



UNITED STATES MARINE CORPS  
MARINE CORPS COMBAT DEVELOPMENT COMMAND  
QUANTICO, VIRGINIA 22134-5001

MCCDCO 5000.5  
B 50  
10 Sep 98

MARINE CORPS COMBAT DEVELOPMENT COMMAND ORDER 5000.5

From: Commanding General  
To: Distribution List

Subj: YEAR 2000 (Y2K) MANAGEMENT PLAN

Ref: (a) DoD Y2K Management Plan  
(b) CMC 0507322 Mar 98  
(c) MCCTA 2008202 Feb 98  
(d) CMC 2907302 Dec 97  
(e) CMC 1116002 May 98

Encl: (1) Year 2000 Websites  
(2) Year 2000 Points of Contact  
(3) USMC Inspector General Year 2000 Checklist  
(4) Year 2000 Compliance Checklist  
(5) Microsoft Products: Compliant/Compliant with Minor Issues  
(6) Sample Software Certification Request Letter  
(7) Year 2000 Contingency Plan for [System Name]  
(8) List of Internal and External Interfaces  
(9) Year 2000 Instructions

1. Purpose. To outline the plan for assessing the impact of the Y2K on all MCCDC information systems. The Y2K Management Plan establishes procedures for conducting system inventories, prioritizing, providing updates of systems, and monitoring progress. The Communication Electronics Division (CED), MCB, Quantico, is assigned the responsibility for oversight of Y2K awareness, assessments, renovations, validations, and implementation of systems within MCCDC.

2. Background

a. The term Y2K is used to describe the potential failure of information technology (IT) systems before, on or after 1 January 2000. This problem is primarily due to the use of two-digit year indicator within software code (in either applications, operating systems, hardware or microchips). In the Year 2000, non-compliant systems will likely interpret "00" as "1900" rather than "2000." Compounding the problem is the unusual and unrelated fact that the Y2K is also a leap year.

b. The Assistant Secretary of Defense for Command, Control, Communications, Computers and Intelligence (C4I) has the

10 Sep 98

responsibility to lead DoD efforts to solve the Y2K problem. In this effort, a DoD Y2K Management Plan (reference (a)) has been developed. Per reference (b), that plan serves as the basis for the MCCDC Y2K effort as well as that for the Marine Corps by providing Y2K centralized management and decentralized execution. The Marine Corps Y2K Website (enclosure 1) contains over 80 naval messages that amplify or provide additional guidance.

c. The Marine Corps Y2K Executive assigned overall responsibility for Y2K problem resolution is the Assistant Chief of Staff (AC/S) for C4I/Chief Information Officer (CIO).

d. The Quantico Y2K process begins with a thorough assessment of existing systems. This includes both software and hardware systems spanning over three decades of IT development. The goal is to have all MCCDC systems certified as Y2K compliant and implemented by 30 March 1999. Mission critical systems must be Y2K compliant NLT 31 December 1998. This will be accomplished through the elimination, replacement, or modification of existing systems. A system is certified as compliant when it can accurately process date/time data over the century change and leap year calculations. A system is not Y2K compliant if another system exchanging data with it is not also Y2K compliant.

### 3. Information

a. Scope. All MCCDC divisions will comply with this management plan. CED will coordinate Y2K actions with MCCTA, MARCORSYSCOM, MCAF, and other tenant commands aboard MCB, Quantico. This plan applies to IT support to include hardware, firmware, data, and developed software to include Commercial Off the Shelf (COTS), Government Off the Shelf (GOTS) packages, operating systems, third and fourth generation language compilers and interpreters, functional applications, system utilities, translators, and database management systems. Data includes databases, files, and other data storage structures and mechanisms, data and system interfaces and interchanges, Electronic Data Interchange transaction sets and implementation conventions, and other messages or forms of data exchange.

b. Goals and Objectives. The goal of the MCCDC Y2K Management Plan is to minimize system failures due to Y2K related problems and to ensure proper contingency planning is executed. The objectives include:

(1) Minimize the adverse impact of Y2K date processing in all mission critical and mission support systems.

(2) Identify and share consistent strategies for finding and fixing Y2K problems and testing solutions.

(3) Minimize duplication of effort for Y2K problem identification and resolution.

10 Sep 98

(4) Minimize the impact of resource reallocation to support Y2K efforts.

(5) Minimize risk and cost in determining the appropriate Y2K solution for each system.

(6) Identify, prioritize, and mobilize needed resources for system conversions and replacements.

c. Manasement Strategy. Quantico has adopted the DoD Y2K Management Strategy which uses a five phase process:

- Awareness. This phase focuses on promoting Y2K awareness.
- Assessment. This phase consists of system inventory and problem assessment.
- Renovation. This phase consists of systems replacement, retirement, or modifications to ensure Y2K compliance.
- Validation. This phase focuses on testing systems for Y2K compliance and interoperability.
- Implementation. The final phase is Y2K compliant system deployment and continuous monitoring.

(1) Information Sharing. To reduce duplication of effort, information on Y2K problems, best practices, and lessons learned are to be actively gathered and distributed to all divisions and commands aboard MCB, Quantico. Through diligent screening of Y2K web pages, open lines of communication with Y2K Action Teams (aboard Quantico and within Headquarters Marine Corps), and attendance at conferences and working groups, information can be gathered that could minimize efforts. Enclosure (1) lists Y2K informational **websites** and enclosure (2) is a list of Y2K points of contact.

(2) Resourcing. Nonessential software sustainment requirements, enhancements, preplanned product improvements, and change request proposals should be closely scrutinized until all systems have been analyzed, fixed, tested, and verified to be Y2K compliant. Funds intended for these activities should include consideration of the Y2K effort.

(3) Prioritization. Systems that are critical to the support of warfighting and peacekeeping missions and those that affect the health, safety, or security of individuals shall receive priority for conversion and replacement. Systems which feed data into Enterprise Systems (e.g., MCTFS, SABRS) should also receive priority for assessment and correction of identified Y2K problems.

10 Sep 98

(4) DoD Standard Date Format. DoD components will use a four-digit contiguous year for the year portion of dates used for interfaces among systems and in all interagency information exchanges. The four-digit date format is required for systems interfaces and data exchanges in DoD to reduce the risk of re-infection of Y2K problems in DoD systems and databases. If the system does not perform manipulations with the date, it is not necessary to convert to a four-digit year. For example, an alpha roster simply lists the date but does not use it for any computation. However, all non-compliant systems must be marked as such regardless of prioritization.

(5) System Elimination. Legacy systems or systems that can be combined into other systems should be considered for termination where possible. This opportunity should be taken to eliminate unnecessary systems from the inventory.

