NATIONAL CREDIT UNION ADMINISTRATION

NATIONAL CREDIT UNION SHARE INSURANCE FUND

LETTER TO CREDIT UNIONS

1775 Duke Street Alexandria, VA 22314

DATE: July 8, 1998 LETTER: 98-CU-13

TO: FEDERALLY INSURED CREDIT UNIONS

SUBJECT: Year 2000 Testing Guidance

The testing phase is the most important phase of the Year 2000 process. Our May 12, 1998 Letter to Credit Unions (98-CU-10) provided you with the Federal Financial Institution Examination Council's (FFIEC) guidance on testing. In that letter, we stated that experts estimate the testing phase will take more than 50 percent of the time, cost, and personnel of Year 2000 preparations. The purpose of testing systems is to make sure that they process transactions correctly before, during, and after the transition from 1999 to 2000 and that the correct dates are stored in the computer system. Thorough testing will help ensure that Year 2000 efforts have been successful. All credit unions are expected to be active in Year 2000 testing.

Many credit unions have stated that the FFIEC testing guidance paper was too general in nature, and that more information that is specifically geared to credit unions is needed. The purpose of this letter is to give you a better understanding of NCUA's expectations and the different ways you can approach Year 2000 testing. Due to the wide variety of hardware, software, and other equipment used in credit unions, we cannot provide a step by step instruction for the testing process. However, we can explain some key testing concepts so that you can better communicate with your vendor(s) or service provider(s).

This letter covers the key questions identified below. The letter is designed so that you can go directly to the question where you need additional guidance and skip over those sections that do not apply to your credit union.

Due Diligence of Test Results

- Should my Supervisory Committee be involved with testing? (See page 9.)
- What actions should I take if I'm going to change to a different system? (See page 10.)

Management is responsible for determining the best testing approach for the credit union. In putting your test approach in writing, you should include the types of specific tests you'll use to make sure that your systems are Year 2000 ready. Part of the testing process is to compare the results from your tests with the results you expected to get. While this letter discusses several ways to test your systems and explains several types of tests to be performed, the list doesn't include everything. You should work with your vendors and organizations where you exchange information electronically to develop the specific ways you will test your systems.

WHAT ARE THE DIFFERENT WAYS I CAN TEST MY SYSTEM?

There are numerous acceptable ways to test your system, and since few credit unions have exactly the same computer set-up, a particular approach may be all right for some credit unions but not for others. You need to work with your vendors, other credit unions that use your same system, and any external organizations where you exchange information electronically to develop the best approach for testing your individual credit union's systems and hardware.

To start the testing process, management should develop an overall approach for testing the credit union's hardware and software. This big picture view should take place even before the credit union has renovated software. After management determines the overall testing approach, that approach should be documented in a written testing plan. Credit unions should include end-users, such as loan processors, tellers, etc., throughout the testing process to make sure that the tests performed include all of the routine activities of the credit union. Credit unions should also work closely with their vendors to make sure that the approach selected is valid for the system(s) being tested. A credit union may discover that its vendor has already developed generic test plans and procedures that the credit union may customize for their own unique computer environment and testing needs.

The following is a list of acceptable approaches for testing. We understand that there may be other acceptable approaches or a combination of approaches which are appropriate for credit unions; therefore, this list is not all inclusive. If you want to use an approach that is not on this list, feel free to contact your examiner to discuss the pros and cons of that approach. Please keep in mind that our examiners are not experts on every aspect of Y2K, and may need to seek additional guidance from the regional office on your planned approach.

TESTING IN MY CREDIT UNION

Testing in your credit union involves testing the software and hardware systems totally within your credit union's computer environment. (NCUA considers this type of testing to include those credit unions that chose to establish a separate computer environment specifically for testing, including identical hardware and software.) Since credit union management has direct control over this type of testing process, testing in your credit union is generally the most thorough and reliable way to test for Year 2000 readiness. However, for this approach to work, credit unions need to make sure that they have sufficient resources available, such as credit union staff or volunteers, or outside contractors. Also, credit unions may find it difficult to get the information needed from their vendors to fully and safely test their systems.

