United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Financial Services and Technology, Committee on Banking, Housing, and Urban Affairs, U.S. Senate

For Release on Delivery
Expected at
10 a.m.
Tuesday,
February 10, 1998

YEAR 2000 COMPUTING CRISIS

Federal Deposit Insurance Corporation's Efforts to Ensure Bank Systems Are Year 2000 Compliant

Statement of Jack L. Brock, Jr.
Director, Governmentwide and Defense Information Systems
Accounting and Information Management Division

19980316 093

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

DTIC QUALITY INSPECTED 3

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here to discuss the progress being made by the Federal Deposit Insurance Corporation (FDIC) in ensuring that the thousands of banks it oversees are ready for the upcoming century date change. If Year 2000 issues are not adequately addressed, key automated bank systems—affecting trillions of dollars in assets, transactions, and insured deposits—are subject to serious consequences ranging from malfunction to failure. Such consequences would at the very least cause significant inconveniences to both banks and their customers. More significantly, system failure could lead to bank closings and serious disruptions to both the banking community and bank customers. Further, we will be discussing the progress FDIC is making in addressing Year 2000 concerns for its own internal systems.

This testimony is the second in a series of reports you requested on the status of efforts by federal financial regulatory agencies to ensure that the institutions they oversee are ready to handle the Year 2000 computer conversion challenge. We also recently testified and reported on the status of the National Credit Union Administration's efforts.[1]

To prepare for this testimony, we evaluated FDIC's efforts to date to ensure that the banks it oversees have adequately mitigated the risks associated with the Year 2000 date change and compared these efforts to criteria detailed in our Year 2000 Assessment Guide.[2] In performing the overview, we reviewed Year 2000 examination policies, procedures, and guidance. We also reviewed FDIC correspondence to banks and third-party contractors (that provide automated systems services and software to many financial institutions) regarding the Year 2000 problem. Furthermore, we interviewed FDIC officials responsible for examining and overseeing the safety and soundness of bank management practices and procedures. Finally, we interviewed officials from the American Bankers Association and the Independent Bankers Association of America.

[1]Year 2000 Computing Crisis: National Credit Union Administration's Efforts to Ensure Credit Union Systems Are Year 2000 Compliant (GAO/T-AIMD-98-20, October 22, 1997) and Year 2000 Computing Crisis: Actions Needed to Address Credit Union Systems' Year 2000 Problem (GAO/AIMD-98-48, January 7, 1998).

[2]Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997). Published as an exposure draft in February 1997 and finalized in September 1997, the guide was issued to help federal agencies prepare for the Year 2000 conversion. It addresses common issues affecting most federal agencies and presents a structured approach and a checklist to aid in planning, managing, and evaluating Year 2000 programs. The guide describes five phases—supported by program and project management activities—with each phase representing a major Year 2000 program activity or segment. While the guide focuses on federal agencies, nonfederal organizations can also use it to assess their automated systems.

We also compared FDIC efforts to fix its internal systems with our guide. To accomplish this, we reviewed the corporation's project plan and other Year 2000 documentation and interviewed officials responsible for fixing the Year 2000 problem. We performed our work at FDIC headquarters in Washington, D.C.; its office in Arlington, Virginia; and its field office in Atlanta, Georgia, during December 1997 and January 1998 in accordance with generally accepted government auditing standards.

In summary, we found that the Year 2000 problem poses a serious dilemma for banks due to their heavy reliance on information systems. It also poses a challenge for FDIC and the other bank regulators who are responsible for ensuring bank industry readiness. Regulators have a monumental task in making sure that financial institutions have adequate guidance in preparing for the Year 2000 and in providing a level of assurance that such guidance is being followed. Further, regulators will likely face some tough decisions on the readiness of individual institutions as the millennium approaches. We found that FDIC is taking the problem very seriously and is devoting considerable effort and resources to ensure the banks it oversees mitigate Year 2000 risks. The corporation has been very emphatic in alerting banks to the Year 2000 problem and has conducted a high-level assessment of the industry's Year 2000 readiness.

