GAO

YEAR 2000 COMPUTING CRISIS

USDA Faces Tremendous Challenges in Ensuring That Vital Public Services Are Not Disrupted

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division

Mr. Chairman and Members of the Committee:

We are pleased to be here today to discuss the computing challenges that the upcoming change of century poses to virtually all major organizations, public and private, including government programs vital to Americans, such as those of the Department of Agriculture (USDA). As the world's most advanced and most dependent user of information technology, the United States possesses close to half of all computer capacity and 60 percent of Internet assets.[1] As a result, the coming century change presents a particularly sweeping and urgent challenge for entities in this country.[2]

For this reason, we have designated the Year 2000 computing problem as a high-risk area[3] for the federal government, and have published guidance[4] to help organizations successfully address the issue. Since early 1997 we have issued over 35 products detailing specific findings and recommendations related to the Year 2000 readiness of a wide range of federal agencies.[5]

The common theme of these reports has been that serious vulnerabilities remain in addressing the federal government's Year 2000 readiness and that much more action is needed to ensure that federal agencies satisfactorily mitigate Year 2000 risks to avoid debilitating consequences. Key economic sectors of the nation are also vulnerable. These include state and local governments; telecommunications; banking and finance; health, safety, and emergency services; transportation; utilities; and manufacturing and small business. While actions by government and industry are underway throughout the nation, the creation of the President's Council on Year 2000 Conversion represents an opportunity to orchestrate the leadership and public/private partnerships essential to confronting the unprecedented information technology challenge that our nation faces.

---

[1]Critical Foundations: Protecting America's Infrastructures (President's Commission on Critical Infrastructure Protection, October 1997).

[2]For the past several decades, automated information systems have typically represented the year using two digits rather than four in order to conserve electronic data storage space and reduce operating costs. In this format, however, 2000 is indistinguishable from 1900 because both are represented only as *00*. As a result, if not modified, computer systems or applications that use dates or perform date- or time-sensitive calculations may generate incorrect results beyond 1999.

[3]High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

[4]Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997) and Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, March 1998 [exposure draft]).

[5]A listing of our publications is included as an attachment to this statement.

This morning we bring a message of urgency relating to the Department of Agriculture (USDA): its progress to date indicates that it will have a great deal of difficulty in correcting, testing, and implementing its automated information systems to work beyond 1999—that is, to become what is called Year 2000 compliant—in time. This could have serious implications for the many vital public health and safety and economic activities that its systems support. Constituencies nationwide could be affected—farmers, consumers, even schools.

At your request, my testimony today will briefly outline our views on what additional actions must be taken to reduce the nation's Year 2000 risks overall; I will then discuss our assessment of USDA's Year 2000 program. My statement on USDA will include (1) an overview of the potential impact of the century change on USDA's mission, (2) how the department is structured to address the crisis, (3) how much work remains to be completed, and (4) the current efforts of 10 of USDA's component agencies and the department as a whole. In addition, I will provide observations on the Year 2000 status at two other organizations, the Farm Credit Administration (FCA) and the Commodity Futures Trading Commission (CFTC).

To prepare for this testimony, we used our Year 2000 readiness guide to perform an initial assessment of USDA's departmentwide Year 2000 strategy.[6] We also discussed USDA's strategy with its Chief Information Officer, Year 2000 Program Executive, and staff in the Year 2000 Program Office. We used the guide to assess the following 10 USDA component agencies: the Agricultural Marketing Service (AMS); Agricultural Research Service (ARS); Animal and Plant Health Inspection Service (APHIS); Farm Service Agency (FSA); Food and Nutrition Service (FNS); Food Safety and Inspection Service (FSIS); Forest Service; Grain Inspection, Packers and Stockyards Administration (GIPSA); National Agricultural Statistical Service (NASS); and the Risk Management Agency (RMA).

We reviewed applicable Year 2000 documentation of these component agencies and interviewed Year 2000 personnel. In addition, we used the guide to assess the Year 2000 programs of FCA's and CFTC's internal systems. Finally, we reviewed FCA's and CFTC's actions to ensure the Year 2000 readiness of the industries that they regulate. We provided USDA, FCA, and CFTC with the facts outlined in this testimony, and they were in general

---

[6]GAO/AIMD-10.1.14, September 1997. This guide details the key tasks to be completed within each of the five phases of a Year 2000 program: awareness, assessment, renovation, validation, and implementation.

agreement with them. FCA and CFTC offered technical corrections which we incorporated into the testimony.

Risk of Year 2000 Disruptions Requires Leadership

The public faces the risk that critical services could be severely disrupted by the Year 2000 computing crisis. Financial transactions could be delayed, airline flights grounded, and national defense affected. The many interdependencies that exist among the levels of governments and within key economic sectors of our nation could cause a single failure to have wide-ranging repercussions. While managers in the government and the private sector are acting to mitigate these risks, a significant amount of work remains.

