Federal Financial Institutions **Examination Council**

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

August 31, 1998

Questions and Answers Concerning FFIEC Year 2000 Policy

To: The Board of Directors and Chief Executive Officers of all federally supervised financial institutions, service providers, software vendors, federal branches and agencies, senior management of each FFIEC agency, and all examining personnel.

The Federal Financial Institutions Examination Council (FFIEC) has issued eight interagency statements concerning the Year 2000 project management process and other significant Year 2000 issues. The guidance covers examination procedures and project management, institution due diligence in connection with Year 2000 readiness of service providers and software vendors, the Year 2000 impact on customers, testing for Year 2000 readiness, contingency planning, and customer awareness. The purpose of this guidance is to answer commonly asked questions and clarify previous FFIEC Year 2000 policy statements, rather than introduce additional expectations.

Q.1. What is the FFIEC's general policy regarding testing for financial institutions that rely on service providers or software vendors for mission-critical products and services?

A.1. The FFIEC recognizes that each financial institution is unique. Management should determine the best testing strategies and plans for its organization taking into account the size of the institution, the complexity of its operation, and the level of its business risk exposure to the Year 2000. The FFIEC also recognizes that there is no single approach to testing for the Year 2000. Options range from testing within a financial institution's own environment to proxy testing. How testing is conducted will depend on a variety of factors, including whether the testing is being conducted on software or services received from third parties, and the type of system or application to be tested.

Financial institutions should develop a written plan outlining their testing strategy and set testing priorities based on the risks that the failure of a system or function may have on its operations. The objective of a financial institution's Year 2000 testing strategy is to minimize business risk due to operational failures. Financial institutions should assign the highest priority to testing mission-critical systems, as the failure of mission-critical services and products almost certainly will have a significant adverse impact on the institution's operations and financial condition.

The FFIEC expects financial institutions to manage effectively the Year 2000 testing process, regardless of how individual systems are developed and operated. In practice, the controls necessary to manage the testing process effectively will differ depending on the design of the financial institution's system, interfaces with third parties, and the type of testing used.

The FFIEC expects service providers and software vendors to conduct extensive testing of their products and services prior to delivery to client financial institutions. In these cases, financial institutions that use these products and services may not need to duplicate the entire range of these tests. However, financial institutions should conduct tests (including future date tests) to ensure that these products and services will operate effectively in the institution's unique operating environment. (Refer to the answer to question two for a more detailed overview of the FFIEC's policy regarding proxy testing.)

Testing results must be assessed, documented, and approved by management, regardless of whether the testing was conducted by the institution in its own environment or through proxy testing. Ultimately, each financial institution is responsible for ensuring its readiness for the Year 2000.

Q.2. What is the FFIEC's policy regarding proxy testing for financial institutions that rely on service providers or software vendors for mission-critical products and services?

A.2. To the extent possible, financial institutions should test their systems in their own environment, because each financial institution is unique. However, the FFIEC recognizes it is not always feasible for financial institutions that rely on service providers (serviced institutions) or software purchased from vendors (turnkey institutions) to test in their own environment. For this reason, the FFIEC has expanded conditions under which proxy testing may be permissible to include both serviced and turnkey institutions. Financial institutions may rely on proxy tests conducted by service providers or user groups, as long as the tests are appropriate. These conditions apply to institutions that provide or receive services, regardless of any affiliations among those institutions (e.g., bank holding company affiliates). Institutions should consider the following conditions when evaluating the applicability of proxy testing of mission-critical systems.

Serviced Institutions. In proxy testing, the service provider tests with a representative sample of financial institutions that use a particular service on the same platform. Test results then are shared with all similarly situated clients of the service provider. Financial institutions that provide or receive data processing to or from affiliated institutions have the same responsibilities as any non-affiliated service provider or recipient institution. Institutions are encouraged to participate, to the extent possible, in the service provider's efforts to develop the scope of the test, test scripts, and the data used in the proxy testing.

To accept proxy testing conducted by service providers, an institution should consider the following conditions:

- Proxy tests are conducted with institutions that are representative of their institution (i.e., similar type and complexity);

- Proxy tests are conducted using the same version of Year 2000 ready software that will be used to service the institution.

- Proxy tests are conducted using the same hardware and operating systems that will be used by the

institution. Where there are differences, the institution should verify and document how the differences would not affect processing;

- Scope and objectives are defined by the users and are not structured or limited by the service provider;

- Test results are documented and validated; and,

- Test results are assessed to determine their reliability. This review should include relevant date related features, functions, options, and calculations.

For any customized software or services used, an institution should test relevant date dependent functions. A financial institution also should test systems and interfaces under its direct control and those functions not covered in the proxy testing. These include items unique to the institution, as well as those for which there are an insufficient number of common users to develop acceptable proxy tests.