(6) Replacement Alternatives. Whenever practical, Y2K compliant COTS or GOTS products should be used to replace a system that has Y2K problems. Another replacement alternative is to rapidly redevelop the system through rapid application development, rapid architect application development, Business Process Reengineering, or object technologies and methodologies.

d. The Five Phase Management Process

(1) The Awareness Phase. This is the first phase of the MCCDC Y2K Management Plan and focuses on promoting Y2K awareness. The purpose of this phase is to familiarize all personnel with the scope of possible Y2K impacts, to define the problem, to establish a Y2K Action Office, to decide on an overall approach, and to obtain high level management support. There is a need for an initial awareness phase and sustained awareness throughout the Y2K compliance process. Enclosure (3) is the Inspector General Y2K checklist.

(a) Define the Problem. It is necessary to clearly define the Y2K problem before it is possible to bring awareness to the problem. (See background paragraph 2).

(b) Establish a Y2K Action Office. CED, MCB, Quantico will establish a Y2K Action Office. Each MCCDC organization at the division level will establish a Y2K point of contact. The first objective of the Y2K Action Office will be the development of detailed plans outlining how the divisions will assess and resolve their Y2K problems.

(c) Identify Technical and Management Representatives. These representatives should include system managers, budgeting **and** resource personnel, legal representatives, senior management, support contractors, and other external contacts.

10 Sep 98

(d) Desktop and Distributed Computing Systems. The interfacing and data exchange between various distributed computing systems must be addressed for Y2K problems to ensure proper data handling and conversion. Dependency links between internal and external systems must be identified.

(e) DoD Contracts. All contracts will conform to the following principles:

- Purchase only Y2K compliant products. This applies to all DoD purchases by any acquisition method, including orders placed under contracts or schedules issued by other agencies as defined in Federal Acquisition Regulation (FAR) Part 39.002.
- Use Y2K compliance language in contracts.
- Issue stop work orders on all contracts for new products being purchased on existing contracts that fail to meet Y2K requirements.
- Contracting offices will request contractors develop a Y2K compliance plan to upgrade their Y2K non-compliant products.

(f) Y2K Compliance Certification. System developers/maintainers and functional managers will certify and document each system's Y2K compliance. Enclosure (4) is a compliance checklist to aid system managers. Marine Corps Y2K policy has directed that orange stickers or tags be placed on all systems to indicate that the system is Y2K compliant. One possible source for procuring tags is from the GSA catalogue. White labels may be purchased and an orange marker can be used to color the tag. The NSN for the white labels is 8135-00-178-9152. The NSN for the orange marker is 7520-00-079-0286. Refer to the Marine Corps Y2K Website (Y2K.CIO.USMC.MIL) for further guidance on Y2K tagging procedures. Reference (c) applies. Each sticker must contain the following information:

- Date checked.
- Method used to determine compliance.
- POC/Section.

(2) Assessment Phase. This is the second phase of Y2K Management Plan. It deals with those activities required to define the scope of the problem and set up the infrastructure necessary to solve it. The primary purpose of this phase is to gather and analyze the compliance checklist, cost factors, list interfaces, and draft contingency strategy plan in order to determine the size and scope of the problem. The determination of the size and scope is critical to the estimation of the cost in terms of dollars and manpower.

10 Sep 98

(a) Code Inventory. The code inventory involves locating all the programming codes that must be modified for the Y2K. The volume and type of code will determine the magnitude of the problem. Source code may be housed in a single repository or decentralized and spread over the work force. All codes must be inventoried and tracked and their relationship to other codes determined. A total count of the lines of code will assist in determining how many and what type of resources will be required in order to make the changes.

(b) Assessment Survey. An assessment survey can be used to gather the necessary information about source codes which are not contained in a central repository. It will also aid in the identification of COTS products that may be embedded within other products. The survey process seeks to collect system data in a standard format in a central database or spreadsheet. Collecting this data is critical to future efforts such as prioritizing and scheduling systems for renovation. Every system, including those currently selected for migration or retirement, must be inventoried.

(c) Missing Source Code. Missing source code increases both the scope and cost of the project because it requires time and resources to develop both the functional specifications and program specifications in order to rewrite the missing modules. Unfortunately, every piece of code must be fully examined for Y2K compliance. This may require the recreation of a source code. To lessen the impact of this problem, assess if the system is truly mission critical or if there is a replacement system already in development. If the impact of the loss of the system is high, the code must be recreated. Functional managers must coordinate with the appropriate sponsors for the source code. CED is not responsible for collecting source codes.

(d) Mapping Source to Executables. Source codes must be mapped to the executable code to ensure the source code in the inventory corresponds to the executable code running in production. There are commercial products available to help in this task; otherwise, the task must be performed manually. Again, this is time and manpower intensive and provides another reason to reduce unnecessary or redundant systems.

(e) Vendor Software. All operating system software and program products that surround the application software may need to be updated. A comprehensive list of vendor software must be compiled and compared against either commercial databases of Y2K compliant software or by comparing against CMC, CIO Y2K Advisories. It is important to remember when using vendor provided information that it is necessary to determine the vendor's definition of Y2K compliant. Often the vendor refers to software as Y2K compliant but this means a patch to the software must be purchased to make it compliant. Enclosure (5) is the comprehensive list of Microsoft compliant products. It is important to notice that Microsoft labels its

non-compliant components as "compliant with minor issues." These products are non-compliant. Enclosure (6) is an example letter for software certification from vendors.

(f) Contingency Plans. Realistic contingency plans must be developed on all systems that may potentially not meet the Y2K deadline. All critical level/class I systems must have a contingency plan to alleviate the risk associated with the Y2K problem. These contingency plans should be robust and maintainable and should be updated at each phase. Enclosure (7) is an example of a contingency plan for an information system. This contingency plan is not relevant to all systems and should only be used as guidance.

(g) External Interfaces/Trading Partners. System interfaces and trading partners are critical considerations in Y2K compliance. An external interface is any aspect of a system that sends and/or receives information from another system outside the control of the Marine Corps system owner. Y2K compliance issues with external interfaces and trading partners can cause systems to fail even if the Marine Corps system is Y2K compliant. For example, in the facilities area, if a base/station receives electrical power from a local utility, and that local utility experiences a failure due to Y2K problems, the Marine Corps base/station will be affected. Even if the Marine Corps utility distribution systems are Y2K compliant, they still may not be able to distribute electrical power because of Y2K failure of external trading partners. For this reason, it is essential that all external trading partners associated with the base/station's mission-critical systems be identified and analyzed as part of the inventory process. Enclosure (8) is an example spreadsheet for recording internal and external interfaces. For system interfaces and external trading partners, the following steps need to be taken:

- Identify all system interfaces and trading partners that may affect a mission-critical system.
- Contact all trading partners and identify POCs.
- Ensure that the trading partner's renovation approach and overall Y2K issues are consistent with the Marine Corps' compliance strategy.
- Exchange appropriate documentation and/or develop a Memorandum of Understanding to document potential issues and their resolution.
- Track the status of renovation activities with external trading partners as appropriate
- Address failure of external trading partners in contingency planning scenarios.