The federal government is extremely vulnerable to Year 2000 problems due to its widespread dependence on computer systems to process financial transactions, deliver vital public services, and carry out its operations. This challenge is made more difficult by the age and poor documentation of many of the government's existing systems, and its lackluster track record in modernizing systems to deliver expected improvements and meet promised deadlines.

Year 2000-related problems have already occurred. For example, an automated Defense Logistics Agency system erroneously deactivated 90,000 inventoried items as the result of an incorrect date calculation. According to the agency, if the problem had not been corrected (which took 400 work hours), the impact would have seriously hampered its mission to deliver materiel in a timely manner.[7]

Our reviews of federal agency Year 2000 programs have found uneven progress, and our reports contain numerous recommendations, which the agencies have almost universally agreed to implement. Among them are the need to establish priorities, solidify data exchange agreements, and develop contingency plans.

One of the largest, and largely unknown, risks relates to the global nature of the problem. With the advent of electronic communication and international commerce, the United States and the rest of the world have become critically dependent on computers. However, with this electronic dependence and massive exchanging of data comes increasing risk that uncorrected Year 2000 problems in other countries will adversely affect

---

[7]Defense Computers: Issues Confronting DLA in Addressing Year 2000 Problems (GAO/AIMD-97-106, August 12, 1997).

the United States. And there are indications of Year 2000 readiness problems internationally. In September 1997 the Gartner Group, a private research firm acknowledged for its expertise in Year 2000 computing issues, surveyed 2,400 companies in 17 countries and concluded that "[t]hirty percent of all companies have not started dealing with the year 2000 problem."[8]

Additional Actions Must Be Taken to Reduce Nation's Year 2000 Risks

As 2000 approaches, the scope of the risks that the century change could bring has become more clear, and the federal government's actions have intensified. This past February, an executive order was issued establishing the President's Council on Year 2000 Conversion. The Council Chair is to oversee federal agency Year 2000 efforts as well as be the spokesman in national and international forums, coordinate with state and local governments, promote appropriate federal roles with respect to private sector activities, and report to the President on a quarterly basis.

As we testified in March,[9] there are a number of actions we believe the Council must take to avert this crisis. In a report issued last month, we detailed specific recommendations.[10] The following summarizes a few of the key areas in which we recommend action.

- Because departments and agencies have taken longer than we and others have recommended to assess the readiness of their systems, it is unlikely that they will be able to renovate and fully test all mission-critical systems by January 1, 2000. Consequently, setting priorities is essential, with the focus being on systems most critical to health and safety, financial well being of individuals, national security, and the economy.
- Agencies must start business continuity and contingency planning now to safeguard their ability to deliver a minimum acceptable level of services in the event of Year 2000-induced failures. In March we issued an exposure draft of a guide providing information on business continuity and contingency planning issues common to most large enterprises; the Office of Management and Budget (OMB) recently adopted this guide as a model for federal agencies.[11] Agencies developing such plans only for systems currently behind schedule, however, are not addressing the need to ensure

---

[8]Year 2000-World Status (Gartner Group, Document #M-100-037, November 25, 1997).

[9]Year 2000 Computing Crisis: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions (GAO/T-AIMD-98-101, March 18, 1998).

[10]Year 2000 Computing Crisis: Potential For Widespread Disruption Calls For Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998).

[11]GAO/AIMD-10.1.19, March 1998 [exposure draft].

business continuity in the event of unforeseen failures. Further, such plans should not be limited to the risks posed by the Year 2000-induced failures of internal information systems, but must include the potential Year 2000 failures of others, including business partners and infrastructure service providers (e.g., power, water, transportation, and voice and data telecommunications).

- OMB's assessment of the current status of federal Year 2000 progress is predominantly based on agency reports that have not been consistently verified or independently reviewed. Without such independent reviews, OMB and the President's Council on Year 2000 Conversion have little assurance that they are receiving accurate information. Accordingly, agencies must have independent verification strategies involving inspectors general or other independent organizations.
- As a nation, we do not know where we stand overall with regard to Year 2000 risks and readiness. No nationwide assessment—including the private and public sectors—has been undertaken to gauge this. In partnership with the private sector and state and local governments, the President's Council could orchestrate such an assessment.

Year 2000 Impact on USDA Programs Could Be Severe

If the systems that support USDA's various programs cannot operate reliably into the next century, it would not take long for the effects to be felt. USDA's systems support many vital public health and safety and economic activities and, if not properly fixed, tested, and implemented, severe consequences could result, such as the following.

- Payments to schools, farmers, and others in rural communities could be delayed or incorrectly computed.
- The economy could be adversely affected if information critical to crop and livestock providers and investors is unreliable, late, or unavailable.
- The import and export of foodstuffs could be delayed, thus increasing the likelihood that they will not reach their intended destinations before their spoilage dates.
- Food distribution to schools and others could be stopped or delayed.
- Public health and safety could be at risk if equipment used in USDA's many laboratories to detect bacteria, diseases, and unwholesome foods is not compliant.