Despite aggressive efforts, FDIC still faces significant challenges in providing a high level of assurance that individual banks will be ready. First, FDIC—as were the other regulators—was late in addressing the problem. Consequently, it is behind the Year 2000 schedule recommended by both GAO and the Office of Management and Budget (OMB). Compounding this problem is that critical guidance, although under development, has not been released by the Federal Financial Institutions Examination Council (FFIEC)[3] for banks and other financial institutions on contingency planning, assessing risks caused by corporate customers (borrowers), and assessing risks associated with third-party automated system service providers. This guidance should have been provided earlier so that banks would have had more time to factor the guidance into their own assessments and plans. Additionally, FDIC's ability to report on individual bank's status in preparing for the year 2000 is limited by insufficient information being reported by bank examiners.

[3]FFIEC was established in 1979 as a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions, and to make recommendations to promote uniformity in the supervision of these institutions. The Council's membership is composed of the federal bank regulators—FDIC, the Federal Reserve System, and the Comptroller of the Currency—plus the regulators for credit unions and thrift institutions—the National Credit Union Administration and the Office of Thrift Supervision, respectively.

FDIC also needs to correct its internal systems used to support agency functions and has initiated efforts to do this. FDIC is behind in assessing whether these systems are Year 2000 compliant. Although OMB guidance states that the assessment phase should have been completed in mid-1997, FDIC has not yet fully assessed its mission-critical systems or established contingency plans in case systems repairs and replacements are not in place on time or do not work as intended.

We are making recommendations to strengthen both FDIC's examination process and its internal mitigation processes.

The Year 2000 Poses a Serious Problem for Banks

The Federal Deposit Insurance Corporation is the deposit insurer of approximately 11,000 banks and saving institutions. Together, these institutions are responsible for about $6 trillion in assets and have insured deposits totaling upwards of $2.7 trillion. FDIC also has responsibility for directly supervising approximately 6,200 of these institutions (commonly referred to as state-chartered, nonmember banks), which on average have $250 million in assets. As part of its goal of maintaining the safety and soundness of these institutions, FDIC is responsible for ensuring that banks are adequately mitigating the risks associated with the century date change. To ensure consistent and uniform supervision on Year 2000 issues, FDIC and the other banking regulators coordinate their supervisory efforts through FFIEC. For example, the regulators established an FFIEC working group to develop guidance on mitigating the risks associated with using contractors that provide automated systems services and software to banks.

The Year 2000 problem is rooted in the way dates are recorded and computed in automated information systems. For the past several decades, systems have typically used two digits to represent the year, such as "97" representing 1997, in order to conserve on electronic data storage and reduce operating costs. With this two-digit format, however, the year 2000 is indistinguishable from 1900, or 2001 from 1901, etc. As a result of this ambiguity, system or application programs that use dates to perform calculations, comparisons, or sorting may generate incorrect results, or worse, not function at all.

According to FDIC, virtually every insured financial institution relies on computers—either their own or those of a third-party contractor—to provide for processing and updating of records and a variety of other functions. Because computers are essential to their survival, FDIC believes

that all its institutions are vulnerable to the problems associated with the year 2000. Failure to address Year 2000 computer issues could lead, for example, to errors in calculating interest and amortization schedules. Moreover, automated teller machines may malfunction, performing erroneous transactions or refusing to process transactions. In addition, errors caused by Year 2000 miscalculations may expose institutions and data centers to financial liability and loss of customer confidence. Other supporting systems critical to the day-to-day business of banks may be affected as well. For example, telephone systems, vaults, security and alarm systems, elevators, and fax machines could malfunction.

In addressing the Year 2000 problem, banks must also consider the computer systems that interface with, or connect to, their own systems. These systems may belong to payment system partners, such as wire transfer systems, automated clearinghouses, check clearing providers, credit card merchant and issuing systems, automated teller machine networks, electronic data interchange systems, and electronic benefits transfer systems. Because these systems are also vulnerable to the Year 2000 problem, they can introduce errors into bank systems.