RISKS: This approach represents the lowest level of testing risk because the credit union's testing occurs in the real-world environment used in the credit union's normal operations. However, this type of testing has increased risks of error in preparing systems for testing. Under no circumstances should testing at your credit union take place using the live production environment. For those more complex credit unions that may have to take all ATM and audio response systems down or disable system security checks while testing, just a reminder that taking these systems down will make these safeguards inaccessible to the members during the test period increasing the risk of withdrawals beyond the available balances during that time. It is very important that the information on systems to be tested is backed up exactly according to procedures provided by the vendor so that the information can be safely restored after the tests

are completed. Credit unions using this approach should have a history of being able to restore backed-up data. Credit unions must be cautious of inadvertently changing member information in the system during this type of testing. In addition, moving the date ahead on some systems may have unexpected consequences and should be discussed thoroughly with the vendor. Again, credit unions using this testing approach should be sure they have specific instructions from the vendor for *data backup*, *data restore*, and *system date change* procedures. Credit unions who do not follow those procedures exactly may have problems that will stop them from returning to normal operations after the testing has been performed.

RELYING ON OTHER CREDIT UNIONS TO TEST MY SYSTEMS

For many credit unions, relying on other credit unions to test systems through vendor user/customer groups can be a viable option for Year 2000 testing and a resource throughout the entire Year 2000 process. User group testing is a form of proxy testing where your vendor or service provider tests the system with a select number or sample of credit unions. Test results are then shared with all similarly situated clients of the vendor. If a credit union is going to use this testing approach, it is very important that credit union officials review the user group's sample of data to be tested, steps to perform the test (also called a test script), and the expected results to ensure they cover the products and services offered by their credit union. For example, if a credit union offers share certificates or share drafts to the membership, yet the test scripts for a particular user group's testing do not contain any test plans or procedures for these products, the credit union will need to test this section of its system separately.

Credit unions planning to rely on user group testing must make sure that their software, operating system, and hardware are either identical, or function in a nearly identical manner to the system(s) tested by the user group. Management is responsible for determining if a credit union's systems are similar enough to the test group for this approach to work. NCUA will allow credit unions to rely, either in whole or in part, on user group testing if, at a minimum, the following conditions are met:

- The composition of the user group must be representative of the credit unions relying on that user group. (When selecting a user group to rely on, credit unions should consider whether the test credit unions are on the same version of the software, using the same or similar hardware and operating system, using the same network product, have similar member services, and similar asset sizes.)
- Credit unions relying on user group testing must obtain full documentation of sample test data, steps to perform the test, and the expected results.
- Credit unions should not rely on the certification of user groups; rather, they must review the test results to satisfy themselves as to the success of the test.
- Credit unions which perform the user group tests should avoid exposure to legal liability by limiting their representations to other credit unions to a factual recounting of how the testing worked in their specific credit union. (These credit unions may chose to obtain additional legal advice as to their liability for certifying that products are ready.)
- There must be oversight for all testing performed by the user group. This oversight can be provided by CPAs, internal auditors, or other third party contractors who perform this type of service. (Ideally, each credit union that is planning to rely on group testing will provide their own oversight by having a representative attend and monitor the testing.)
- User groups must specifically identify the hardware, software, operating system, etc., that is used during testing. Credit unions are responsible for performing additional tests for any product, service, or system component that is not adequately tested by the user group(s).
- Credit unions must perform due diligence by fully reviewing all user group test scripts and results that they rely on. The review should include some form of notation or signature on the test scripts to document that a review actually took place.

RISKS: The risks involved with user group testing include:

- The software, hardware, and operating system tested may not be the same;

- The depth of the tests conducted by the user group may not be adequate for all credit unions using that system; and

- The system being tested is generally tested in only a few computer environments which may not be representative of the actual environment used by the credit union. (For example, computer hardware or external interfaces such as sponsor payroll typically are not tested under the user group approach.)