USDA's Approach Relies on Component Agencies

USDA's Chief Information Officer (CIO) is responsible for leading the department's preparation for the Year 2000 date change and ensuring that all critical USDA information systems are Year 2000 compliant and operational. In October 1997 USDA's CIO established the Year 2000 Program

Office under the direction of a Year 2000 Program Executive. This office is responsible for providing oversight and guidance for the department's Year 2000 program, and serves as USDA's liaison with other government entities on the Year 2000 issue, such as the CIO Council.[12]

Direct accountability for assessing, renovating, validating, and implementing systems conversion, however, rests with USDA's 31 component agencies, which include staff offices. The Secretary of Agriculture has required each component agency administrator to appoint an executive sponsor specifically accountable for Year 2000 issues, establish technical and program teams, ensure that an action plan is developed, and certify that critical agency systems are reflected in Year 2000 implementation plans.

Component Agencies Have a Tremendous Amount of Remaining Work

USDA's component agencies have a great deal of work still to be accomplished in the next 19 months in making its mission-critical systems ready for the year 2000. As figure 1 indicates, for the 10 component agencies in our review, 250 mission-critical systems were initially assessed as compliant. As of this month 132 have been reported as repaired or replaced, while work remains to be completed on 596 mission-critical systems.[13] Looked at another way, about 80 percent of the work remains for these component agency systems.

---

[12]The CIO Council is comprised of CIOs and Deputy CIOs from 28 large federal departments and agencies, 2 CIOs from small federal agencies, agency representatives from OMB, and the Chairs of the Government Information Technology Services Board and Information Technology Resources Board.

[13]USDA's last quarterly report to OMB, submitted in February 1998, stated that the department as a whole had 1,319 mission-critical systems, of which 539 were compliant, 261 were to be replaced, 372 were to be repaired, and 147 were to be retired. USDA's next quarterly report is due May 15, 1998.

Figure 1: Reported Year 2000 Conversion Status of Ten Component Agencies' Mission-Critical Systems, May 1998

Assessed Compliant

250

132

Repaired/Replaced

596

Work Remaining
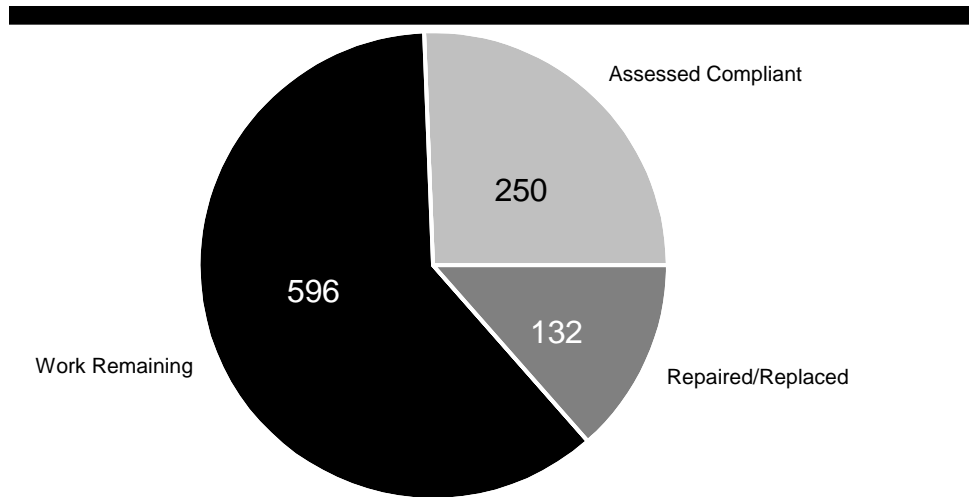
Source: USDA. We did not independently verify this information.

In addition, about 42 percent of the reported 596 mission-critical systems awaiting action are to be replaced. This is cause for some concern, as replacement systems are often a high risk because federal agencies, and USDA in particular, have a long history of difficulty in delivering planned systems on time. Further, some USDA replacement systems are already scheduled to miss the March 1999 implementation deadline established by OMB and are at risk of not being compliant on January 1, 2000. For example:

- AMS' planned replacement of its Marketing News Information System—which provides critical market information to producers, processors, and distributors of agricultural commodities throughout the United States—is currently not scheduled to be implemented until August 1999. Further adding to the risk of this tight schedule is the fact that AMS is currently not working on this and three other replacement systems (which are scheduled to be implemented in September 1999), pending approval by the CIO to do so.
- Although ARS plans to replace its existing Nutrient Data Bank System, it does not yet have a contract in place to develop it. Concerned that it may not meet USDA's March 1999 deadline, ARS now plans to develop a contingency plan.

- In April 1998 Forest Service decided to delay agencywide implementation of the Foundation Financial Information System[14] until October 1, 1999, because of significant unresolved issues related to its capabilities.[15] Forest Service has not yet decided what to do about the over 20 existing applications that are scheduled to be replaced by the Foundation Financial Information System.