10 Sep 98

(3) Renovation Phase. This phase involves making and documenting software and hardware changes, developing replacement systems, eliminating systems, and updating contingency plans. At all times, system interdependencies must be considered. A system is not Y2K compliant if another system feeding data into it is not also Y2K compliant.

(a) Data Sources. It is important to remember to ensure all internal and external data sources are Y2K compliant. It may be necessary to develop bridges to convert data or filters to edit out data that is not compliant.

(b) Replacement. Ensure replacement products are Y2K compliant including their ability to handle leap year calculations. For products that are purchased, contract specialists and legal staff need to review contracts and warranties.

(c) Configuration Management. Use configuration management procedures to ensure all changes are properly tracked.

(d) Testing. Testing is likely the most important stage of the Y2K process and the most involved. Unit, integration and system tests should be conducted after each application and module is completed. Ensure all components of the system are tested to include bridges and filters. Test cycles must include time for regression testing (selective retesting to detect faults introduced during modification of a system). CED will coordinate with commands for testing methodology.

(e) Share Information. Disseminate lessons learned and best practices. This information will be continually gathered by CED and passed on to each Y2K POC.

(f) Repairing. This involves the conversion or repair of an existing system. In converting application systems, consider changes in operating systems, compilers, utilities, domain-specific programming products, and commercial database management systems. The common Y2K fixes are listed below; however, local Automated Information Systems that trade data with other organizations need to ensure that data is transmitted in identical formats.

1 Field Expansion. Changing two-digit year values to four-digit values throughout a system.

2 Sliding Window. Use of a 100-year window to convert data and codes to the appropriate century, to include 1999 and 2000.

3 Procedural Code. Any of the following methods.

a Encapsulation or data fake.

b Compiler modification.

10 Sep 98

c Manipulation of object code.

d Data bridges and filters.

e Combinations.

(4) Validation Phase. This phase requires extensive integration and acceptance testing of all converted and replacement systems.

(a) Test Facilities. In some cases, it may be necessary to run parallel systems implemented in a Y2K test facility to prevent production cycles from being disrupted. These test platforms must have realistic production-sized databases and multiple versions of application software to ensure a full, robust test.

(b) Test Plans and Schedules. Must be developed and documented.

(c) Contracting Conversions. If conversions are contracted out, the effort must be closely managed to ensure the contractor follows the Y2K conversion standards. It is necessary to ensure proper Y2K language is provided for in the contract. The converted system must be fully tested and certified by the same checklists as for non-contracted conversions.

(d) Perform Testing. It is important to define, collect, and use test metrics to manage the testing and validation process. Testing can not be performed arbitrarily. At a minimum, the National Software Testing Laboratories (NSTL) Y2K compliance test must be conducted on all PC's. Enclosure (9) is a list of instructions for the NSTL Y2K Test and a spreadsheet for recording the data.

(5) Implementation Phase. After testing is completed, compliant systems must be implemented. Since it is likely that not all system components will be completed simultaneously, components must be able to operate in a mixed environment of Y2K compliant and non-compliant applications. While reintroducing components into the environment, system interdependencies must be taken into consideration. Parallel processing is strongly recommended.

(a) Transition Environment and Procedures. Transitioning from the current environment to a Y2K compliant environment requires extensive planning. Some considerations:

1 Operating systems, database, utilities and other COTS products may not be available until late 1998 or early 1999.

Note: It is important to back up all data and installed software on Mission Critical Systems prior to conducting Y2K compliance tests.

10 Sep 98

2 External data suppliers may not complete their conversions and testing until 1999.

3 Testing, validation and correction processes may last through most of 1998 and possibly into 1999.

(b) Disaster Recovery Plans. All critical Y2K compliant systems will have disaster recovery plans for the restoration of operations and data in case of extended outage, sabotage or natural disaster. This should include converted and replaced systems and related databases.

(c) Post Implementation Considerations. Although the implementation phase is the final phase of the Y2K Management Plan, systems should be closely monitored beyond the end of the phase. Contingency plans should include the possibility of unforeseen problems which result in the expenditure of additional funds. All verified Y2K problems should be documented and tracked.

## 5. Action

a. C4I (CIO). Reference (d) established the AC/S C4I, as the Marine Corps-wide Y2K Executive, responsible for oversight on all Y2K related issues. AC/S C4I will direct this in the capacity of the CIO of the Marine Corps.

b. (I&L) LFF Facilities. Per reference (e), (I&L) LFF Facilities has been designated as being responsible for facilities infrastructure oversight. Oversight is defined as responsible for functional/departmental coordination including service-wide and external Y2K reporting.

c. Director, CED, MCB, Quantico. Serves as the Quantico Y2K Executive and has the overall management responsibility for MCCDC Y2K issues. CED will be responsible for any network infrastructure device that CED has installed or currently operates aboard MCB, Quantico.

d. Y2K Action Office. Located within CED, MCB, Quantico, oversees progress and provides Y2K guidance for Information Systems Technology while gathering and reporting information regarding the Y2K status of facilities. The office coordinates the efforts with tenant commands/organizations at MCB, Quantico.

e. Quantico Y2K Advisory Group. Assists the Y2K Action Office in the resolution of cross-functional Y2K issues and facilitates the sharing of information within Quantico. Initially each MCCDC division shall provide a representative to the advisory group to provide recommendations and avoid duplication of effort. The advisory group will develop standardized tools and an approach for testing, training, and progress.

f. Individual MCCDC Divisions/Commands. All MCCDC divisions/commands and selected tenant commands aboard MCB, Quantico will designate an IT Y2K POC. IT Y2K POC will do the following:

(1) Prepare and execute a Y2K oversight program for systems under their control.

(2) Identify and prioritize mission critical systems in support of their organizations.

(3) Discontinue or replace application systems as needed.

(4) Monitor Y2K corrections for systems under their control.

(5) Make resource decisions and develop strategies for systems with Y2K problems.

(6) Purchase and develop only Y2K compliant systems.

(7) Include Y2K compliant language in all new contracts and contract modifications.

(8) Beginning 1 September 1998, submit a Y2K status report on the first Monday of each month to the Y2K Action Office, (SSgt Keith Dubay, [SSgtDubay@the-Pentagon.com](mailto:SSgtDubay@the-Pentagon.com)) including an overall appraisal of the situation, major concerns, and recommendations.

g. The following are specific Y2K responsibilities:

(1) MCCDC CDC ISMO. Responsible for overall CDC actions. POC is Captain Dennis J. Hart at DSN 278-6018.

(2) MARCORSYSCOM. Responsible for all devices past the demarc point (data/voice PBX) or fiber patch panels. POC is Joann A. Bernier at DSN 278-3643 (CSI).

(3) MCU. Responsible for all their own systems with the exception of four Bay 5000 switches in Bldg. 2076. POC is 1stLt Robert E. Freeland at DSN 278-5785 (C40IT).

