2K compliant but others not compliant). There will also be a number of systems that cannot be fully tested without first finding additional computing capacity. For example, not many of us could partition our PC’s

---

<sup>4</sup> Office of Management and Budget report to Congress, June 23, 1997. URL for full text of report is <<http://cio.fed.gov/yr2krev.htm>> (2 Sep 1997).

hard drive and duplicate our entire operating system and applications for test purposes. Similarly, few information systems are operating at less than 50 percent of machine capacity.



A well designed assessment phase will reveal each particular system's unique issues and challenges. But what questions need to be asked? FMS customers will find a particularly useful list of assessment questions at [http://www.mitre.org/research/cots/Y2K\\_QUESTIONS.html](http://www.mitre.org/research/cots/Y2K_QUESTIONS.html). A generic "Risk Assessment" document can be found at <http://www.navy.mil/y2k/risk.html>. This document gives an excellent overview of the areas of Y2K concern and a management approach to assess the impact of the Y2K problem. Another guide (GAO/AIMD-10.1.14) can be found at the General Accounting Office web site <http://www.gao.gov>. Another option for Y2K assessment is to have an outside contractor conduct an assessment and provide recommendations and cost estimates for corrective actions.

The Defense Information Systems Agency (DISA) maintains a "compliance catalog" that permits a search of both hardware and software vendors who have provided information about their products and/or services. This page is updated weekly and is hosted at [http://www.mitre.org/research/cots/COMPLIANCE\\_CAT.html](http://www.mitre.org/research/cots/COMPLIANCE_CAT.html).

## CONTINGENCY PLANS

Any user of an information system should develop a contingency plan in case the needed Y2K fixes cannot be accomplished in time. Even if one system is Y2K compliant, the users need a contingency plan that covers the possibility of system crash from non-compliant system data. While a contingency plan is required for DoD agencies, it's a good idea for FMS customers too. They face the additional problem of integrating U.S. systems with those produced in other countries.

## *Personal Computer Systems Year 2000 Issues*

The DOS operating system gets the date and time from the hardware clock when the PC is booted, but DOS maintains its own system clock after boot-up. Many PCs will not handle the rollover to the year 2000 correctly. If the PC has the wrong date, then applications will also have the wrong date. To test a PC, execute the following tests (these tests assume you are using DOS 5 or 6, whose DATE command also sets the real-time clock):

- DOS clock rollover:
  - Using the DOS Date and Time commands, set the date to 12-31-1999 and set the time to 23:59.
  - Verify the date and time.
  - Leave the PC on.
  - Wait 1 minute.
  - Check the date and time; it should be 1-1-2000 and a few seconds after midnight.
- Hardware clock rollover:
  - Using the DOS Date and Time commands, set the date to 12-31-1999 and set the time to 23:59.
  - Verify the date and time.
  - Turn off the PC.
  - Wait 1 minute.
  - Turn on the PC.
  - Check the date and time; it should be 1-1-2000 and a few seconds after midnight.
- Hardware clock setting:
  - Using the DOS Date and Time commands, set the date to 1-1-2000 and set the time to 1:00.
  - Verify the date and time.
  - Turn off the PC.
  - Wait 30 seconds.
  - Turn on the PC.
  - Check the date; it should still be 1-1-2000.
  - You might also try this with 2-29-2000 and 1-1-2001.

All PCs should pass the DOS clock rollover test, but many fail the hardware clock rollover test. If a PC fails the hardware clock rollover test, but passes the hardware clock setting test, then you should be able to manually correct the date on 1-1-2000. But if a PC won't let you set the date correctly, then you will have to check into the problem more carefully. It may be that a BIOS upgrade will fix the problem, or you may have to set the date in DOS each time the PC is booted.

Courtesy of: <[http://sun35.npt.nuwc.navy.mil/nss\\_secr/year2000/pc2000.html](http://sun35.npt.nuwc.navy.mil/nss_secr/year2000/pc2000.html)>

## **NEW PROCUREMENTS**

It is one thing to fix existing systems to ensure they will work in the year 2000, but what about new procurements? The Acquisition Council and the Defense Acquisition Regulations

---

Council have adopted a new rule that amends the Federal Acquisition Regulation (FAR) to increase awareness of Year 2000 procurement issues and to ensure that solicitations and contracts address Year 2000 issues. The new rule<sup>5</sup> is effective October 21, 1997, and addresses the following:

- Defines “Year 2000 compliance.”
- Requires new contract solicitations for IT to include the Y2K compliance statement.
- Recommends that agency solicitations *describe existing information technology that will be used with the information technology to be acquired.*
- Requires the contracting officer to *identify whether the existing information technology is Year 2000 compliant.*

Unfortunately, one effect of this rule may be to cause delays in awarding contracts unless the contracting office has already been provided with the required information about existing IT. Another impact that Case Managers will need to discuss with customers involves increased costs to the FMS case.

### WHO IS GOING TO FIX IT?

The Assistant Secretary of Defense [(Command, Control, Communications, and Intelligence (ASD/C3I)], as Chief Information Officer (CIO) of the Department of Defense, will oversee the DoD’s solution to the Y2K problem. ASD/C3I promulgated the Year 2000 DoD Management Plan in April, 1997. This plan “applies to all interfaces between the DoD and external organizations, including other Government agencies, the private sector, non-profit organizations, allies, coalition partners, NATO and other alliances.”<sup>6</sup> ASD/C3I plans on co-hosting a NATO/Allied Y2K Interface Assessment Workshop in the near future.

If a customer desires support for an obsolete system, a request should be made for an FMS case, or for an amendment to an existing case. For Security Assistance policy questions, send an e-mail to DSAA’s Mr. Joe Irwin, <joe.irwin@osd.pentagon.mil> or Lt. Col. Mike Clements <mike.clements@osd.pentagon.mil> .

There is a lot of information freely available on the Y2K problem. There are many technological, policy, cost, and personnel constraints on developers, owners, and consumers of information systems as we attempt to beat the Y2K deadline. While the Y2K challenge poses many threats, it also presents an opportunity to replace or update obsolete systems. There are many questions yet *unasked* in addition to *unanswered* questions. Stayed tuned for further developments!

### ABOUT THE AUTHOR

LCDR Berdahl has been a faculty member at DISAM since August, 1996. He is DISAM’s lead instructor in providing DSAMS training to the military departments. LCDR Berdahl is a 1996 graduate of the University of Georgia’s Master of Business Administration program with concentrations in MIS and Decision Support Systems. He has been actively involved in providing DSAMS training to the military departments.

---

<sup>5</sup> The full text of the new Y2K Federal Acquisition Regulation (FAR) rule (48 CFR Parts 39 and 52) can be found at <<http://www.itpolicy.gsa.gov/mks/yr2000/finalfar.htm>>.

<sup>6</sup> Op. Cit., DoD Y2K Management Plan, p. 2.