In addition to these risks, we identified two agencies that were inaccurately reporting the number of compliant systems. GIPSA and RMA reported 1 and 14 systems, respectively, as compliant, even though these systems were under development or were planned. The GIPSA Year 2000 Executive Sponsor stated that the GIPSA system was reported as compliant because the system is replacing a manual process. According to the RMA Year 2000 Program Manager, RMA systems were reported as compliant because they were being developed as compliant. We do not agree with GIPSA and RMA. It is misleading to list systems as compliant when work is still to be completed. USDA's Year 2000 Program Executive stated that he agreed that these systems should not be listed as compliant.

At the same time that USDA is facing an enormous challenge to replace, repair, and retire its mission-critical systems, component agencies are beginning to report losses of information technology staff. While USDA has not performed a departmentwide assessment of its Year 2000 technology staffing needs and losses, several component agencies have recently expressed concern that the loss of staff will affect their ability to complete their Year 2000 programs. For example, FSA stated that it had lost 28 of 403 (7 percent) of its information technology staff between October 1997 and April 1998, and Forest Service officials said that they lost 12 information technology staff in the past 5 months. Moreover, in its May 1998 report, Forest Service reported losing contractors to better paying positions. The CIO has taken some action, such as obtaining a waiver from the Office of Personnel Management that allows USDA to rehire former federal personnel without financial penalty. However, according to USDA, this rehiring authority does not cover USDA employees who left the agency under the department's specific buyout authority.

---

[14]USDA's Office of the Chief Financial Officer has overall responsibility for implementing this system USDA-wide. The Office of the Chief Financial Officer shares responsibility with the Forest Service for implementing the system at this component agency.

[15]Our report, Forest Service: Status of Progress Toward Financial Accountability (GAO/AIMD-98-84, February 27, 1998) details some of these problems.

USDA will incur substantial costs to implement its Year 2000 program. It has estimated its Year 2000 costs at $118 million (as of February 1998). However, this estimate does not include all Year 2000-related costs, such as (1) FNS' share of repairing or replacing the state systems that are used to implement its programs and (2) the cost to renovate or replace telecommunications or vulnerable systems (which USDA defines as embedded systems such as laboratory equipment and facility systems). At the request of the Year 2000 Program Office, some component agencies started reporting these cost estimates and USDA intends to incorporate the costs to renovate or replace telecommunications and vulnerable systems in its next quarterly report to OMB, due May 15, 1998.

Major Weaknesses in Component Agency Efforts

Although agencies should have completed the assessment phase of Year 2000 readiness last summer, critical assessment tasks for many USDA agencies remain unfinished. Even some basic tasks, such as inventorying systems, have not yet been completed. For example, while some of the component agencies in our review reported having completed inventories of telecommunications and vulnerable systems, most have not. USDA expects these inventories to be completed this July.

Table 1 identifies key tasks that should be done during the assessment or renovation phases, yet remain incomplete in many cases.

Table 1: Reported Status of Component Agencies' Completion of Critical Assessment/Renovation Tasks

USDA agency	Detailed project tracking	Actual costs tracked	Test or validation strategy	Contingency/continuity plans intended
AMS	No	Some	Planned	Planning to develop system-related contingency plans
APHIS	Yes	Some	Draft	Planning to develop system-related contingency plans
ARS	No	Some	Planned	Planning to develop system-related contingency plans
FNS	Yes	Yes	Yes	If system is behind schedule
Forest Service	Some	Some	Draft	If system is behind schedule
FSA	Yes	Yes	Yes	One system-related plan completed
FSIS	No	No	Planned	If system is behind schedule
GIPSA	Yes	Some	Planned	Planning to develop system-related contingency plans
NASS	No	Yes	No	Draft
RMA	No	Some	No	Planning to develop system-related contingency plans

Source: GAO's analysis based on USDA data.

According to our Year 2000 readiness guide,[16] agencies should track their renovation and replacement efforts and use project metrics to manage costs and schedules. Although all of the component agencies we reviewed performed some form of project tracking, many of the component agencies' Year 2000 program offices did not track baseline to actual completion dates for project milestones, or track the percentage of milestone completion. Also, Forest Service currently performs detailed tracking for only its major applications but plans to perform such tracking for all of its applications in the future. Moreover, while three component agencies tracked actual costs, one did not, and others tracked some costs but not others, such as contractor costs but not staffing.

---

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

As expressed in our Year 2000 readiness guide, the scope of a component agency's testing and validation requires careful planning; accordingly, overall testing and validation strategies should initially be developed during the assessment phase. However, eight of the ten component agencies in our review lacked such strategies; only FNS and FSA had them. Moreover, in some agencies—such as NASS and FSIS—only the programmers who made the changes or developed the systems determined the scope of the tests to be completed. In addition, while FNS had a testing strategy, it planned to implement this strategy only for about half of its mission-critical systems; it lacks a testing strategy for the other mission-critical systems. According to an FNS official, the other systems will be tested through a combination of the responsible contractor or FNS staff who made the change and user acceptance testing. One of these systems is vital to ensuring that schools and other entities are reimbursed for providing food services to children and adults.