(4) T&E Division. Responsible for all systems past the demarc point (data/voice PBX) or fiber patch panels with the exception of one centillion 100 switch in Bldg. 1019 and one centillion 100 switch in Bldg. 2006. POC is 1stLt Barry A. Dowdy at DSN 278-2999 (C46DL).

(5) MCWL. Responsible for all systems excluding the CED CISCO, 7513 router in Bldg. 3255 and phone switches. POC is Cpl Jason A. Wiltrout at DSN 278-1384.

MCCDCO 5000.5

10 Sep 98

(6) MCAF. Responsible for all systems excluding the demarc point (phone switch, PBX, etc.) or fiber patch panels. POC is CW03 Taninecz at DSN 278-1464 (143-4).

(7) MSTP. Responsible for all systems excluding the demarc point (phone switch, PBX, etc.) or fiber patch panels. POC is Capt Heidi J. McKenna at DSN 278-2853.

(8) Facilities. All facilities and Base infrastructure related components are the responsibility of Facilities Division. Related actions will be coordinated with CED. The facilities POC will:

(a) Prepare and execute a Y2K oversight program for systems under their control.

(b) Identify and prioritize mission critical systems in support of local commanders.

(c) Ensure Y2K compliance of facility related information systems as needed (i.e., climate control, elevators, etc.)

(d) Monitor Y2K corrections for systems under their control.

(e) Make resource decisions and develop strategies for systems with Y2K problems.

(f) Purchase and develop only Y2K compliant systems.

(g) Include Y2K compliant language in all new contracts and contract modifications.

(h) Develop facilities Y2K Plan with milestones geared to specific requirements. POC is Mr. Herlan at DSN 278-5102 (B041-7).

h. MCCDC Y2K Timeline

(1) Phase I (Awareness)

Completion Date: 1 September 1998 (in progress)

-- End State

- Completed and distributed MCCDC Y2K Management Plan.
- Individual division's strategies developed.
- Y2K POC's identified and educated.
- System users and owners identified and educated.

10 Sep 98

- Phase II strategy developed.
- Phase II plan completed and distributed.
  - (2) Phase II (Assessment)
    - Completion Date: 1 November 1998
    - End State
- 100% inventory of all systems: 1 October 1998.
- Phase III strategy developed.
- 100% of systems to be replaced, redeveloped and/or retired are identified and confirmed.
- 100% of systems analyzed for Y2K compliance.
- 100% of systems requiring renovation are prioritized and scheduled for Phase III.
- Identify critical funding requirements.
- Risk management and contingency strategy developed, documented, and distributed.
- Phase III plan completed and distributed.
  - (3) Phase III (Renovation)
    - Target Completion Date:
      - Mission critical systems: 31 December 1998
      - All other systems: 30 March 1999
    - End State
- Phase IV strategy developed.
- Implementation of selected renovation strategy for all scheduled systems.
- Risk management and contingency strategy updated.
- Phase IV plan completed and distributed.

MCCDCO 5000.5

10 Sep 98

(4) Phase IV (Validation)

Target Completion Date: 1 May 1999

-- End State

- Phase V strategy developed.
- Unit, integration, and system testing completed, systems certified.
- Acceptance testing and certification completed.
- Phase V Plan completed and distributed.

(5) Phase V (Implementation)

Target Completion Date: 1 June 1999

-- End State

- Risk management and contingency strategy updated and distributed.

(6) Information systems will be monitored on a continuous basis up to and after 1 January 2000. Y2K issues will be addressed in an expeditious manner by the MCCDC Y2K Action Office and the individual divisions.

  
J. N. STROCK  
Chief of Staff

DISTRIBUTION: A

# Year 2000 **Websites**

## **Marine Corps Year 2000 website-**

[http://issb-www1 .quantico.usmc.mil/year2000/frames/index.html](http://issb-www1.quantico.usmc.mil/year2000/frames/index.html)

## **DoD Y2K Management Plan website-**

<http://www.dtic.mil/c3i/y2k/title.html>

## **Vendors**

### **Hardware**

Compaq- <http://www.compaq.com/support/files/index.html>

Dell- <http://www.us.dell.com/filelib/>

Everex- <http://www.everex.com/>

IBM- <http://www3.software.ibm.com/download/>

Micron- [http://www.micronpc.com/support/file\\_lib/file.html](http://www.micronpc.com/support/file_lib/file.html)

Cisco- <http://www.cisco.com/warp/public/752/2000/>

### **Software**

Microsoft- <http://www.microsoft.com/year2000/>

Banyan- <http://www.banyan.com/html/download.html>

Lotus- <http://www.lotus.com/home.nsf/tabs/y2k>

NSTL- <http://www.nstl.com/html/y2klogo.html>

### **Other informational websites**

U.S. Army Material Command website- <http://www.monmouth.army.mil/y2k/y2khome.htm>

Navy [http://www.doncio.navy.mil/y2k/year\\_2000.htm](http://www.doncio.navy.mil/y2k/year_2000.htm)

Army <http://imabbs.army.mil/army-y2k>

Air Force <http://infosphere.safb.af.mil/~jwid/fadl/world/y2k.htm>

Link Center-<http://pw2.netcom.com/~helliott/00.htm>

Compliant Bios- [http://www.mitre.org/research/cots/COMPLIANT\\_BIOS.html](http://www.mitre.org/research/cots/COMPLIANT_BIOS.html)

10 Sep 98

## Year 2000 Points of Contact

### **CG MCCDC**

Captain Dennis J. Hart  
CAPT DENNIS J HART@HQTRSMCCDC@MCCDC  
Phone 278-6018

### **MARCORSYSCOM**

GS13 JoAnn A. Bernier  
GS13 JOANN A BERNIER@IS@MARCORSYSCOM  
Phone 278-2408

### **T&E Division**

1stLt Barry A. Dowdy  
1STLT BARRY A DOWDY  
Phone 278-2999

### **MCWL**

Sgt William F. Parker  
SGT WILLIAM F PARKER@CMCLAB@MCCDC  
Phone 278-1384

### **MCU**

1stLt Robert E. Freeland  
1LT ROBERT E FREELAND\_JR@MCRC.MCU@MCCDC  
Phone 278-5785

### **MCAF**

Captain Jorge L. Medina  
CAPT JORGE L MEDINA@OPS@MCAF QUANTICO  
Phone 278-1464

### **MSTP**

Captain Heidi J. Mckenna  
MCKENNAH@MSTP.QUANTICO.USMC.MIL  
Phone 278-2853

### **Facilities**

Mike Herlan  
MR MIKE HERLAN@FAC MAINT@MCB QUANTICO  
Phone 278-5 102

### **CED/ISMO**

SSgt Keith L. Dubay  
SSGT KEITH L DUBAY@ISMO@MCB QUANTICO  
Phone 278-2033

ENCLOSURE (2)