TESTING AT YOUR DISASTER RECOVERY SITE

Some credit unions have access to remote back-up locations as part of their routine disaster recovery plans. These locations can be used to test for Year 2000 readiness. Credit unions which plan to use these locations to test renovated software must plan ahead to make sure that sufficient time and resources are available at the disaster recovery site. As with user group testing, credit unions must make sure its hardware, software, and operating system are identical or function identically to that provided at the disaster recovery site.

RISKS: The risks involved with disaster recovery site testing relate to the degree of similarity, or differences, between the disaster recovery site and the credit union's actual operations. In addition, duplicating and testing the credit union's external interfaces may not be practical or feasible which would require credit unions to supplement the disaster recovery site testing with some testing within the credit union. An additional risk is that some disaster recovery site vendors may not be able to schedule all of their customers at convenient testing times due to the volume of testing requests.

RELYING ON MY VENDOR TO TEST MY SYSTEMS

Vendor testing is another form of proxy testing that is generally reserved for on-line/real time and batch type systems where the primary hardware and software generally are at the vendor's location. With these types of processing systems, the vendor will most likely conduct the tests since credit unions do not have sufficient access to the hardware and software to perform adequate tests. Also, the risk of losing member information is much greater when testing a live database, and may represent an undue risk of loss. Therefore, NCUA will accept this type of testing if the following conditions, at a minimum, are met:

- End users or user group representatives should be involved in the testing process to make sure that the tests are complete and the results are accurately reported. The user group involvement will also ensure a proper level of independence and impartiality in the testing process.
- Credit unions must perform due diligence by fully reviewing all vendor test scripts and results that they rely on. The review should include some form of notation or signature on the test scripts to document that a review actually took place.
- Credit unions must supplement vendor testing as needed to cover areas the vendor did not test and hardware or software systems housed at the credit union. In addition, credit unions will need to test interfaces that exchange information electronically with external parties.

RISKS: For some systems, vendor testing may be the most risky method for testing Year 2000 readiness primarily because credit unions do not maintain direct control over the testing process. Vendors may be more liberal in determining that test results are accurate due to an inherent lack of impartiality and oversight for the process.

WHAT ARE THE TYPES OF TESTS THAT SHOULD BE PERFORMED ON MY SYSTEMS?

In this section, we list some of the basic types of tests that should be performed on systems. Understanding the basic

terms involved may help clarify the testing process. The listing will define five testing terms that your vendor or examiner may use.The first three types of testing are normally performed by the system developer.

UNIT (COMPONENT) TESTING: This type of testing focuses on one particular program or module, such as a loan initiation process or the general ledger module. Vendors will perform some level of unit testing to assure that the renovated program works.

INTEGRATION TESTING: This type of testing involves checking several units (programs or modules) together to make sure that they function together as intended. Interfaces (or bridges) between programs or modules within the system should be tested as part of the integration testing to assure that they continue to share and interpret information correctly. An example of this type of testing would be opening an account, granting a loan, performing an ATM transaction, and finally closing the account. In this example, many different programs or components must work together properly to successfully complete the test.

REGRESSION TESTING: This testing type involves checking the programs to make sure that Year 2000 fixes haven't created new problems in other areas of the program. Vendors will usually be responsible for this type of testing.

EXTERNAL INTERFACE TESTING: Testing electronic information exchanges between organizations (third parties) is an essential part of Year 2000 testing. Examples of these interfaces include:

- electronically-received sponsor payroll;
- data transmitted to, and received from, corporate credit unions;
- ATM and ACH Systems;
- Federal Reserve wire transfers; and
- other third parties, such as credit bureaus, which perform transaction processing or provide data electronically to the credit union.

In many systems, standard third party interfaces will be tested by the vendor. In these cases, credit unions should review the proposed testing process to make sure that the interface is adequately tested and compliant (using the same due diligence process as discussed above under user group and vendor testing). Management should contact vendors to receive documentation on the data to be tested, the steps used in the test, and the expected results. Credit unions will need to make sure that the test data covers the transactions, products, and services provided by the credit union. As an example, the vendor may test the actual electronic exchange of information between the organizations, but not test the actual posting and use of the information in the credit union's system. Credit unions should also discuss with vendors the actions taken to make sure that the credit union's information is not changed if the external party's exchange of information does not work.