In addition to these computer system risks, banks also face business risks from the Year 2000. That is exposure from its corporate borrower's inability to manage their own Year 2000 compliance efforts successfully. Consequently, in addition to correcting their computer systems, banks have to periodically assess the Year 2000 efforts of their large corporate customers to determine whether they are sufficient to avoid significant disruptions to operations. FDIC and the other regulators established an FFIEC working group to develop guidance on assessing the risk corporate borrowers pose to banks.

To address Year 2000 challenges, GAO issued its Year 2000 Assessment Guide[4] to help federal agencies plan, manage, and evaluate their efforts. It advocates a structured approach to planning and managing an effective Year 2000 program through five phases. These phases are (1) raising awareness of the problem, (2) assessing the extent and severity of the problem and identifying and prioritizing remediation efforts, (3) renovating, or correcting, systems, (4) validating, or testing, corrections, and (5) implementing corrected systems.

As part of the assessment phase, the guide stipulates that interfaces with outside organizations be identified and agreements with these

[4]GAO/AIMD-10.1.14, September 1997.

organizations executed for exchanging Year 2000-related data. Contingency plans must be prepared during the assessment phase to ensure that agencies can continue to perform even if critical systems have not been corrected. Working back from January 1, 2000, GAO and OMB have established a schedule for completing each of the five phases. According to that schedule, agencies should have completed assessment phase activities last summer and should complete the renovation phase by mid- to late 1998.

FDIC Has Developed a Strategy and Has Initiated Action to Address the Year 2000 Problem

FDIC has taken a number of actions to raise the awareness of the Year 2000 issue among banks and to assess the Year 2000 impact on the industry. To raise awareness, FDIC formally alerted banks in July 1996 to the potential dangers of the Year 2000 problem by issuing an awareness letter to bank Chief Executive Officers. The letter, which included a statement from the interagency Federal Financial Institutions Examination Council, described the Year 2000 problem and highlighted concerns about the industry's Year 2000 readiness. It also called on banks to perform a risk assessment of how systems are affected and develop a detailed action plan to fix them.

In May 1997, FDIC issued a more detailed awareness letter that

- described the five-phase approach to planning and managing an effective Year 2000 program;
- highlighted external issues requiring management attention, such as reliance on vendors, risks posed by exchanging data with external parties, and the potential effect of Year 2000 noncompliance on corporate borrowers;
- discussed operational issues that should be considered in Year 2000 planning, such as whether to replace or repair systems;
- related its plans to facilitate Year 2000 evaluations by using uniform examination procedures; and
- directed banks to (1) inventory core computer functions and set priorities for Year 2000 goals by September 30, 1997, and (2) to complete programming changes and to have testing of mission-critical systems underway by December 31, 1998.

To manage both internal and external Year 2000 efforts, FDIC established a Year 2000 oversight committee, consisting of the deputy directors of all offices and divisions, that reports to the FDIC Board of Directors. Among other matters, the committee is responsible for coordinating interagency working groups, contingency planning, public information campaign,

institution outreach and education, and reporting on the results of bank assessments and examinations.

As of December 31, 1997, FDIC had completed its initial assessment of all banks for which it has supervisory responsibility. In doing so, FDIC surveyed banks on whether (1) their systems were ready to handle Year 2000 processing, (2) they had established a structured process for correcting Year 2000 problems, (3) they prioritized systems for correction, and (4) they had determined the Year 2000 impact on other internal systems' important to day-to-day operations, such as vaults, security and alarm systems, elevators, and telephones. In addition, FDIC assessed whether sufficient resources were targeted at the Year 2000 problem and if bank milestones for renovating and testing mission-critical systems were consistent with those recommended by FFIEC. According to the FDIC, this assessment identified over 200 banks that were not adequately addressing the Year 2000 problem and over 500 banks that are very reliant on third-party servicers and software providers and have not followed up with their servicers and providers to determine their Year 2000 readiness.