10 Sep 98

## USMC Inspector General Year 2000 Checklist

			Major Subordinate Commands, 11 Mar 1998
Inspection Item	Yes	No	Comments
Have points of contact been assigned in writing?			0507322 MAR 98 AND ALMAR 436/97, par 4.J
Who is the point of contact for your organization?			0507322 MAR 98 AND ALMAR 436197, par 4.5
Will that point of contact be here in the year 2000?			0507322 MAR 98
Is the Year 2000 the number one priority?			0507322 MAR 98
Is the Year 2000 point of contact a full time representative or is this a collateral duty?			0507322 MAR 98
Do you have a Year 2000 Management Plan?			ALMAR 436/97, par 4.B
Does the plan relate to the DoD Y2K Management Plan?			DOD Y2K MGT PLAN, par 7.4
Does the plan assign responsibilities within your organization?			ALMAR 436/97, par 4.B
Does the plan establish clear deadlines?			DOD Y2K MGT PLAN, par 8.2-8.6
Have you prioritized your systems as to their criticality?			DOD Y2K MGT PLAN, par 3.1, par 4.1
Are the most critical systems receiving priority attention?			DOD Y2K MGT PLAN, par 4.1

ENCLOSURE (3)

Are the most critical systems receiving priority attention?			DOD Y2K MGT PLAN, par 4. I
What is your number of critical systems?			DOD Y2K MGT PLAN, par 4.1 AND ALMAR 436/97, par 4.C
Is there a service wide Year 2000 point of contact?			ALMAR 436/97, par 1
Who is the service wide Year 2000 point of contact?			ALMAR 436/97, par 1
Who do you receive Year 2000 information from?			ALMAR 436/97, par 3.A
Who do you pass Year 2000 information to?			050732Z MAR 98, par 5.F
Who does the Year 2000 point of contact report to within your organization?			ALMAR 436/97, par 4.B
Is there a process to track and validate data submitted by subordinate units?			ALMAR 436/97, par 4.B
Is the component providing adequate quarterly data to higher headquarters?			050732Z MAR 98, par 5.F
Have all the systems been checked for year 2000 compliance?			DOD Y2K MGT PLAN, par 3.1 AND 050732Z MAR 98, par 5.A
For non-compliant systems, is there a completed contingency plan?			081405ZDEC97, par 2, 3.A AND DOD Y2K MGT PLAN, par 4.18

Is your organization aware of the testing available at the Joint Interoperability Test Command (JITC)?			190755ZDEC97, Par 1-3
--	--	--	-----------------------

10 Sep 98

Are there adequate resources to solve the problem?			DOD Y2K MGT PLAN, par 3.1
Have appropriate funds been diverted to solve the Year 2000 problem?			DOD Y2K MGT PLAN, par 3.1, 4.6 AND 181520ZJUN97, par 2
Is there a budget shortfall?			DOD Y2K MGT PLAN, par 7.4
Was that shortfall reported to the CIO's office?			050732Z MAR 98, par 5.F, AND ALMAR 436/97, par 4.G
What is the impact of the Year 2000 fixes on your normal operating and maintenance budgets?			050732Z MAR 98, par 5.G AND 051300ZJAN98, par2
What would you have done differently if additional funds were available?			050732Z MAR 98, par 5.I
Were there existing contracts available for Year 2000 work?			301450ZDEC97, par 1 AND DOD Y2K MGT PLAN, par 4.14, 4.15
Did you use the existing contracts?			301450ZDEC97, par 1 AND DOD Y2K MGT PLAN, par 4.14, 4.15
Are you currently buying any information technology products that are not Year 2000 compliant?			301450ZDEC97, par 1 AND DOD Y2K MGT PLAN, par 4.14, 4.15
Do you have legal recourse for non-compliant items that you may have purchased?			050732Z MAR 98, par 6.E AND DOD Y2K MGT PLAN, par 4.15
Have the commands checked the BIOS on there PC's?			270905ZOC97, par 3
How many 286 PC's total?			050732Z MAR 98 par 6.f, AND 270905ZOC97, par 3

10 Sep 98

How many 386 PC's total?			050732Z MAR 98 par 6.f, AND 270905Z OCT97, par 3
How many 486 PC's total?			050732Z MAR 98 par 6.f, AND 270905Z OCT97, par 3
How many 286 PC's are non-compliant?			270905Z OCT97, par 3
How many 386 PC's are non-compliant?			270905Z OCT97, par 3
How many 486 PC's are non-compliant?			270905Z OCT97, par 3
Do you have plans to replace or fix all non-compliant computers prior to the Year 2000?			270905Z OCT97, par 4
How many Pentium's do you have total?			270905Z OCT97, par 4
How many Pentium's are non-compliant?			270905Z OCT97, par 3
Do you have plans to replace or fix non-compliant Pentiums prior to the Year 2000.			050732Z MAR 98 par 6.f, AND 270905Z OCT97, par 3
Do you have any locally developed or purchased COTS packages that are non-compliant?			141906Z JAN98, par 2
Have you solicited the vendor for certification letters?			141906Z JAN 98, par 2
Have you assessed your telecommunications devices and developed a plan to replace or repair all non-compliant devices?			050732Z MAR 98, par 5.D
Have you looked at your routers?			221550Z JAN98, par 7

ENCLOSURE (3)

Number non-compliant and cost to fix?			
Have you looked at your hubs? Number non-compliant and cost to fix?			04 16 15ZFEB98, par 6
Have you looked at your bridges? Number non-compliant and cost to fix?			231530Z FEB 98, par 3
Have you looked at your faxes? Number non-compliant and cost to fix?			18 1400Z FEB 98, par 3
Have you looked at your data switches? Number non-compliant and cost to fix?			181010Z FEB 98, 181020Z FEB 98, 181030Z FEB 98
Have you assessed possible infrastructure and facilities Year 2000 problems, and are you tracking those issues with Facilities?			050732Z MAR 98, par 5.F.5
Has facilities checked your heating and air conditioning units? Number non-compliant and cost to fix?			051645ZFEB98, par 3
Have the power distribution systems been checked? Number non-compliant and cost to fix?			051645ZFEB98, par 3
Have the security and alarm systems been checked? Number non-compliant and cost to fix?			051645ZFEB98, par 3
Have the water and sewage service systems been checked? Number non-compliant and cost to fix?			051645ZFEB98, par 3
Is your IT equipment properly tagged?			200820Z FEB 98, par 3

**YEAR 2000 COMPLIANCE CHECKLIST**

**The purpose of this checklist is to aid system managers in ensuring that their systems are compliant for the Y2K. Make sure the following items are included in your Y2K testing and compliance process for all of the developed, gratis, licensed, and purchased software, hardware, and firmware used in your system's operation, development/maintenance, support, and testing activities,**

Y2K compliant system accurately processes date/time date from, into and between the twentieth and twenty-first centuries and the leap year calculations. Finally, "compliant" systems have no extended semantics, calendar errors, date overflow, and inconsistent semantics.

Please respond to each question with the appropriate answer.