Turnkey Institutions. The FFIEC "Guidance Concerning Testing for Year 2000 Readiness" outlined conditions for proxy testing with service providers only. Since the testing guidance was issued in April 1998, financial institutions and software vendors have sought FFIEC approval to expand proxy testing to include products provided by software vendors (turnkey software packages) to lessen the financial institution's burden and allow for increased efficiencies. The FFIEC now believes proxy testing can be acceptable for turnkey software packages under certain conditions. Financial institutions may work with other financial institutions through user groups, who can conduct proxy tests without the software vendor's participation.

To accept proxy testing of products provided by software vendors, an institution should consider the following conditions:

- Proxy tests are conducted with institutions that are representative of their institution (i.e., similar type and complexity);

- Proxy testing is conducted using the same software version that the institution will use in its production environment;

- Proxy tests are conducted using the same hardware and operating systems that the institution will use. Where there are differences, the institution should verify and document how the difference will not affect processing;

- The scope of the proxy testing is appropriate. This will require the institution to analyze which features of its mission-critical applications will be tested by the user group. Any date-dependent features used by a financial institution and not tested by the user group should be tested by the institution;

- Scope and objectives are defined by the users and are not structured or limited by the software vendor. A degree of independence from the vendors is necessary to ensure the validity of the tests. Vendors may, however, help the user group configure the equipment and software correctly and provide technical support;

- Test results are documented and validated; and,

- Test results are assessed to determine their reliability. This review should include the type of transactions performed by the financial institution, relevant date related features, functions, options, and calculations.

If the financial institution has modified the code provided by a software vendor, proxy tests cannot be used. The financial institution should test date-dependent functions of that customized software.

Financial institutions should test functions not covered by the proxy tests to ensure that they operate effectively in the institution's unique operating environment. Financial institutions are responsible for reviewing the testing documentation and comparing transactions it conducts to those tested. Any differences, with emphasis placed on those involving dates or date-related calculations, will require separate testing by the institution (e.g., the user group did not test the function that calculates interest on home equity lines of credit and the institution has home equity lines of credit).

Financial institutions should test interfaces between systems they operate, as well as interfaces with external entities with which they exchange information.

Q.3. Do financial institutions that rely on proxy tests have to conduct any additional testing?

A.3. Financial institutions that rely on proxy testing should test internal and external interfaces not covered in the proxy tests and other items under their control. Such items may include customized software applications and hardware configurations unique to the institution, and any hardware or software, including proof machines, reader/sorters, local area networks (LANs), personal computers (PC's), and automated teller machines (ATMs). Financial institutions are reminded that testing of environmental systems, including vaults, security systems, HVAC, etc., also should be included in their overall Year 2000 project plan.

Q.4. Should financial institutions participate in transaction testing efforts coordinated by industry trade associations and other organizations?

A.4. The FFIEC encourages financial institutions to participate in testing efforts coordinated by industry trade associations and other organizations. These testing efforts may provide an opportunity to conduct end-to-end testing of mission-critical transactions with other financial institutions and material third parties in a more cost effective manner than could be achieved on an individual basis.

Q.5. Should financial institutions hire outside auditors or consultants to verify their testing processes?

A.5. Financial institution management may use qualified independent internal parties or external parties to verify the testing process. If the financial institution lacks internal expertise, management should use other qualified professionals, such as management consultants or CPA firms, to provide an independent review. Verification of the testing process should involve the project manager, the owner or user of the system tested, and an objective independent party such as an auditor, consultant, or a qualified individual independent of the process under review. This objective verification should ensure that the testing process is effective, that key dates are checked, and that the changes made resulted in reliable information processing. If a financial institution is relying on proxy testing, management should ensure that an independent verification of the testing process, similar to the type described above, has occurred.

Q.6. May financial institutions use operating systems that are not Year 2000 ready?

A.6. The FFIEC strongly encourages financial institutions to use Year 2000-ready operating systems, because operating systems are central to computerized systems. Although there have been claims by particular software vendors that a non-compliant operating system can be used to run that vendor's software, a non-compliant operating system could cause a variety of problems. For example, the institution may have several programs purchased from different vendors interfacing with the non-compliant portions of the operating system. This interaction could cause or contribute to operational failures. Institutions also may find that non-compliant versions of operating systems may not be supported or maintained by the manufacturer or third party maintenance organization.

Q.7. Should a financial institution test its computer's system clock by rolling the dates forward without consulting with the manufacturer or vendor?

A.7. Financial institutions should work with the manufacturer or software vendor to determine the best and safest way to assure the equipment is Year 2000 ready. Rolling forward the dates on a computer without proper instructions could cause serious problems and should be done only after a careful analysis is made of the implications of such action. It is important to note that some of the problems caused by this type of testing may not be immediately apparent.