FDIC plans to follow up on this initial assessment, which was conducted largely by telephone, with on-site visits to all banks to be completed by the end of June 1998. FDIC has also been participating with other regulators to conduct on-site Year 2000 assessments of 275 major data processing servicers and 12 major software vendors. According to FDIC, these servicers and vendors provide support and products to a majority of financial institutions. FDIC and the other regulators expect to complete their first round of servicer and vendor assessments by March 31, 1998. FDIC is providing the results of the servicer assessments to FDIC-supervised banks that use these services. Together with the results of on-site assessments conducted at banks, FDIC expects to have a better idea of where the industry stands, which banks need close attention, and thus, where to focus its supervisory efforts.

Concerns With FDIC's Efforts to Ensure Banks Are Year 2000 Ready

The primary challenge facing FDIC, and indeed all the banking regulators, in providing a level of assurance that the banking industry will successfully address the Year 2000 problem is time. FDIC's late start in developing an industry assessment is further compounded by two other factors: (1) its initial assessment and the follow-on assessment to be completed in June 1998 are not collecting all the data required to be definitive about the status of individual banks and (2) key guidance—being developed under the auspices of FFIEC—needed by banks

to complete their own preparations is also late which, in turn, could potentially hamper individual banks' abilities to address Year 2000 issues.

Need for Additional Data Precision

Although late in getting its initial assessments completed, FDIC has developed a perspective of where the banks it regulates stand on being ready for Year 2000. As outlined earlier, it plans on completing a more detailed assessment of banks by the end of June 1998. FDIC plans to use this information along with information obtained from the FFIEC servicer and vendor assessments to further refine its oversight activities.

We think FDIC's strategy in using this information to target activities over the remaining 18 months is appropriate and necessary to make the best use of limited time. However, we believe that neither the initial nor the follow-on assessment work program is collecting all the data needed to determine where (i.e., in which phase) the banks are in the Year 2000 correction process. For example, neither the guidance used to conduct the initial assessment nor the guidance that is to be used to conduct follow-on assessments contains questions that ask whether specific phases have been completed. In addition, the terms used in the FFIEC guidance to describe progress are vague. For example, it notes that banks should be *well into* assessment by the end of the third quarter of 1997, that renovation for mission-critical systems should *largely* be completed, and testing should be *well underway* by December 31, 1998. Without defining any of these terms, it will be very hard to deliver uniform assessments on the status of banks' Year 2000 efforts.

Furthermore, the tracking questionnaire examiners are required to complete after their on-site assessments is organized on the basis of the five phases; however, it does not ask enough questions within each of the five phases to determine whether the bank has fully addressed the phases. For example, for the assessment phase, the questionnaire asks whether (1) a formal assessment has been conducted and if all mission-critical application and hardware systems have been identified, (2) a budget has been established for testing and upgrading mission-critical systems, and (3) the budget is reasonable. But these questions do not specifically cover critical assessment steps recommended in our Assessment Guide, including:

- conducting an enterprisewide inventory of information systems;
- using the inventory to develop a comprehensive automated system portfolio;

- establishing Year 2000 project teams for business areas and major systems;
- developing a Year 2000 program, which includes schedules for all tasks and phases, a master conversion and replacement schedule, and a risk assessment;
- developing testing strategies and plans;
- defining requirements for testing facilities;
- identifying and acquiring Year 2000 tools;
- addressing interface and data exchange issues; and
- formulating contingency plans.

In discussing this concern with FDIC officials, they told us that they intended to rely on the judgment of the examination staff to place institutions in specific categories. We agree on the need to rely on examiner judgment; however, we believe that having additional information will allow the examiners to conduct a more thorough assessment and can greatly enhance their capability to make a more accurate judgement. In turn, this could improve the ability of FDIC to properly focus its resources over the remaining time available.