In reviewing the test documentation of systems that were repaired or replaced at FNS and FSA to determine whether their testing strategies were followed for the three systems that these agencies reported as Year 2000 compliant, we found mixed results.

- The FNS system, called the National Integrated Quality Control System—used by state welfare agencies to perform federally-mandated quality control functions—was not one of the systems covered by FNS' test strategy, and we were unable to verify whether the system was indeed Year 2000 compliant. The system was replaced by a contractor who conducted limited Year 2000 testing; neither FNS nor the contractor had developed test plans for the system. Further, while FNS utilized its regional offices and nine states for acceptance testing, it did not provide instructions on what to test, and had no documentation concerning exactly what was tested. As a result, FNS officials did not know whether the testing included any Year 2000 test scenarios.
- Two FSA mission-critical systems had more positive results. Written test plans existed, the testing was carried out by an independent organization, and test result documentation showed that sufficient testing had been performed to determine that the system was Year 2000 compliant.

Turning to business continuity and contingency planning, most of the component agencies intended to develop contingency plans only for specific systems or only if the systems were likely to miss the USDA March 1999 deadline for compliance. Agencies that develop contingency plans only for systems currently behind schedule, however, are not addressing

the need to ensure the continuity of a minimal level of core business operations in the event of unforeseen failures. As a result, when unpredicted failures occur, agencies will not have well-defined responses and may not have enough time to develop and test effective contingency plans. Contingency plans should be formulated to respond to two types of failures: those that can be predicted (e.g., system renovations that are already far behind schedule) and those that are unforeseen (e.g., a system that fails despite having been certified as Year 2000 compliant or a system that cannot be corrected by January 1, 2000, despite appearing to be on schedule today).

Moreover, contingency plans that focus only on agency systems are inadequate. Federal agencies depend on data provided by their business partners as well as on services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. Given these interdependencies, it is imperative that contingency plans be developed for all critical core business processes and supporting systems, regardless of whether these systems are owned by the agency. NASS was the only component agency in our review that had drafted a plan to address the agency's options in the event that Year 2000-induced failures do not enable it to use its normal processes to develop and issue its January 2000 statistical reports. NASS intends to finalize this plan in the fall of 1998.

More Effective Departmental Leadership Required

Given the enormous potential risk, USDA has determined that the Year 2000 crisis is its top information technology priority. It has not, however, translated that sentiment into effective action. The department's role has remained limited—a condition that cannot continue if sufficient progress is to be achieved.

USDA Has Not Identified Its Highest Priority Systems

Just as federal departments and agencies establish their own priorities among mission-critical systems, we have recommended that the government as a whole determine national priorities.[17] Similarly, it is important for the Secretary of Agriculture to know, as time dwindles, which mission-critical systems are USDA's highest priorities. However, USDA's CIO stated that the department has not set Year 2000 priorities. Priority setting has, rather, been left to the individual component agencies, which determined which systems are mission-critical.

---

[17]GAO/AIMD-98-85, April 30, 1998.

The component agencies judged systems to be mission-critical in an inconsistent manner. For example, while Forest Service tells us that it has 17 mission-critical systems, it has reported to the department that it has 423 mission-critical systems.[18] This is because Forest Service reported applications and not systems. Forest Service reports applications rather than systems because it tracks its system migration and Year 2000 project at the application level. Further, not all of these applications are critical. For example, a January 1998 Forest Service analysis of the applications that it plans to repair indicated that only 48 of 137 are critical applications.

Another example of USDA's inconsistent reporting is provided by USDA's two data centers, the National Information Technology Center (NITC) and the National Finance Center (NFC). NITC reported as mission-critical the systems that support its infrastructure (e.g., operating systems and utilities), while NFC reported its application systems but not the systems that support its infrastructure.

We further found that the department's Year 2000 Program Office and most of the component agencies lacked a key piece of information necessary for setting such priorities: the system's failure date. This is the first date that a system will fail to recognize and process dates correctly.

The Year 2000 Program Office Has Performed Limited Oversight

The oversight provided by the Year 2000 Program Office has been limited to monthly meetings with component agency executive sponsors, regularly scheduled meetings on topics such as telecommunications and reviews of monthly status reports, and written guidance on awareness and assessment. In lieu of developing additional written guidance, the Year 2000 Program Executive stated that he told the component agencies to use our readiness guide.[19]

Further, the program office maintains no up-to-date portfolio of components' mission-critical systems, and has performed only limited analysis of what it does have. For example, in November 1997, the Program Office collected information on the (1) planned completion date of the awareness, assessment, renovation, validation, and implementation dates of systems to be renovated; (2) implementation dates of replacement systems; and (3) planned dates for systems to be retired. This information was updated in February 1998. However, the Year 2000 Program Office did

---

[18]Forest Service reported an additional 59 mission-critical systems that we did not include because the agency had retired them.