Q.8. May an institution test its remediated mission-critical applications at a hot-site location (disaster recovery site equipped with an appropriate computer and associated equipment)?

A.8. If an institution determines that the hardware and operating system used at the hot-site are the same as the hardware and operating system (type and version) used in-house, then the institution may test at its hot-site. If the hardware and operating systems are not the same as those used in-house, they may be used if the institution can demonstrate that the differences will not cause future processing problems. The hardware and software (including interfaces) running at the hot-site should be Year 2000 ready.

Q.9. Must institutions test all critical dates outlined in the April 10, 1998, FFIEC "Guidance Concerning Testing for Year 2000 Readiness"?

A.9. The FFIEC identified the critical dates in the "Guidance Concerning Testing for Year 2000 Readiness", because they are generally considered to be dates critical to banking applications. Testing of various dates may be waived, if they are not critical to particular applications. An institution may need to test critical dates that are not included in the FFIEC guidance given the characteristics of particular applications. In either case, a financial institution should document the critical dates tested and explain why they were chosen.

Q.10. Can testing be eliminated if the software uses an eight digit date field?

A.10. An eight digit date field does not relieve financial institutions, service providers, or software vendors from the need to test systems and applications or otherwise ensure that the financial institution's technical environment, including communications systems, software and hardware are Year 2000 ready. For a variety of reasons, the number of digits in a date field is not determinative of whether a system or application is Year 2000 ready. For example, data received from internal or external sources may not have an eight digit date field, and therefore, might not be compatible. The differences from incompatible date routines may not become apparent until testing is performed. Also an eight digit date field does not ensure accurate leap year processing. Another purpose of testing is to ensure that all date fields and date routines have been made Year 2000 ready. In addition, sometimes what appears to be an eight digit date field is not. Users may be required to enter eight digits, but the software may be dropping the century indicators and processing using only the remaining six digits.

Q.11. If a financial institution tests a particular software product in 1998 and receives an update to the product in 1999, does it need to test the updated version?

A.11. The following factors should be considered when determining whether an update, new release, or patch to a mission-critical software application or operating system should be re-tested thoroughly, partially, or not at all:

- The financial institution should consult with its service provider or software vendor to identify the types of changes made, and the extent to which the service provider or software vendor has conducted internal testing before releasing the updated product or service;

- If the changes do not affect date fields or date-related calculations, the financial institution may not have to test, other than to perform acceptance testing that would accompany the introduction of any software update, release, or patch; or new or updated operating system; and,

- If the changes affect date fields or date-related calculations, the financial institution should ensure the new release, update, or patch is appropriately tested, and that the service provider or software vendor has adequately documented and warranted the specific testing performed to ensure continued Year 2000 readiness.

As the Year 2000 approaches, financial institutions should carefully evaluate the benefits and risks of installing new software, software upgrades, or operating system upgrades given the potential Year 2000 complications.

Q.12. What testing documentation should financial institutions retain?

A.12. Management, in consultation with legal counsel, should retain appropriate documentation associated with Year 2000 efforts to demonstrate that they have fulfilled, or attempted to fulfill, their fiduciary, contractual, and regulatory responsibilities in the event of third party litigation. Financial institutions, in discussing document retention with their legal counsel, also should be aware that they must be able to present sufficient documentation to examiners to enable them to perform comprehensive Year 2000 examinations. The documentation retained should enable a reasonably knowledgeable person to understand what tests were performed, on what applications, systems, or hardware, what the results were, and how the results were validated. Testing documentation also could assist the institution in resolving issues that may occur after the century date change. The following list includes some of the testing documentation items that institutions should consider retaining:

- The organization's overall Year 2000 plan and its Year 2000 testing plan;
- The types of tests performed (e.g., baseline, unit, regression) and a summary of the results;
- The reason the institution chose the tests and how extensive those tests were;
- The criteria used to determine whether an application or system is Year 2000 ready;
- Plans for remediating and re-testing any computers, systems or applications that failed Year 2000 tests;
- The names of persons responsible for authorizing the testing plan and accepting testing results;
- Communications with service providers and software vendors, including assurances regarding their service or product; and,
- Any other documentation the institution believes supports their decisions and conclusions, as well as their due diligence effort.

Institutions with in-house data centers also should determine the appropriate extent to which they need to retain copies of the programs that produced the test results. These may be archived on storage media, such as disk, CD ROM, or tape.

Q.13. What should a financial institution do if its service providers or software vendors are not providing adequate information on their testing efforts?

A.13. The FFIEC expects service providers and software vendors to work with financial institutions and share adequate information on their testing efforts. In the event a financial institution encounters resistance, it should convey its concerns to its service provider or software vendor. It also may join forces with other institutions, as part of a user group, to exert collective pressure to improve the flow of information. If, after such efforts, an institution's service provider or software vendor continues to refuse or is unable to participate in Year 2000 readiness efforts, or if commitments to migrate software or replace or repair equipment cannot be made by certain "trigger dates" established by the institution, then the financial institution should implement its remediation contingency plans. Institutions should keep their primary federal regulator informed if any of the preceding situations occur.

Q.14. Does certification by a nationally recognized organization qualify as testing if the institution's program is reviewed by this organization?

A.14. Such certification is not a substitute for testing, because it generally involves only a review of the process and does not involve actual testing of applications and systems.

Q.15. What will the regulators stance be on institutions converting to a new mission-critical system in 1999?

A.15. Whether an institution converts to a new system in 1999 is a decision for the board of directors of that institution and may be appropriate in some circumstances. The risk resulting from a conversion will be assessed on a case-by-case basis.

Q.16. What should financial institutions do to ensure telecommunications and power companies are taking steps to deliver Year 2000 ready products and services? What is the FFIEC doing to ensure the appropriate government agencies address the Year 2000 problem with telecommunications and power companies?

A.16. Financial institutions, service providers and software vendors should contact their telecommunications companies and/or work through user groups to encourage telecommunications and power companies to provide information on their Year 2000 efforts and to coordinate testing.

The FFIEC has discussed concerns with the Congress, the President's Year 2000 Council, and the Federal Communications Commission and will continue its active involvement in these issues. Information on the efforts of the telecommunications and energy sectors can be found on the President's Year 2000 Council webpage (www.y2k.gov).

Q.17. What is the FFIEC's procedure for examining service providers and software vendors and distributing the results of the examinations to client financial institutions?

A.17. The FFIEC agencies examine certain service providers and software vendors. The first phase of examinations of service providers and software vendors using standardized examination procedures has been completed. Distribution of the Year 2000 reports on these companies has begun and will continue during the third quarter of 1998. The Year 2000 reports supplement, but are not a substitute for, a financial institution's due diligence efforts to monitor progress and obtain necessary information directly from its service providers and/or software vendors. The FFIEC agencies will continue to monitor service providers and software vendors Year 2000 preparedness on a quarterly basis. The examination and distribution processes for each are discussed below.

Large Service Providers and Software Vendors. The FFIEC has established a Year 2000 examination program for large service providers under the Multi-Regional Data Processing Servicers (MDPS) program and large software vendors under the Shared Application Software Review (SASR) program. Companies included in the MDPS and SASR programs process for, or provide software to, a large number of financial institutions that are regulated by more than one agency. Each of these companies potentially poses a high degree of systemic risk. As of June 30, 1998, there were 16 companies in the MDPS program and 12 financial institution software packages (sold by 11 different companies) in the SASR program.

The purpose of the FFIEC's Year 2000 reviews of MDPS and SASR companies is to ensure a degree of consistency among the FFIEC agencies relative to the Year 2000 reviews, to assign summary ratings, and to distribute report findings to client financial institutions. FFIEC agencies follow FFIEC examination procedures and use a specialized Year 2000 report format. The appropriate FFIEC agency will release Year 2000 examination reports from MDPS examinations to client financial institutions that are subject to the supervisory authority of each of the FFIEC agencies. Results of Year 2000 SASR reviews will be released by the FFIEC agency to client financial institutions if the software vendor consents. Disclosed information will be nonproprietary in nature and

only will discuss the FFIEC's overall assessment of the SASR's Year 2000 remediation process.

Independent Data Centers and Smaller Software Vendors. In addition to the examination of MDPS and SASR companies, the FFIEC agencies also examine other data centers and may examine some smaller software vendors using similar criteria as the MDPS and SASR reviews. The report format is similar to the MDPS and SASR reports and will be distributed by the responsible FFIEC agency in much the same manner.

Q.18. Should financial institutions hire outside parties to validate Year 2000 contingency plans?

A.18. The FFIEC expects that contingency plans be reviewed and validated by an independent party to ensure effectiveness and then be approved by senior management and the board of directors of the financial institution. The independent party may be an internal auditor, external auditor, qualified consultant, or a qualified person from an independent area within the institution. For additional information on contingency planning expectations, see the FFIEC "Guidance Concerning Contingency Planning in Connection with Year 2000 Readiness."

Q.19. Why can't service providers or software vendors distribute copies of their Year 2000 examination reports and ratings to client financial institutions?

A.19. Year 2000 examination reports are confidential and the property of each FFIEC agency. Service providers, software vendors, and their respective financial institution clients are reminded that they may not disclose publicly the contents of federal supervisory agency examination reports or reviews of the institution or any service provider or software vendor, including the confidential Year 2000 ratings contained therein. Financial institutions, service providers, and software vendors are not authorized to state and or make any statements that indicate or imply their Year 2000 plan or actual Year 2000 readiness has been approved or certified by a supervisory agency.