Office of Thrift Supervision
Department of the Treasury

John F. Downey
Executive Director, Supervision

1700 G Street, N.W., Washington, D.C. 20552

August 2, 1996

MEMORANDUM FOR: Chief Executive Officers

FROM: John Downey
Executive Director, Supervision

SUBJECT: FFIEC Statement on "Year 2000"

Enclosed is an interagency statement entitled, "The Effect of Year 2000 on Computer Systems" as approved by the Federal Financial Institutions Examination Council (FFIEC). The statement alerts you to various computer system risks that may arise from the forthcoming calendar rollover to the next century.

In addition to explaining the issues and apparent concerns, the document provides an action plan and guidelines that your institution should follow to ensure that computer systems will function properly and without disruption when the year 2000 arrives. Careful planning at this stage should help alleviate what could become significant problems in the future.

If you need further information or have any questions, please contact Mr. Paley Pang at (415) 616-1554 for assistance.

Attachment

Federal Financial Institutions **Examination Council**

Board of Governors of the Federal Reserve System
Office of the Comptroller of the Currency
Federal Deposit Insurance Corporation
Office of Thrift Supervision
National Credit Union Administration

2100 Pennsylvania Avenue, NW, Suite 200 • Washington, DC 20037 • (202)634-6526 • FAX (202)634-6556

Interagency Statement
June 1996 statement
other statements | home

THE EFFECT OF YEAR 2000 ON COMPUTER SYSTEMS

To: Chief Executive Officers of all Federally Supervised Financial Institutions, Senior management of each FFIEC Agency, and all examining personnel.

PURPOSE

This interagency statement alerts financial institutions to substantial risks to the industry represented by the programming code in existing computer systems as the industry enters the new millennium (year 2000).

BACKGROUND

The "year 2000" problem is pervasive and complex. Virtually every organization will have its computing operations affected in some way by the rollover of the two digit year value to 00. The majority of computer operating systems and programs currently in use have been developed utilizing six digit date fields (YYMMDD). For example, December 31, 1999, would be represented by "991231" in computer code. The two digit field for the year (in example "99") is the basis for all calculation formulas within most computer systems, particularly those processed through mainframes.

Up until now, this two digit field has sufficed, using a subtraction of current date from some future date (up to 12-31-99). As the industry enters the year 2000, the two digit field "00" will not permit accurate calculations based on the current formulas. January 1, 2000 would be read as 000101. Many computer systems will recognize this date as the year 1900. The potential impact is that date sensitive calculations would be based on erroneous data or could cause a system failure. This affects all forms of financial accounting (including interest computation, due dates, pensions, personnel benefits, investments, legal commitments). It can also affect record keeping, such as inventory, maintenance, and file retention. Reliable information is necessary for financial institutions to conduct business.

These coding changes impact billions of lines of program code, throughout government, banking, and all other users of computer technology. Most large financial institutions should be aware of this potential problem; however, industry estimates are that only 30 percent are currently addressing the issue. In some cases, individual financial institutions are projecting costs of $50 to $100 million over the next three years. Most vulnerable are the community financial institutions that do their own programming with in-house developed software systems. According to industry "guesstimates," costs to resolve these programming challenges worldwide will approach $600 billion (all computer systems, not just banking). Banking, however, is a heavily technology sensitive industry and will be impacted greatly.

CONCERNS

Many financial institutions, servicers, and vendors have not adequately addressed the risks

associated with the coming millennium. This lack of planning could result in the extended or permanent disruption of computer system operations. This may be the result of either the problem itself or the cost of fixing it.

Time is critical. Commitments to action and funding cannot be deferred, as the year 2000 is a finite date. This issue affects EVERY financial institution, whether processing information internally, through service bureaus, or a combination of both.

ACTION PLAN

Financial institutions should achieve year 2000 compatibility by performing a high level risk assessment of how systems are affected. This should be followed by the development of a detailed action plan. The board of directors and senior management should take the following steps in addressing this issue:

- Developing a risk assessment that identifies systems and applications that must be modified.

- Identifying the segments of computer systems that must be modified.

- Evaluating various alternatives (determining which applications should be redeveloped, replaced, or modified).

- Estimating costs for modifications.

- Reviewing, approving, and establishing milestones to ensure the timely completion of the institution's millennium plan.

- Ensuring that new systems are year 2000 compliant.

An institution should review all aspects of computer systems to include those provided by service bureaus, hardware vendors, and other software vendors. For any aspect of its information systems processing management must:

- Ensure that external vendors and servicers are adequately addressing the system and software issues related to the coming millennium.

- Ensure that the institution has taken adequate steps to ensure that critical operations will continue if the servicers or vendors are unable to achieve millennium requirements.

TESTING

All reprogramming efforts must be completed in time for adequate system testing. It is recommended that reprogramming efforts be completed by December 31, 1998. This will provide one full year for testing. It is important to note that all systems from mainframes to personal computers and local area networks are susceptible to the impact of year 2000 consequences.

The appendix to this issuance provides a suggested outline of the process that should be followed to ensure that issues concerning the millennium are addressed.

APPENDIX

Millennium Planning Process

I. Establish a Year 2000 Review Team
    A. Management should consider utilizing both internal and external information systems and audit resources to ensure that a risk-based Year 2000 Action Plan is developed.
    B. An inventory of all computer operating systems, applications and files should be created. All those with year 2000 issues must be identified.
II. Develop an institution wide year 2000 plan.
    A. The initial step in developing the plan should be to consider whether current systems and files should be modified, replaced, outsourced, or discontinued. It should be noted that even if new systems are purchased, old files may still have to be modified. (All computer systems, including mainframes, personal computers, local area networks, etc., should be considered).
    B. The year 2000 plan should also identify and prioritize applications and processes that are the most date sensitive and those which are most vulnerable. Interdependent applications should be grouped together.
    C. Management and the board of directors need to ensure that adequate funds and resources are allocated so that all year 2000 projects are completed in a timely manner.
III. Year 2000 Plan Implementation.
    A. Initiate pilot projects to test solutions to identified problems. It may be feasible to work with more than one vendor in order to evaluate their various solutions/capabilities before making a final decision.
    B. Begin the process of systematically implementing year 2000 changes by priority in accordance to risk. These projects should be conducted within the framework of the system development life cycle process currently in place.
    C. Conduct post implementation reviews to ensure the integrity and functionality of the modified systems.

▲Return to top | other statements | press release | home