**System Identification**

*(An asterisk indicates an optional question)*

B. 1 .Please provide system information.

a.	Name of system	
b.	Defense Integration Support Tools (DIST) Number of system	
c.	Operational date of system (current or a future date)*	
d.	Planned or actual replacement date of system (retirement or discontinuation qualifies as replacement)*	
e.	For planned replacements what is the contingency plan and under what conditions will it be invoked?*	
f.	What are the safety critical portions of the system, if any?*	

B.2. Each system has its own window of time, before and after the present date, in which it functions. Planning and scheduling systems work with dates that are weeks, months, and sometimes years in the future. Likewise, trend analysis systems and billing systems regularly reference dates in the past. For your system, and its window of time, please verify its ability to successfully process data containing dates with no adverse effect on the application's functionality and with no impact on the customer or end user beyond adjustment to approved changes in procedures and data formats.

	VERIFIED	NO	N/A
a. Dates in 20th century (1900s)			
b. Dates in 21st century (2000s)			
c. Dates across century boundary (mix 1900s and 2000s)			
d. Crosses 1999 to 2000 successfully			

**Other/Indirect Date Usage**

B.3. Have you verified performance (and corrected if necessary):

	VERIFIED	NO	N/A
a. Dates embedded as parts of other fields			
b. Dates used as part of a sort key			
c. Usage of values in date fields for special purposes that are not dates (e.g. using 9999 or 99 to mean "never expire")			
d. Date dependent activation/deactivation of passwords, accounts, commercial licenses			
e. Date representation in the operating system's file system (creation dates and modification dates of files and directories)			

f.	Date dependent audit information					
g.	Date dependencies in encryption/decryption algorithms					
h.	Date dependent random number generators					
i.	Date dependencies in firmware					
j.	Personal Computer BIOS and RTC does not reset the year to 1980 or 1984 on reboots <b>after</b> 31 December 1999 ( <i>corrections by operating system utilities allowed</i> )					

**Leap Year**

B.4. System accurately recognizes and processes Year 2000 as a leap year.

		VERIFIED		NO		N/A
a.	February 29, 2000 is recognized as a valid date					
b.	Julian date 00060 is recognized as February 29, 2000					
c.	Julian date 00366 is recognized as December 31, 2000					
d.	Arithmetic operations recognize Year 2000 has 366 days					

**Usage of Dates Internally**

B.5. Internal application usage of dates and date fields must be clear and unambiguous in the context of the systems which use them.

		VERIFIED		NO		N/A
a.	Display of dates is clear and unambiguous (the ability to correctly determine to which century a date belongs either by explicit display, i.e. 4-digit year, or system or user inference)					

b.	Printing of dates is clear and unambiguous					
c.	Input of dates is clear and unambiguous					
d.	Input of logically correct dates					
e.	Storage of dates is clear and unambiguous		I	I		

**External System Interfaces**

B.6. External interactions are identified and validated to correctly function for all dates

		VERIFIED		NO		N/A
a.	Interaction between this system and any other external time source, if existing, has been verified for correct operation.					
	For example, the GPS system is sometimes used as a time source. Many GPS receivers cannot correctly deal with the roll-over of the GPS 10-bit epoch counter that will occur at midnight, 21 August 1999. GPS receivers also deal with an 8-bit Almanac Week counter which has a 256 week roll-over span.					
b.	You and the responsible organization for each interface have negotiated an agreement dealing with Year 2000 issues.					
	For example, is the interface currently Y2K compliant. is it being worked on, does it have an unknown fix date, or will it be fixed by a future date you have mutually agreed					
	011					
	<b>For each interface that exchanges date data, you and the responsible organizations have discussed and verified that you have implemented consistent Year 2000 corrections that will correctly work for date data passed between your systems.</b>					

**Date Field Type**

**B.7. Describe** the type of date fields used by the system, in either software or data bases.

		VERIFIED		NO		N/A
a	Does the system use 4 digit year data fields?					
b	Does the system use 2 digit year data fields?					
c	If 2 digit, does the system use a century logic technique to correctly infer the century?					
d	At what date will the century logic fix fail?					
				YES		NO
e	Are there any internal data types for dates?					

If yes to e, what is the range of dates that the date field can represent?

Minimum Date		Maximum Date	
--------------	--	--------------	--

Year 2000 Testing Information

B.8.Optional: Please provide the following information for all year 2000 compliance tests that are conducted, i.e. system test, integration test, acceptance test:

		Narrative Answer		
a.	Testing Organization			
b.	Name of Test Team Chief			
c.	Date that Year 2000 compliance testing was completed			
d.	How was Year 2000 compliance determined? (certified by vendor or contractor. tested in-house, inspected but not tested. etc )			
		YES		NO
e.	Are the test data sets available for regression testing on the next version release for questions 2. 3. 3. 5. 6. 7d. and 7e?			
f.	Are the detailed test results and reports available for review and audit for questions 2. 3. 3. 5. 6. 7d. and 7e?			
g.	Do you follow a defined process for tracking the status of all Year 2000 problems reported. changes made, testing, compliance, and return to production?			

B.9.Optional: Please provide the following information with regard to COTS/GOTS components

		YES		NO		N/A
a.	Does the system use COTS/GOTS application packages and/or infrastructure components?					
b.	If yes, have those items been verified to be Year 3000 compliant?					
		Narrative Answer				
c.	How was Year- 2000 compliance determined? (certified by vendor or contractor, tested in-house, etc.)					

10 Sep 98

B. 10 Certification levels are defined below. Yes, verified and N/A are considered positive responses. No is considered a negative response.

LEVEL

- 0 System retired or replaced
- 1 Full independent testing completed with either:
  - All questions have positive responses except possibly 7b or
  - All questions have positive responses except possibly 7a
- 2  Independent audit of system and existing testing completed with either:
  - All questions have positive responses except possibly 7b or
  - All questions have positive responses except possibly 7a
- 3  Self-certification  
CAUTION: Self-certification assumes a higher risk level of potential failures
- 3a Self-certification with full use of 4 digit century date fields
  - All questions have positive responses except possibly 7b
- 3b Self-certification indicates risk due to use of 2 digit century fields
  - All questions have positive responses except possibly 7a
- 3c Self-certification indicates risk due to ambiguous usage of dates
  - Question 5-a,b,c or d have negative responses.
- 3d Self-certification indicates potential problems (System needs additional work before Year 2000 processing can be assured with any level of reliability)
  - Question 2-a,b,c or d have negative responses, or-
  - Question 3-a,b,c,d,e,f,g,h,i or j have negative responses, or
  - Question 4-a,b,c or d have negative responses, or-
  - Question 5-a,b,c or d have negative responses, or
  - Question 6-a or b have negative responses, or
  - Question 9-b has a negative response.
- 4 Not certified or not certified yet.