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

not compare the November 1997 and February 1998 data to determine whether there were any changes that needed to be reviewed. Further, many of the dates in the February 1998 inventory were questionable. For example:

- In 39 cases, the validation date was before the renovation date.
- In 40 cases, there were no dates for renovation and/or validation.
- In 233 cases, the renovation date equaled the validation date.

To assist the Year 2000 Program Office in identifying and selecting appropriate courses of action, on April 29, 1998, the program office awarded a contract for a review of its plans, documentation, and products. Among other items, the contractor is to review whether mission-critical systems have been appropriately identified, Year 2000 time frames are realistic, appropriate test plans are being developed and implemented, and the Year 2000 program office is appropriately staffed. In addition, the contractor is to identify Year 2000 testing methodologies and risks, and risk mitigation strategies. These deliverables are expected in about a month.

Observations on the Farm Credit Administration and the Commodity Futures Trading Commission

At your request, Mr. Chairman, we also reviewed the Year 2000 readiness of the Farm Credit Administration (FCA) and the Commodity Futures Trading Commission (CFTC), two independent agencies that regulate, respectively, the Farm Credit System and the futures and options industry. FCA and CFTC are concerned not only with the Year 2000 compliance of their internal systems, but also with those of the institutions they regulate. These organizations are heavily dependent on information technology, and Year 2000-induced failures on the part of the industries that FCA and CFTC regulate could have repercussions for the financial services industry and the national economy.

The Farm Credit Administration

FCA regulates, and performs periodic examinations of, the entities that make up the Farm Credit System. The Farm Credit System consists of a network of banks, associations, cooperatives, and other related entities that make short, intermediate, and long-term loans. In addition, FCA oversees the system's fiscal arm that markets its debt securities and the Federal Agricultural Mortgage Corporation that provides a secondary market for mortgage loans secured by agriculture real estate and rural housing. Its risks associated with the century change are similar to those of other financial institutions: errors in interest calculation and

amortization schedules. In addition, the Year 2000 problem may expose the institutions and data centers to financial liability and loss of customer confidence.

With respect to their internal systems, FCA identified 25 mission-critical systems of which FCA considers 17 compliant. Of the 8 considered by FCA to be noncompliant systems, 6 are being repaired, 1 is being replaced, and 1 is being retired. Two of the systems being repaired are the responsibility of other entities, USDA's National Finance Center's payroll processing system and the Department of the Treasury's electronic payment system. FCA does not have a written test or validation strategy for any of its internal systems. At the conclusion of our review, FCA officials told us that they plan to develop a written test strategy by the end of this month.

To address the Year 2000 readiness of its regulated institutions, FCA has (1) had its institutions provide responses to a Year 2000 questionnaire, (2) conducted reviews of institutions' Year 2000 programs during its examinations, and (3) issued informational memoranda to the institutions. For example, in November 1997, December 1997, and March 1998, FCA asked its regulated institutions to complete Year 2000 questionnaires. Additionally, in November 1997, FCA issued Year 2000 examination procedures for its examiners. As of March 30, 1998, FCA reported completing 58 safety and soundness examinations that included a review of the institutions' Year 2000 programs. In addition, 15 examinations were in process and 85 were planned through the end of fiscal year 1998. According to FCA, it will perform targeted Year 2000 examinations by December 30, 1998, for institutions that are not scheduled for a safety and soundness examination in fiscal year 1998.

Both the questionnaire and the examination procedures were based on the guidelines developed by the Federal Financial Institutions Examination Council.[20] We have previously reported[21] that the Council's guidance and procedures were not designed to collect all the data needed to determine where (i.e., in which phases) the institutions are in the Year 2000 correction process. FCA plans to issue this June a more detailed questionnaire requesting more specific information on renovation, testing,

---

[20]This organization is made up of the following federal regulators: the Federal Reserve System, the Comptroller of the Currency, the National Credit Union Administration, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision.

[21]Year 2000 Computing Crisis: Federal Regulatory Efforts to Ensure Financial Institution Systems Are Year 2000 Compliant (GAO/T-AIMD-98-116, March 24, 1998).

and validation. In addition, on March 31, 1998, FCA issued new examination procedures that superseded those of November 1997.

FCA has assessed the risks that each of its institutions face based on the responses to the questionnaire, as well as the knowledge of its examiners. Each institution was placed in one of three risk categories—low, moderate, or critical. As of March 31, 1998, 70 institutions were in the low risk category in that the institutions met FCA's guidelines; 71 were classified as at moderate risk, where some key actions have not been completed or were not consistent with FCA guidelines; and 74 were classified as critical, where actions have not been taken in key areas and there is an increased risk that the institution will not be prepared for the year 2000.