THIRD PARTY INTERFACE PROXY TESTING: This type of testing involves vendor level testing for the electronic funds transfer products and services provided through third parties. In-house developed systems and service bureau system vendors can test the interfaces to external processors (such as share drafts, ATMs, ACH, POS, etc.) on behalf of the credit union, if at a minimum the credit union makes sure that:

- The share and loan system interface for the process is the same version as that used by the credit union.
- Both vendors' transmission formats and file specifications are the same version as that used by the credit union.
- Testing is conducted using the credit union's data file, where possible.
- Full documentation is provided by both vendors to the credit union.

Credit unions which interface directly with the Federal Reserve should become familiar with the Federal Reserve's Century Date Change Bulletins. These bulletins can be found on the Internet at http://www.frbsf.org/fiservices/cdc.

WHAT ARE NCUA'S EXPECTATIONS FOR TESTING MY SYSTEM?

NCUA's expectations for testing remain unchanged from our previous statements contained in NCUA Letters to Credit

Unions 97-CU-12 and 98-CU-4. NCUA expects credit union officials to practice due diligence in making sure that their systems are Year 2000 ready. This means that management and officials must be aware of the status of their plans to fix the credit union's systems. As stated earlier, testing is the most critical part of making sure that a credit union's systems are ready for the Year 2000. Management and officials should continue to receive reports on the status of testing plans and results.

THIRD PARTY CERTIFICATIONS: NCUA is unaware of any external party or company that certifies whether a system, vendor, institution, or business is Year 2000 compliant. The legal liabilities associated with such a statement are simply too great. Typically, those companies which provide certification are stating that the approaches and procedures used should result in Year 2000 readiness. Credit unions cannot rely upon this type of certification for determining whether a system or vendor is Year 2000 ready.

COMPONENT CERTIFICATION: Some companies provide Year 2000 "certification" for components they produce. This type of certification is not a substitute for testing. As an example, a credit union may use a network interface card which has been certified as compliant. Management may decide not to perform unit testing for that particular card; however, as they perform test of the entire system they will test the network where that card resides.

REVIEW OF TEST STRATEGIES: Our examiners will review testing documentation to make sure credit unions are actively involved in the process. Credit unions may not rely on vendor or third party statements of compliance without comparing test results with expected results. We anticipate that all credit unions will need to be involved in some level of testing within the credit union itself due to the differences in hardware, software, operating systems, and third party interfaces from one credit union to the next.

Examiners will review the credit union's overall Year 2000 test strategy, written plan, and the actual performance of the steps contained in the plan. The goal of these reviews will be to assess management's program toward achieving Year 2000 readiness and the appropriateness of the testing approach selected.

HOW SHOULD I DOCUMENT MY EFFORTS AT TESTING?

TEST PLANS: Developing a test plan is crucial to efficiently performing this phase of Year 2000 preparation. The examiner will review the credit union's test plan to assess management's awareness of the testing issues and the appropriateness to their circumstances. All credit unions should put testing plans in writing. The amount and type of documentation for the test plan should be based on the complexity of a credit union's systems, the testing approach management selected, and the specific testing environment. The purpose of a written plan is to provide guidance to the credit union as it implements the testing process. The written plan should consider the following key elements, where appropriate, based on the complexity of systems and approach selected:

- Approach used to test mission critical systems, such as user group, disaster recovery site, at the credit union itself, etc..

- Critical transactions and processes to be tested, including daily, month-end, quarter-end, and year-end processing.

- Dates to be tested.
    - Sample of dates that occur before and after the year 2000;
    - Transactions that begin in 19XX and end in 20XX;
    - Transaction completed in 20XX that must be back-dated to 19XX;
    - Retrieval of historical data after 2000;
    - Dates with special meanings that are peculiar to your system; for example, September 9, 1999. These dates will need to be provided by your vendor(s).
    - Transactions before, during, and after February 29, 2000;
    - Additional dates can be found in the FFIEC testing guidance paper in NCUA Letter to Credit Unions No.