**B. 11 It would be advisable but not required for the system/program/project manager to have the responsible programmer(s) fill out a similar checklist covering the software they are responsible for before completing this checklist for the overall application.**

**LEVEL OF CERTIFICATION FOR THIS DATA SYSTEM: (*Circle only one*)**

**01233a3b3c3d4**

I certify that the information provided above is true and correct to the best of my knowledge and belief

ADDITIONAL,  
COMMENTS: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_  
System Manager Date

I certify that the information provided above is true and correct to the best of my knowledge and belief:

ADDITIONAL  
COMMENTS: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_  
System Customer Date

10 Sep 98

**Microsoft Products:  
Compliant / Compliant with Minor Issues**

Access 97 v. 8.0	Compliant
<b>ADO</b> v. 1.0 - 1. 5	Compliant
Bookshelf 98	Compliant
Encarta Encyclopedia v. 1998	Compliant
Encarta Reference Suite 98	Compliant
Encarta Virtual Globe	Compliant
Excel 95 v. 7.0	Compliant
Excel 97 v. 8.0	Compliant
Excel 98 (Mac)	Compliant
Excel v. 5.0	Compliant
Exchange Server 5.5	Compliant
<b>FoxPro</b> v. 2.6	Compliant with minor issues
Frontpage 98	Compliant
IntelliPoint (2-Button Mice) v. 1.1 c, 1.1 d	Compliant
IntelliPoint (Wheel Mice) v. 2.0, 2.0a, 2.1, 2.2	Compliant
Internet Explorer (16-bit) v. 4.01	Compliant
Internet Explorer (32-bit) v. 3.0, 3 .O 1, 3.02	Compliant with minor issues
Internet Explorer (32-bit) v. 4.0, 4.01	Compliant with minor issues
Internet Explorer (Mac) v. 4.0a, 4.01	Compliant
Internet Explorer (UNIX) v. 4.0	Compliant
MS-DOS 6.22	Compliant with minor issues
<b>NetShow</b> , <b>Netshow</b> Theater, ACM v. 3.0	Compliant
Office (Mac) 98	Compliant
Office 4.x Standard Edition	Compliant with minor issues
Office 95 Professional Edition	Compliant with minor issues
Office 95 Standard Edition	Compliant with minor issues
Office 97 Professional Edition	Compliant
Office 97 Standard Edition	Compliant
Office 98 (Mac)	Compliant
Outlook 97 v. 8.0, 8.01, 8.02 and 8.03	Compliant
Outlook 98 v 8.5	Compliant
Outlook Express (Mac) v. 4.0	Compliant with minor issues
Power Point (Mac) 98	Compliant
<b>PowerPoint</b> 95 v. 7.0	Compliant
<b>PowerPoint</b> 97 v. 8.0	Compliant
<b>PowerPoint</b> v. 4.0	Compliant with minor issues
Project 98, 98 SR-1	Compliant
SQL Server 6.5 Enterprise, Small Business Server	Compliant with minor issues
Systems Management Server v. 1.2	Compliant
<b>Visual Basic</b> v. 5.0, 4.0, 3.0, 2.0, 1.0	Compliant with minor issues

ENCLOSURE (5)

MCCDCO 5000.5  
10 Sep 98

Visual C++ Professional, Learning Edition v. 5 .O	Compliant with minor issues
Visual FoxPro v. 3 .Ob	Compliant with minor issues
Visual FoxPro v. 5.0a	Compliant
Visual Source Safe v. 5.0	Compliant with minor issues
Visual Studio Enterprise v. 5 .O	Compliant with minor issues
Visual Studio Professional v. 5.0	Compliant
Windows 95 v. 4.00.950	Compliant with minor issues
Windows for Workgroups 3.11	Compliant with minor issues
Windows NT Server, Standard / Enterprise v. 4.0	Compliant with minor issues
Windows NT Workstation v. 4.0	Compliant with minor issues
Word (Mac) 98	Compliant
Word 95 v. 7.0	Compliant with minor issues
Word 97 v. 8.0	Compliant
Word v. 6.0	Compliant with minor issues

**Microsoft Products:  
Non-compliant**

Access 2.0	Not-compliant
Word for MS-DOS v. 5.0	Not-compliant
Office Professional v. 4.3 (Access 2.0 only)	Not-compliant

ENCLOSURE (5)

**Sample Software Certification Request Letter**

[CONTRACTOR'S NAME]

Attn: [POC]

[ADDRESS]

[CITY, STATE, ZIP]

Dear { POC } :

[YOUR UNIT NAME] is a current licensee of your product (see enclosure) either purchased or maintained under contract number [CONTRACT NUMBER].

We are currently canvassing our software suppliers to determine if their products will **function** properly when processing dates, regardless of century. Our Year 2000 (Y2K) vendor compliance language is [DEPENDING ON YOUR COMPLIANCY LANGUAGE.. , **INTERNAL REPRESENTATION OF DATES, TIMES AND DATE/TIME GROUPS IS VENDOR DEPENDENT, BUT SHALL BE CONSISTENT WITH THE REQUIREMENT OF APPLICATIONS AND FUNCTIONS THAT MANIPULATE DATES AND TIME, INCLUDING COLLATING SEQUENCES USED IN SORTS AND MERGES COMPUTATION OF TIME PERIODS; TIME BEFORE OR AFTER A SPECIFIC TIME, DATE, OR DATE/TIME GROUPS SUCH AS DETERMINATION OF VALID DATES OR DETERMINATION OF LEAP YEARS, OR OTHER SIMILAR TYPES OF FUNCTIONS. VENDORS SHALL PROVIDE EVIDENCE THAT SOFTWARE ACQUIRED UNDER THESE PROVISIONS PERFORM ACCORDING TO THESE SPECIFICATIONS, AND SHALL WARRANT THE OPERATION OF SUCH SOFTWARE FROM THE DATE OF SALE**].

It is our intention to migrate to an environment which will achieve compliance with the ISO Date Standard (ISO Date Standard 8601). Furthermore, it is our intention to only use or retain **software** which is warranted by the supplier as having the capability to process all date data with no adverse impacts, including dates which cross century bounds.

We request you provide in writing, within 30 days of receipt of this letter, the current status of your software products in regard to the **Y2K** issue discussed above. If the product is not currently compliant, we request a date when the software will be compliant. If compliance requires a specific release/version of your product, we request that the release date at which compliance is achieved be specified and when the government will be provided the update under the purchase/maintenance contract.

In a related matter, we plan to test our applications for **Y2K** compliance. We plan to set up a test environment, **advance** the date to 1999/2000 and test our applications to determine what problems may exist. In the past we have found that some of our vendor-supplied products have internal expiration dates. If internal expiration dates exist in your product, we request that you provide us with a means to use your product in an environment with a system date set in the future (1999/2000 timeframe). We view the matters described in this letter to be within the scope of your existing maintenance contract or license/warranty provisions provided to the government. All concerns should be in writing and addressed to the Contracting Officer.