The informational memoranda that FCA has issued to the institutions that it regulates covered issues such as testing and establishing a due-diligence process to determine the Year 2000 readiness of service providers and software vendors. However, FCA has not called for the regulated institutions to develop business continuity and contingency plans unless certain deadlines are not met or service providers and software vendors have not provided adequate information about their Year 2000 readiness, or where the provider or vendor solutions do not appear to be viable. As I stated earlier, business continuity and contingency plans should be formulated to respond to those types of failures that can be predicted (e.g., system renovations that are already far behind schedule) and those that are unforeseen (e.g., a system that fails despite having been certified as Year 2000 compliant or a system that cannot be corrected by January 1, 2000, despite appearing to be on schedule today). In response to our review, FCA officials stated that they would issue an information memorandum by the end of May requiring institutions to develop business continuity and contingency plans for all core business processes.

Commodity Futures Trading Commission

CFTC's mission is to protect market participants from manipulation, fraud, and abusive trade practices, related to the sale of commodity futures and options and to foster open, competitive, and financially sound commodity futures and options markets. CFTC works in conjunction with self-regulatory organizations (SRO), such as the commodity exchanges and independent clearinghouses to regulate these markets. All companies and individuals handling customer funds or providing trading advice must register with the Commission and be a member of at least one of these organizations. SROs audit their member institutions, and CFTC regularly

reviews SROs' audit activities. The SROs and member institutions are, not surprisingly, very reliant on information technology, with many interdependencies among them; these include foreign firms and exchanges as well. Major Year 2000 failures could easily, then, have worldwide economic repercussions.

CFTC reports having two mission-critical systems, which it states it repaired to be Year 2000 compliant in 1993 and 1994. It has also inventoried and assessed its external data exchanges, telecommunications, and personal computers; it plans to upgrade its personal computers and network servers next month and replace noncompliant equipment and a noncompliant network operating system by March 1999.

Regarding CFTC's oversight of SROs, on March 18, 1998, CFTC sent a letter to all exchanges and independent clearinghouses requesting information on the Year 2000 readiness status of SRO, SRO's member firms, and floor brokers and floor traders. In particular, CFTC requested information on (1) contingency plans, both with regard to processes that cannot be made compliant in the necessary time frame and for instances in which, despite the best plans, procedures developed to address the Year 2000 problem do not work, (2) whether and how SRO can ensure full participation in the Year 2000 testing being planned by the Futures Industry Association,[22] and (3) SRO's authority under its own rules to intervene and, if necessary, restrict or terminate the member's business, and what procedures would apply. CFTC asked SROs to provide the information by May 15, 1998. CFTC has a coordinator for external Year 2000 activities who will evaluate SRO responses with assistance from CFTC's Office of Information Resources Management, which is in charge of CFTC's internal systems, and CFTC's audit and evaluation group.

Although CFTC has not yet reviewed the Year 2000 readiness of the SRO member institutions, it has worked with the SRO audit organization, the Joint Audit Committee.[23] The members of this committee have requested that the registrants for which they are responsible fill out questionnaires on their Year 2000 progress. According to CFTC's Chief Accountant, CFTC's auditors will (1) confirm that the SRO auditors had sent the questionnaires to its members, (2) determine whether SRO auditors had reviewed the questionnaires for completeness and unusual items, and (3) determine

---

[22]The Futures Industry Association plans to hold a series of industry tests beginning in June 1998 and continuing through the first quarter of 1999.

[23]This committee is a representative committee of U.S. futures exchanges and regulatory organizations.

whether SRO auditors had followed up on any exceptions found. However, because CFTC does not have any electronic data processing auditors, it may have difficulty assessing the SRO's Year 2000 audit activities.

CFTC also issued advisory notices, in November 1997 and April 1998, and has participated in meetings with the Futures Industry Association. The advisory notices asked the SROs to report on their Year 2000 programs, asked the SRO auditors to include a Year 2000 readiness inquiry to their inspections, set disclosure requirements for institutions with Year 2000 problems, and strongly encouraged registrants to share information with SROs and membership organizations.

While CFTC has taken some action to address the effect the year 2000 will have on the futures and options markets, the potential major disruption that the year 2000 could hold for these markets suggests that the commission should take a strong leadership role in providing reasonable assurance that the futures and options markets will be Year 2000 compliant in time.

In conclusion, the change of century will present many difficult challenges in information technology and in ensuring the continuity of business operations, and has the potential to cause serious disruption to the nation and to government entities on which the public depends, including the Department of Agriculture. These risks can be mitigated and disruptions minimized with proper attention and management. However, much work remains at USDA and its agencies to address these risks and ensure continuity of mission-critical business operations. Continued congressional oversight through hearings such as this can help ensure that this attention is sustained and that appropriate actions are taken to address this crisis.