Contingency Planning Guidance Not Yet Available

FDIC and FFIEC have yet to complete and issue contingency planning guidance to the banks. Our Assessment Guide recommends that contingency planning begin in the assessment phase for critical systems and activities. FDIC officials told us they are working with the other regulators to establish a working group to address this issue. While this guidance is needed, it would have been more appropriate to make it available before banks began completing their assessment phase efforts.

Guidance Late for Bank Interaction With Vendors

Regulators have found that some financial institutions, relying on third-party data processing servicers or purchased applications software, have not taken a proactive approach in ensuring Year 2000 compliance by their vendors. In a May 1997 letter to banks, the regulators recommended that banks begin assessing their risks with respect to vendors and outlined an approach for dealing with vendors that included the need to (1) evaluate and monitor vendor plans and milestones, (2) determine whether contract terms can be revised to include Year 2000 covenants, and (3) ensure vendors have the capacity to complete the project and are willing to certify Year 2000 compliance. The regulators also agreed to provide guidance on how each of the steps should be implemented. However, the regulators do not plan to issue this guidance until the end of

March 1998. While this time frame cannot be significantly shortened, the timing of this specific guidance is coming at a very late date for some banks that have not been active in working with their vendors or that may lack sufficient technical expertise to evaluate vendor preparedness.

Guidance Late on Corporate Customer Year 2000 Readiness

Banks—even those who have Year 2000 compliant systems—could still be at risk if they have significant business relations with corporate customers who, in turn, have not adequately considered Year 2000 issues. If these customers default or are late in repaying loans, then banks could experience financial harm.

In its May 1997 letter, the regulators also recommended that banks begin developing processes to periodically assess large corporate customer Year 2000 efforts and to consider writing Year 2000 compliance into their loan documentation, and FDIC later informed its institutions that the Year 2000 risks associated with corporate customers and reliance on vendors would be included in FDIC's follow-up assessments. The regulators again agreed to provide guidance on how institutions should do this, and the criteria defining safe and sound practices. However, the guidance being developed on this issue is also not expected until the end of March 1998. These time lags in providing guidance increase the risk that banks may have initiated action that does not effectively mitigate vendor and borrower risks or that banks have taken little or no action in anticipation of pending regulator guidance.

Concerns With FDIC's Efforts to Correct Its Internal Systems

FDIC internal systems are critical to the day-to-day operation of the corporation. For example, they facilitate the collection of bank assessments, keep accounts and balances for failed banks, schedule examinations, and calculate FDIC employee payroll benefits. The effects of Year 2000 failure on FDIC, in its own words, could range from "annoying to catastrophic." FDIC system failures could, for example, result in inaccurate or uncollected assessments, inaccurate or unpaid accounts payable, and miscalculated payroll and benefits. Accordingly, FDIC developed an internal Year 2000 project plan that followed the structured five-phased approach recommended in our Assessment Guide. To raise awareness among FDIC employees, FDIC conducted more than 40 briefings for corporate staff throughout its divisions and offices. It also has disseminated Year 2000 information through the Internet and internal newsletters. To assess Year 2000 impact, FDIC conducted an inventory and "high-level" assessment of approximately 500 internal systems that consist of about 15 million lines of

program code. In addition, FDIC engaged a contractor to assist in conducting detailed system assessments, defining requirements for test environments, and renovating and testing code.

We have two concerns with FDIC's effort to correct its internal systems. First, FDIC is taking much longer to assess its systems than is recommended by our guide as well as OMB and technology experts. Second, FDIC has yet to develop contingency plans to ensure continuity of core business processes, which our guide points out need to be started early in the Year 2000 effort.

Currently, FDIC is still assessing which of its systems need Year 2000 corrections, and it does not expect to finish this assessment until March 1998. Specifically, FDIC has yet to fully assess its 40 mission-critical systems. Our guide recommends that agencies make these determinations by mid-1997 in order to have enough time to complete the next three stages of correction. By taking additional time to complete assessment, FDIC is leaving itself with much less time to complete renovation, testing, and implementation, and, thus, it is increasing the risk that it will not complete its Year 2000 fixes on time.

Compounding this problem is the fact that FDIC has yet to develop contingency plans for its mission-critical systems and core business processes. Rather than begin developing contingency plans for critical systems and core business processes, as our Assessment Guide recommends, FDIC intends to develop plans only for those systems that experience unforeseen problems or delays in correction or replacement efforts. In addition, FDIC had not yet prepared a contingency plan to ensure continuity of its core business processes. In pursuing this approach, FDIC is failing to heed advice that it holds banks accountable to: preparing contingency plans that focus on ensuring that internal operations will be sustained. The FFIEC states that the board of directors and senior management are responsible for organizationwide contingency planning, which assesses the importance of an institution's departments, business units, and functions and determines how to restore critical areas should they be affected by disaster.

In addition, preparing contingency plans on an as-needed basis is risky in several respects. First, programmers cannot always foresee system problems. Without contingency plans, FDIC will not be prepared to respond to unforeseen problems. Second, FDIC's Year 2000 strategy for many systems involves replacing systems in 1998 and 1999. In the event that

replacement schedules slip, FDIC may not have enough time to renovate, test, and implement a legacy system or identify other alternatives, such as manual procedures or outsourcing. Third, even if systems are replaced on time, there is no guarantee that the new systems will operate correctly. FDIC tasked its contractor with providing guidance on preparing contingency plans for its mission-critical systems and the contractor provided draft guidelines on January 28, 1998, with the goal of making them final by the end of February 1998.

In conclusion, Mr. Chairman, we believe that FDIC has a good appreciation for the Year 2000 problem and has made significant progress since last year. Further, we believe that FDIC's strategy of using the results of the service provider and vendor assessments in conjunction with the more complete assessments of individual banks in order to best focus resources is a reasonable approach. However, FDIC and the other regulators are facing a finite deadline that offers no flexibility. We believe that FDIC needs to take several actions to improve its ability to make informed judgments about bank status and to enhance the ability of banks to meet the century deadline with minimal problems. We, therefore, recommend that FDIC

- work with the other FFIEC members to expeditiously revise the Year 2000 assessment work program to include questions on each phase of the correction process, such as those outlined in our Assessment Guide, to better enable examiners to determine and report the exact status of each bank and vendor in addressing the Year 2000 problem. FDIC should also apply the revised Year 2000 assessment work program to each bank and vendor, including those where assessments are completed, to determine whether appropriate data have been obtained to make complete assessments.

We also recommend that FDIC

- work with the other FFIEC members to complete by the end of March 1998, their guidance to institutions on mitigating the risks associated with corporate customers and reliance on vendors. Further, FDIC should work with the other FFIEC members to quickly establish a working group to develop contingency planning guidance and set a deadline for completing this effort.

Additionally, we believe that a combination of factors including starting the bank assessment process late and issuing more specific guidance to

banks at a relatively late date has greatly compressed the time schedule available for FDIC and other members of FFIEC to develop more positive assurance that banks will be ready for the year 2000. Accordingly, we recommend that FDIC work with the other FFIEC members to

- develop, in an expeditious manner, more explicit instructions to banks for carrying out the latter stages of the Year 2000 process—renovation, validation, and implementation—which are the critical steps to ensuring Year 2000 compliance.

Because the results of the bank assessments to be completed this June are so critical to FDIC in focusing its activities through the year 2000, we recommend that FDIC

- develop a tactical plan that details the results of its assessments and provides a more explicit road map of the actions it intends to take based on those results.

Finally, with regard to FDIC's internal systems, we recommend that the Chairman direct the Year 2000 oversight committee to (1) ensure that adequate resources are allocated to complete the internal systems' assessment by the end of March 1998 and take necessary action to ensure this effort is completed on time and (2) develop contingency plans for each of FDIC's mission-critical systems and core business processes.

Mr. Chairman, that concludes my statement. We welcome any questions that you or Members of the Subcommittee may have.