98-CU-10. (Note: The FFIEC testing guidance paper lists several dates. The list is not an all inclusive list, nor is it a list of dates that must be tested. Credit unions must determine what dates are applicable to their various systems and test for those dates. To determine what dates may impact a system, credit unions should contact the vendor of that system.)

- Information to use during the tests.
    - Calculate the expected results;
    - Include transactions that should generate error messages;
    - Retain a copy of this information for future reference;
    - Ensure ability to recreate test data.

- A work plan to perform the tests.
    - Participants;
        - Technical staff, including amount of time estimated;
        - End-users (i.e., tellers, loan processors, etc.);
    - Type of testing to be performed (i.e., unit, integrated, etc.);
    - Schedule for testing, including start and end dates.

- Credit union wide test - final verification that all systems work properly together.

DUE DILIGENCE OF TEST RESULTS: Management must document their due diligence efforts to make sure that systems are Year 2000 ready. The reason for this documentation is two-fold, first to assist the credit union in managing the risks associated with the Year 2000 process. Second, the credit union's documented efforts of due diligence are the credit union's best defense if any Year 2000 litigation is brought against the credit union.

The credit union should identify in board minutes the following aspects of their Year 2000 plans:

- Individuals responsible for reviewing testing results.
    - Documentation of the comparison of test results with expected results;
    - Written explanations of the differences between test and expect results.

- Approach for the acceptance of systems by users (i.e., tellers, loan processors, collectors, member service staff, etc.).

- Communication with the membership to maintain member confidence.
    - Members may want to test with the credit union to be assured that home banking and Internet transactions are working.

- Documentation from external parties when the credit union chooses to rely on their efforts.
    - Should include standard reports, member trial balances, delinquency reports, proof sheets that show the manual calculations to validate test calculations, etc..

SHOULD MY SUPERVISORY COMMITTEE BE INVOLVED WITH TESTING?

NCUA expects supervisory committees and/or internal auditors to provide a proper level of oversight for the testing phase as discussed in NCUA Letter to Credit Unions No. 97-CU-10. Some items to consider include:

- Reviewing test plans and budgets to make sure all mission critical systems will be adequately tested for Year 2000 readiness.

- Reviewing any slippage of testing schedules and the effect on the credit union's ability to complete its Year 2000 project.

- Reviewing the appropriateness and adequacy of putting into place the credit union's contingency plan (Plan B if Plan A goes awry).

- Reviewing documentation, such as the comparison of expected results with test results after tests are performed.

- Providing written reports to the board of directors disclosing any problems noted in the testing process.

WHAT ACTIONS SHOULD I TAKE IF I'M GOING TO CHANGE TO A DIFFERENT SYSTEM?

NCUA recognizes that credit unions may change data processors between now and the Year 2000 for a variety of reasons. If a credit union plans to change or convert a mission critical system, and that change will cause the credit union to miss one of the dates contained in NCUA Letter to Credit Unions No. 98-CU-4, NCUA's Year 2000 Contingency Plan, the credit union must submit a letter detailing the credit union's conversion plans to the NCUA Regional Director, with a copy to the State Supervisior. In these circumstances, credit unions do not need to test the old system for Year 2000 compliance. To help NCUA analyze the credit union's due diligence in reviewing the conversion decision, the letter must include the following information:

- The time frame for entering into a contract to change or convert to the new system.
- A contracted delivery date for the Year 2000 ready system.
- Information on the new vendor's experience in converting credit unions from the current system.
- Planned participation in testing with other users, or user groups, to familiarize yourself with the Year 2000 readiness of the new system to ensure a smooth transition to the new system.
- Communication with the vendor of your Year 2000 needs regarding testing and requirements for the new system.
- A test plan for the new system and any interfaces. This should include a review of test data from other users or user groups of the new system.
- The completion dates for renovation, testing, and implementation of the new system.

NCUA remains committed to working with credit unions to help them prepare for the Year 2000. If you have any questions, please contact your district examiner, regional office, or state supervisory authority.

/S/

NORMAN E. D'AMOURS

Chairman

Enclosure

cc: All Primary Credit Union Share and Loan Information Systems Vendors