Compliance with requests in this letter are within the scope of the maintenance contract of license/warranty provision that is currently in force. Should you disagree, take no action except to inform the Contracting **Officer** of your position and detail the rationale supporting your stance.

POC in this matter is the below signed **officer** [YOUR NAME AND TELEPHONE NUMBER].

Sincerely,

[YOUR NAME]

[TITLE]

ENCLOSURE (6)

**YEAR 2000 CONTINGENCY PLAN FOR**  
**[SYSTEM NAME]**

1. **PURPOSE.** The purpose of this Contingency Plan is to provide instructions if the *[System Name]* fails to operate before, on, or after January 1, 2000. This document will attempt to address the major scenarios that are possible, and will focus on those scenarios that critically impact the ability of this system to perform in the manner it was designed.

2. **GENERAL/IMPACT.** *[Explain briefly in this paragraph what the system does, who does it support, what are some of the junctions that are provided to the user, and other capabilities that the user has through use of the system.]*

*Explain what type of conversion was made to the system for the year 2000. Explain what type of failure might occur. For example :*

*“The *[System Name]* has been changed to expand the date fields to an eight digit year. However, the possibility exists that the system could fail before, on, or after January 1, 2000. This failure could be total or partial and could result in the disruption of *[reports, database updates, etc.]*. Each failure situation would require differing levels of response and will be evaluated upon occurrence. This is a dynamic document and will be adjusted as necessary. It requires establishment of a *[core team or responsible person]* to perform the necessary functions to fix the system problems, and if necessary, direct *[state alternative method for processing, maybe use of another system, manual processing, etc.]*“.*

3. **RESPONSIBILITIES**

3.1 *[Functional Manager or organization that OWNS the system].*

3.1.1 *[State responsibilities of the owner of the system. For example:]*

*[Title of person or organization]* is responsible for developing and managing the Contingency Plan if it must be invoked. This person should also be prepared to make resource decisions should this system fail. The *[core team or responsible person]* will work closely with the Functional Manager.]

3.2 *[Software maintenance organization or developer].*

3.2.1 *[State responsibilities of developer or maintainer. For example:]*

*[Title of person or organization]* is responsible for providing input into this Contingency Plan, programming changes, testing and implementation.

3.3 *[User/Customer]*

3.3.1 *[State responsibilities of user/customer. For example:]*

*[Title of person or organization]* is responsible for providing input into this Contingency Plan, directing installation of any changes to the system in hardware or software upgrades, directing installation of new releases of the system, and any provided training necessary due to upgrades.

3.4 *[Contractor, if applicable]*

3.4.1. *[State contractor responsibilities].*

4. **CRITERIA FOR PLAN ACTIVATION.** This plan will be activated when it becomes apparent that a major process will not execute correctly as a direct result of date processing problems. These processes include *[daily, monthly cycle, etc.]*,

10 Sep 98

5. PROCEDURES FOR INVOKING CONTINGENCY MODE. *[State who is responsible for invoking this Contingency Plan, who is responsible for **notifying** users that the system is down (titles and **organization**), and who should be notified. If you provide a list of customers at paragraph 8, you can refer to that.]*

6. POSSIBLE SCENARIOS. Due to the level of effort and attention given to resolving problems, any given problem will be resolved in most cases prior to [30 days or minimum estimate] and in all cases no more than [45 days or maximum estimate].

*[Other scenarios may be added, choose those scenarios that are appropriate to your system.]*

6.1 Scenario 1: Hardware/operating system problems. Due to errors in the [system hardware, client-server or personal computer hardware], users are not able to run the system.

Action: *[State who should be contacted and course of action in case of hardware failure.]*

6.2 Scenario 2: Proprietary Commercial Off the Shelf/Government Off the Shelf software problems. Due to errors in the proprietary software or supporting utilities or tools, the system will not process correctly.

Action: *[State who should be contacted and course of action in case of software failure. State procedures for backing out of a process, instructions for backups, restores of data, and restart procedures. List any **processes** that must be performed manually or by alternative methods until the system is **fixed**. If the system is brought back up in stages, list processes that should **be fixed first**.]*

6.3 Scenario 3: Interfaces problems. Due to errors caused by data received or sent to interface systems, the system will not process correctly.

Action: *[State procedure to be followed to determine where the problem lies; provide procedures for backups, restores, restarts, and points of contact at interfacing organizations. List any processes that must be performed manually or by alternative methods until the system is **fixed**.]*

6.4 Scenario 4: Application code failure. Due to errors caused by code failure (programming error), the system will not process correctly.

Action: *[State procedures to validate code (**identify** code failure). State procedures for backing out of a process, instructions for backups, restores of data, and restart procedures. List any processes that must be performed manually or by alternative methods until the system is **fixed**. If the system is brought back up in stages, list processes that should **be fixed first**.]*

7. RESOURCE REQUIREMENTS. *[No additional resources or what additional resources] are necessary for operating in contingency mode. [State any requirements to pre-approve and pre-schedule additional working hours, pre-approve funds required, and who performs this **function**. State who would have the authority to release the resources.]*

8. CUSTOMERS. A list of customers is provided below for notification of system failure:

*[List customers and points of contact, if applicable.]*

9. CRITERIA FOR RETURNING TO NORMAL OPERATING MODE. Return to normal operating mode when system modification and testing is completed. *[Optional: **The functional** manager will conduct acceptance test to determine that the problem is corrected.]*

10. PROCEDURES FOR RETURNING TO NORMAL OPERATING MODE. Once the criteria is met for returning to operational mode, user/customers will be informed by [**functional** manager or person in authority] that the system is back up and begin using the system.

ENCLOSURE (7)



# Year 2000 Instructions

1. Close all programs\shut down services and turn off pc\server.
2. Insert 3.5" floppy into floppy drive.
3. Turn on pc\server.
4. Program will start running, press 'y' to start diagnostics.
5. Program will run. Annotate whether equipment is compliant on inventory sheet.(yes/no)
6. Take floppy out of floppy drive and reboot equipment.
7. Fill in inventory data on inventory sheet using the following:

**Serial Number,Bldg. #, Floor, Room #-**  
Self explanatory

**Equip Type-**  
Type of equipment being tested. (pc,server,router,fax,switch,etc.)

**OS-**  
Operating system-(win3.1,win95,win3.11,vines version,router IOS,etc.)

**Make-**  
Make of equipment being tested (Dell,Compaq,Zenith,Cisco,etc.)

**Model-**  
Model of equipment being tested (check on label)

**Compliant-**  
Passes/fails compliancy test (yes/no)

**Patch Need-**  
Patch needed to make **Y2K** compliant using the following-  
a - Win3.1/Dos upgrade  
b - Win3.11 Y2K patch  
c - Win95 Y2k patch

**Date-**  
Date tested

Put appropriate sticker on pc. For Orange sticker fill in the following-  
Date-Date Certified Year 2000 compliant  
Method-NSTL  
POC/Section-Name of **POC/Section**

ENCLOSURE (9)