Mr. Chairman, this completes my statement. I would be happy to respond to any questions that you or other members of the Committee may have at this time.

GAO Reports and Testimony Addressing the Year 2000 Crisis

Year 2000 Computing Crisis: Continuing Risks of Disruption to Social Security, Medicare, and Treasury Programs (GAO/T-AIMD-98-161, May 7, 1998).

IRS' Year 2000 Efforts: Status and Risks (GAO/T-GGD-98-123, May 7, 1998).

Year 2000 Computing Crisis: Potential For Widespread Disruption Calls For Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998).

Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998).

Department of the Interior: Year 2000 Computing Crisis Presents Risk of Disruption to Key Operations (GAO/T-AIMD-98-149, April 22, 1998).

Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, Exposure Draft, March 1998).

Tax Administration: IRS' Fiscal Year 1999 Budget Request and Fiscal Year 1998 Filing Season (GAO/T-GGD/AIMD-98-114, March 31, 1998).

Year 2000 Computing Crisis: Strong Leadership Needed to Avoid Disruption of Essential Services (GAO/T-AIMD-98-117, March 24, 1998).

Year 2000 Computing Crisis: Office of Thrift Supervision's Efforts to Ensure Thrift Systems Are Year 2000 Compliant (GAO/T-AIMD-98-102, March 18, 1998).

Year 2000 Computing Crisis: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions (GAO/T-AIMD-98-101, March 18, 1998).

Post-Hearing Questions on the Federal Deposit Insurance Corporation's Year 2000 (Y2K) Preparedness (AIMD-98-108R, March 18, 1998).

SEC Year 2000 Report: Future Reports Could Provide More Detailed Information (GAO/GGD/AIMD-98-51, March 6, 1998).

Year 2000 Readiness: NRC's Proposed Approach Regarding Nuclear Powerplants (GAO/AIMD-98-90R, March 6, 1998).

Year 2000 Computing Crisis: Federal Deposit Insurance Corporation's Efforts to Ensure Bank Systems Are Year 2000 Compliant (GAO/T-AIMD-98-73, February 10, 1998).

Year 2000 Computing Crisis: FAA Must Act Quickly to Prevent Systems Failures (GAO/T-AIMD-98-63, February 4, 1998).

FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically (GAO/AIMD-98-45, January 30, 1998).

Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998).

Year 2000 Computing Crisis: Actions Needed to Address Credit Union Systems' Year 2000 Problem (GAO/AIMD-98-48, January 7, 1998).

Veterans Health Administration Facility Systems: Some Progress Made In Ensuring Year 2000 Compliance, But Challenges Remain (GAO/AIMD-98-31R, November 7, 1997).

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).

Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain (GAO/AIMD-98-6, October 22, 1997).

Defense Computers: Technical Support Is Key to Naval Supply Year 2000 Success (GAO/AIMD-98-7R, October 21, 1997).

Defense Computers: LSSC Needs to Confront Significant Year 2000 Issues (GAO/AIMD-97-149, September 26, 1997).

Veterans Affairs Computer Systems: Action Underway Yet Much Work Remains To Resolve Year 2000 Crisis (GAO/T-AIMD-97-174, September 25, 1997).

Year 2000 Computing Crisis: Success Depends Upon Strong Management and Structured Approach (GAO/T-AIMD-97-173, September 25, 1997).

Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997).

Defense Computers: SSG Needs to Sustain Year 2000 Progress (GAO/AIMD-97-120R, August 19, 1997).

Defense Computers: Improvements to DOD Systems Inventory Needed for Year 2000 Effort (GAO/AIMD-97-112, August 13, 1997).

Defense Computers: Issues Confronting DLA in Addressing Year 2000 Problems (GAO/AIMD-97-106, August 12, 1997).

Defense Computers: DFAS Faces Challenges in Solving the Year 2000 Problem (GAO/AIMD-97-117, August 11, 1997).

Year 2000 Computing Crisis: Time is Running Out for Federal Agencies to Prepare for the New Millennium (GAO/T-AIMD-97-129, July 10, 1997).

Veterans Benefits Computer Systems: Uninterrupted Delivery of Benefits Depends on Timely Correction of Year-2000 Problems (GAO/T-AIMD-97-114, June 26, 1997).

Veterans Benefits Computers Systems: Risks of VBA's Year-2000 Efforts (GAO/AIMD-97-79, May 30, 1997).

Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses (GAO/AIMD-97-78, May 16, 1997).

Medicare Transaction System: Serious Managerial and Technical Weaknesses Threaten Modernization (GAO/T-AIMD-97-91, May 16, 1997).

Year 2000 Computing Crisis: Risk of Serious Disruption to Essential Government Functions Calls for Agency Action Now (GAO/T-AIMD-97-52, February 27, 1997).

Year 2000 Computing Crisis: Strong Leadership Today Needed To Prevent Future Disruption of Government Services (GAO/T-AIMD-97-51, February 24, 1997).

High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested