



U. S. AGENCY FOR
INTERNATIONAL
DEVELOPMENT

December 16, 1999

MEMORANDUM FOR DAA/M, Richard C. Nygard

FROM: IG/A/ITSA, Theodore P. Alves

A handwritten signature in dark ink, appearing to read "T. P. Alves".

SUBJECT: Audit of USAID's Efforts to Develop Year 2000 Contingency Plans
(Audit Report No. A-000-00-002-P)

This report presents the results of our audit of the U.S. Agency for International Development's (USAID) efforts to develop Year 2000 (Y2K) contingency plans. We conducted the audit to determine whether USAID has developed adequate contingency plans to ensure business continuity in the event of a Y2K problem. The audit found that USAID has a business continuity plan but it is inadequate because it focuses only on financial management operations. Contrary to Office of Management and Budget (OMB) requirements and General Accounting Office (GAO) guidance, USAID has not developed contingency plans for its core business functions such as emergency humanitarian and development assistance activities provided by the Bureau for Humanitarian Response, the Bureau for Africa, and the Global Bureau.

This report concludes that because USAID has not followed the disciplined approach called for by GAO, it faces unnecessary risks of encountering disruptions to its humanitarian and development assistance programs as result of a Y2K problem.

The report contains two recommendations (see page 11). Recommendation No. 1 is closed upon issuance of this report. Regarding Recommendation No. 2, we consider that a management decision has been reached based on management's response to the draft report. The full text of the management comments is included as Appendix II of this report.

Thank you for the cooperation and assistance extended to our staff during this audit.

Background

The Y2K problem—potential problems that might be encountered by computer systems when processing information related to dates on or after January 1, 2000—is primarily a business problem, according to the GAO. With many organizations facing the risk of Y2K-induced interruptions or failures of their core business processes, the GAO has stressed the importance of developing contingency plans to ensure continuity of business operations, and issued guidelines to help agencies complete contingency plans.¹ To ensure that federal agencies are prepared, OMB required USAID and other federal agencies to develop and submit high-level Business Continuity and Contingency Plans (BCCP). OMB asked the agencies to follow the GAO guide to prepare the plans. The GAO guide approaches contingency planning in four phases: initiation, business impact analysis, contingency planning, and testing. Appendix III describes in detail the contingency planning processes in the GAO guide.

Business continuity and contingency planning ensures the continuity of an agency's core business processes by identifying, assessing, managing, and mitigating its Y2K risks. This effort focuses on risks posed by Y2K-induced failures of internal information systems, as well as the potential failures of others, including business partners and infrastructure service providers. The business continuity planning process safeguards an agency's ability to produce a "minimum acceptable level" of outputs and services in the event of failures of internal or external critical information systems and services. It also helps facilitate the restoration of normal service at the earliest possible time and in the most cost-effective manner.

USAID needs a BCCP because it is responsible for important humanitarian and development assistance programs that help advance U.S. economic and political interests worldwide. USAID is the primary agency of the United States that helps other countries recover from disasters, escape poverty, and embrace democratic processes. USAID accomplishes its goals through its bureaus and offices in Washington, D.C., and its missions located in about 80 countries around the world.

To ensure continuity of its programs in Year 2000 and beyond, USAID has taken the following notable actions:

- Recognizing the difficulties it faces dealing with Y2K issues, USAID identified its Y2K program as a material weakness in its fiscal year 1998 Integrity Act Report to the President.
- USAID has developed contingency plans for its Washington, D.C. and missions financial management operations. The plans are designed to ensure that USAID has available alternative methods to perform its essential accounting functions of obligating funds, controlling funds, and making payments.

¹ Year 2000 Computing Crisis: *Business Continuity and Contingency Planning*, (GAO/AIMD-10.1.19, August 1998).

- USAID, through the Global Y2K Consortium, has developed inexpensive and easy to distribute tools to help developing countries address Y2K problems. The tools are designed to shorten or “fast-track” the process of fixing systems, preparing contingency plans, and recovering from Y2K-induced disruptions.
- Some USAID Bureaus and Missions such as the Bureau for Europe and Eurasia and USAID/Cairo have drafted specific contingency plans for their missions.
- The USAID Y2K Program Office regularly provides Y2K updates to USAID program managers. These updates provide current information about Y2K issues affecting government, private industry, and international organizations.

On June 15, 1999, USAID submitted its BCCP to the OMB. In the plan, USAID recognized that Year 2000 has the potential to adversely affect its work at its headquarters in Washington and through the many locations where USAID is represented abroad. USAID therefore asserted that preparations must be made to assure that it can continue to operate despite the worst that Year 2000 could bring to the developing world.

Audit Objective

We performed this audit to answer the following audit question:

- **Has USAID developed adequate business continuity and contingency plans in accordance with the GAO guidance?**

Appendix I includes a discussion of the scope and methodology for this audit.

Summary of Results

USAID has not yet developed adequate business continuity and contingency plans to ensure the continuity of its operations should critical computer systems fail to operate as intended in the Year 2000 and beyond. Although USAID used the GAO guidance to develop its BCCP, it has not yet completed key steps for all USAID business processes, such as delivery of emergency humanitarian assistance overseas; procurement and delivery of contraceptive overseas; and development assistance through its overseas missions. These key steps include identifying all core business processes, analyzing risks and possible Y2K impact, documenting contingency plans and implementation modes, and testing. As a result, USAID faces increased risks that it will encounter disruptions in the event of Y2K system failures.

On the other hand, USAID did not develop contingency plans for its other core business processes, such as those performed by the Global Bureau, the Bureau For Humanitarian Response, and the Bureau for Africa. Also, in its agency-wide business continuity and contingency plan to the OMB, USAID did not address all critical business processes. The plan did not identify and document implementation modes, did not define triggers for activating the contingency plans, and did not establish business resumption teams for these core business processes. Our subsequent reviews in the Bureau for Humanitarian Response, the Bureau for Africa, and the Global Bureau confirmed that USAID did not develop contingency plans for the programs managed by these organizations. The following is an example of USAID's failure to develop contingency plans for its core activities.

Humanitarian Assistance Activities Lack Contingency Plans

USAID provides immediate humanitarian assistance when disasters strike. For example, USAID provides daily rations, plastic sheeting, water, and water bottles to help people to recover from natural or man-made disasters, such as hurricane Mitch that hit Central America and the earthquake in East Timor. USAID reported that in 1997 it provided 780,000 metric tons of emergency food aid, through the P.L. 480 program, to more than 11.5 million people in 28 countries. Additionally, the USAID Office of Foreign Disaster Assistance reported that it provided emergency assistance; primarily in health, sanitation, shelter, and water, totaling \$140 million to help 18 million disaster victims in 46 countries. USAID may also be called on to provide humanitarian assistance to help countries recover from Y2K-induced problem, yet the organization responsible, the Bureau for Humanitarian Response has not developed contingency plans for its business functions.

The Bureau for Humanitarian Response carries out its functions through five primary offices: Office of Food for Peace, Office of Transition Initiatives, Office of Private and Voluntary Cooperation, Office of American Schools and Hospitals Abroad, and the Office of Foreign Disaster Assistance. To determine whether USAID has developed contingency plans for its humanitarian assistance function, we contacted these offices to review their Y2K efforts. To its credit, the bureau acquired a contractor to assess the computer systems within the bureau for Y2K compliance. However, none of the Bureau for Humanitarian Response offices had developed a contingency plan. Therefore, Y2K risks to these very important agency functions are left unmitigated.

One responsible official told us that he did not think contingency plans are needed because the existing arrangements are adequate. He noted that the office has agreements with contractors to supply goods, and an agreement with the Department of Defense to provide airlift capabilities if needed. Another official also stated that USAID has three fully stocked depots positioned in the state of Maryland, Italy, and Guam. However, if extensive Y2K problems develop, the Bureau might be called on to respond at a time when these support services might not be readily available. In a recent testimony to a U.S. Senate Committee, the Central Intelligence Agency observed that Y2K has unique capacity to produce multiple, simultaneous crises. The CIA also stated that it expects calls for the U.S. to intervene in humanitarian crisis resulting from Y2K problems abroad. Following GAO's disciplined process would help officials consider how to deal with potential problems such as inadequate supplies for victims, unavailable transportation, or a shortage of human resources to deliver the supplies. An indicator that transportation

problems could affect supply routes, on September 9, 1999, the Coast Guard restricted the operations of 175 U.S. ships and 85 port facilities because it did not have adequate assurance that their Y2K risks had been resolved.

Testing: Plans Not Adequately Tested

Key steps during the testing phase of the business continuity and contingency planning process include developing test plans, preparing and executing tests, rehearsing business resumption teams, and updating business continuity plans based on lessons learned. Testing is important because it evaluates the contingency plans' capability of providing the desired level of support to the core business processes and whether the plans can be implemented within a specific period of time. Unless USAID tests contingency plans it cannot be assured that they will be effective in the event of Y2K-induced business failures.

Our review showed that USAID had performed some testing of its financial management processes but had not completed all the testing steps recommended. However, for other important business functions, USAID has not developed test plans, established business resumption teams, or provided training to ensure that the staff is familiar with the business resumption procedures and their roles. The agency-wide BCCP did not document any testing planned for USAID's development assistance activities.

M/FM Contingency Plans Need Adequate Testing

Concerning the Financial Management Operations, USAID had two contingency plans, one for the missions and the other for Washington D.C. operations. We found that each mission was provided a copy of the Contingency Plan for Financial Management Operations dated August 24, 1999, which details the manual procedures mission controllers would use for financial management operations in case of a Y2K disruption. The missions were further instructed to form business resumption teams, to rehearse the contingency plans and to report their results to USAID/Washington by September 1, 1999. As of October 21, 1999, USAID records show that 44 missions have provided some responses on testing. Several of the missions commented on problems encountered and suggested their approach to dealing with the problems, others posed questions back to M/FM. Overall, the responses did not clarify whether that the tests have been successfully completed. M/FM officials have also not analyzed these responses to identify common problems and update the plans.

Regarding the Washington D.C. operations, USAID records show that two tests were performed. The first test was performed on June 29, 1999, and the second test on July 2, 1999. During the first test, a total of 76 transactions were recorded on 21 coding sheets. Eighteen of those sheets related to obligations, three related to payments, and none related to funds control. During the second test, only five payments transactions were made. Furthermore, M/FM officials informed us that the business resumption teams for the Washington D.C. operations have not yet been named. Given the lack of analyses of the mission tests, the low number of transactions tested in Washington D.C., the lack of Funds Control tests, and the lack of business resumption teams rehearsing the procedures, USAID does not yet have assurance that its financial management

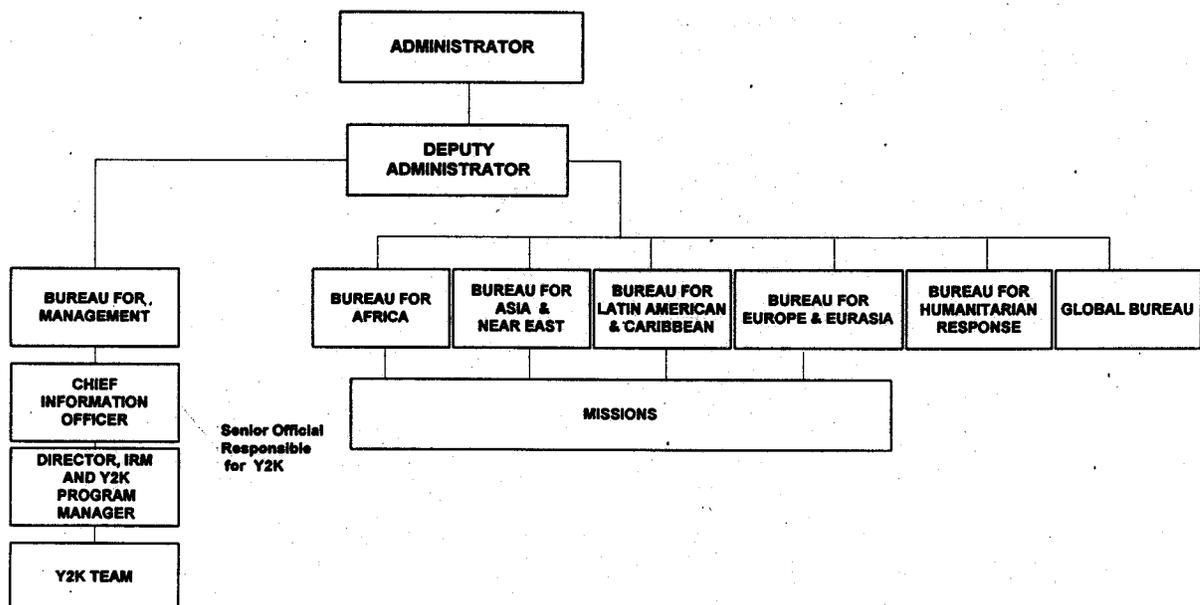
operations contingency plans are adequate. USAID continues to face risks of disruptions to its financial management operations.

**Roles and Responsibilities
Need to be Clearly Assigned**

The risks identified in this report exist primarily because USAID has not adequately responded to two key recommendations from a prior audit report.² That report pointed out that USAID had not completed several steps that address Y2K challenges, including preparing contingency plans. USAID had not done so because the Y2K team lacked the authority to require Bureaus and Missions to address Y2K issues. The report recommended that (1) the Administrator clearly assign responsibility and authority for implementing the Y2K program, and (2) the responsible official then direct Bureaus and Missions to develop and test contingency plans. According to senior USAID officials, the Administrator directed the Bureaus to ensure that adequate plans were prepared. However, this action did not fully correct the deficiency because a single manager was not assigned the responsibility, authority, and resources to ensure adequate plans were developed.

Bureaus and Missions were not more engaged in the project because the Y2K team did not have adequate authority to require other organizations to address Y2K issues. The Y2K team, which is located in the M/IRM office, reported through the Y2K Program Manager to the Chief Information Officer (CIO). The CIO, the senior official responsible for the Y2K effort, was organizationally located in the Bureau for Management and did not have authority to direct Bureaus and Missions. The following organization chart describes the structure for USAID's

Table 2: USAID/YEAR 2000 ORGANIZATIONAL CHART



² Audit of USAID's Assessment of the Year 2000 Problem (Audit Report No. A-000-98-006-P, September 21, 1998)

Y2K program and shows that the Y2K team is located several hierarchy levels below the Bureaus and Missions.

The report recommended that the Administrator clarify the assignment of responsibility to implement the Y2K program and provide the responsible official adequate authority and resources to complete it. To address the lack of contingency planning, the report recommended that the responsible Y2K official direct Bureaus and Missions to develop and test contingency plans. According to a senior USAID official, the Administrator met with the head of each Bureau to emphasize the importance of completing business continuity and contingency plans and received assurance that the Bureaus had adequate plans in place. Although this action partially addressed the recommendations, in our opinion, it did not correct the problem because USAID did not identify a single responsible manager.

Without a responsible manager it is difficult to establish effective controls, provide appropriate oversight, and hold other managers accountable for results. GAO's Standards for Internal Control in the Federal Government emphasize the need for agencies to clearly define responsibility and authority and to establish clear reporting lines. GAO's internal control standards also require a system of internal controls to ensure that important activities are performed correctly. A single responsible manager would help USAID to implement effective controls over the Y2K effort, ensuring that adequate resources are devoted, GAO guidelines are followed, and results meet quality control standards.

Recommendations

We are making two recommendations to correct the problems identified in this report.

Recommendation No. 1: We recommend that the Assistant Administrator for Management requests the Administrator to make a senior executive responsible and accountable for developing contingency plans; and give the individual the authority and resources to ensure that the plans are developed.

Recommendation No. 2: We recommend that the Assistant Administrator for Management ensure that the contingency plans for the financial management operations are completely tested in accordance with the GAO guide.

Conclusion

Because USAID has not followed the disciplined approach called for by GAO, it has not completed adequate contingency plans for its development assistance programs and is, therefore, facing unnecessary risks of encountering disruptions to its development assistance activities. As we noted earlier, some USAID Missions and Bureaus, such as, USAID/Cairo and the Bureau for Europe and Eurasia, are drafting contingency plans that address USAID development assistance activities. This effort needs to be implemented throughout USAID. The designation of the Deputy Administrator as USAID's Senior Policy Official on Y2K and the Agency's recent instructions to all missions to review mission contingency plans for adequate coverage of mission program activity and continuity will help mitigate the existing risks.

Management Comments and Our Evaluation

In response to the draft report, USAID concurred with the two recommendations contained in the report. On September 30, 1999, the Administrator designated the Deputy Administrator as USAID's senior policy official on Y2K. She was assigned the responsibility to ensure that the bureaus and missions take all necessary steps regarding contingency planning to permit the Agency to continue operations into the new year. On November 29, 1999, the Deputy Administrator directed all missions to verify that the missions contingency plans provide for continuity of core mission functions and the provision for humanitarian and development assistance. In its response, USAID also advised that an Agency Task Force has been established and each bureau is organizing appropriate personnel into Bureau Response Teams. Therefore, based on the USAID's actions, Recommendation No. 1 is closed upon issuance of this report.

Recommendation No. 2 calls for USAID to ensure that contingency plans for the financial management operations are completely tested in accordance with the GAO guide. The response stated that the Office of Financial Management (M/FM) has concluded that its testing phase activities probably met the letter of the GAO guidelines. However, M/FM accepts that taking the additional steps identified by OIG will further reduce business risk to the Agency. One of the steps M/FM plans to take is to analyze the responses from the missions to confirm that each mission can implement the plan as written. We agree that a management decision has been reached. However, USAID needs to complete this action quickly because as we reported on page 9 of this report, our analysis found that some missions reported problems with their rehearsals that need to be addressed. Evidence of final action on Recommendation No. 2 should be provided to USAID's Office of Management Planning and Innovation for consideration in closing the recommendation.

SCOPE AND METHODOLOGY

Scope

We audited USAID's efforts to develop and test Y2K contingency plans. Because of Y2K risks, business continuity and contingency plans are needed to reduce the impact of Y2K failures on business operations. Our review was conducted at USAID/Washington during the period March 1999 and September 1999. This audit was conducted in accordance with generally accepted government auditing standards.

Based on a judgmental selection, we met with personnel and reviewed documentation in four USAID bureaus: the Bureau for Management, the Bureau for Humanitarian Response, the Bureau for Africa, and the Global Bureau. In the Bureau for Management, we focused on the Office of Financial Management (M/FM) and the Y2K Program Office within the Office of Information Resource Management. We also met with the Chief Information Officer (CIO) and the Deputy CIO. In the Bureau for Africa, we worked with the Y2K coordinator for program funds and the Y2K coordinator for operating expenses. In the Global Bureau, we concentrated on the activities within the Contraceptive and Logistics Management Office. We did not perform specific reviews in the Bureau for Asia and the Near East (ANE), the Bureau for Europe and Eurasia (E&E), or the Bureau for Latin America and the Caribbean (LAC).

As with our previous Y2K work, the question of independence needs to be addressed because the Office of Inspector General (OIG) also has information systems that are vulnerable to Y2K problem and needs to develop contingency plans. The second standard of generally accepted auditing standards, independence, calls for the organization and individuals conducting the audit to be organizationally independent and to maintain an independent attitude and appearance. Because deficiencies in USAID's contingency planning efforts could reflect deficiencies in OIG's activities, our organizational independence could be questioned. In order to prevent the appearance of an organizational conflict, we excluded OIG business processes from the scope of the audit. Therefore, this report does not address the adequacy of OIG contingency planning efforts.

We audited the extent to which USAID has developed and tested contingency plans and whether the plans are consistent with guidance issued by the GAO and other industry best practices. To the extent that Y2K contingency planning deficiencies existed, we identified the factors that caused the deficiencies.

Methodology

We used the GAO's contingency planning guide³ to assess USAID's contingency planning efforts. We reviewed both the plans themselves and the process followed to prepare them. We covered M/FM and business functions in three other bureaus; reviewing studies, reports, and other documents that described the planning process and results. We also discussed the issues with responsible officials, including the Y2K program manager, the Chief Information Officer (CIO), and responsible officials in the M/FM, the Bureau for Humanitarian Response, the Global Bureau, and the Bureau for Africa. We obtained oral comments from USAID management on our draft findings and incorporated those comments where appropriate.

We reviewed a copy of USAID's Business Continuity & Contingency Planning document dated June 15, 1999, which USAID submitted to OMB. This document describes USAID's contingency planning efforts and includes:

- Y2K Contingency Plan for USAID/W Financial Management Operations, and
- Y2K Contingency Plan for Mission Financial Management Operations.

We also reviewed other documentation submitted to OMB on the status of USAID's contingency planning efforts.

In addition to the above documents, we reviewed the following:

- reports on Y2K assessment performed on various missions worldwide,
- Post contingency plans from various missions in Africa,
- Mission contingency plans testing data,
- draft USAID/Cairo Contingency Plan,
- draft USAID/Cairo Command and Control Center Plan, and
- documents related to the Global Y2K Consortium.

The audit methodology was not sufficiently rigorous to detect all problems in USAID's efforts to develop and test contingency plans. Since we only audited selected bureaus and few offices within those bureaus, lack of adequate contingency planning could impact other core business process within USAID that are not identified in this report.

³ Year 2000 Computing Crisis: *Business Continuity and Contingency Planning*, (GAO)/AIMD-10.1.19, August 1998)



U.S. AGENCY FOR
INTERNATIONAL
DEVELOPMENT

MEMORANDUM

DEC 10 1999

TO: IG/A/ITSA, Theodore P. Alves

FROM: M/DAA, Richard C. Nygard *R*

SUBJECT: USAID Review of Draft IG Audit Report No.
A-000-00-XXX-P: USAID's Efforts to Develop Year
2000 Contingency Plans.

Thank you for sharing your draft report concerning USAID's activities related to the development and testing of Y2K contingency plans based on your audit during the period March to September 1999. I welcome the opportunity to provide detailed comments concerning your recommendation No. 2 related to the testing of USAID's contingency plan for financial management operations.

I am pleased that the OIG has closed recommendation No.1 based upon USAID actions taken since your audit work was completed in September. The designation of the Deputy Administrator as the Policy Manager for Y2K ensures that Y2K will continue to be given the highest priority, enabling USAID to respond quickly and effectively to problems. An Agency Task Force has been established and each bureau is organizing appropriate personnel into Bureau Response Teams. This overall structure, supported by an Agency-wide Operations Center, will provide an effective leadership role in guiding USAID's relations with other agencies.

You are also aware that USAID has continued to work with missions to ensure that their critical systems are Y2K compliant, that missions are an integral part of embassy contingency plans and that efforts were made to repair and test many IT systems employed within USAID projects and

1300 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, D.C. 20523

test many IT systems employed within USAID projects and systems critical to host government operations. The Deputy Administrator has also requested that all missions verify that they have, or are in the process of putting in place, contingency plans which adequately demonstrate an ability to respond to possible Y2K disruptions to programs and projects and which can mitigate the significant loss of program resources. We believe that these activities are responsive to many comments made in your draft audit regarding the need to ensure business continuity and contingency planning.

I want to point out two other specific developments. First, your report makes reference to the lack of a contingency plan for the Contraceptive and Logistics Management Division in the Global Bureau. A plan was shared with your office on November 7 which addressed a number of issues related to ordering, shipping and distributing commodities. I would be happy to review this with you at your earliest convenience. Second, the Bureau for Humanitarian Response has completed a contingency plan for OFDA, which I am more than happy to share with you. These plans will continue to be adjusted as conditions dictate.

The balance of this memorandum concerns our review of your recommendation No.2.

The OIG found that M/FM had done a faithful job of initiating contingency planning, analyzing business impact, and preparing the contingency plan in compliance with the GAO guidelines. The OIG concluded that the level of testing of the plan was not quite up to the GAO standard. While M/FM has concluded that its testing phase activities probably met the letter of the GAO guidelines, M/FM accepts that taking the additional steps identified by the OIG in the time remaining before Y2K will further reduce business risk to the Agency. Therefore, management accepts the recommendation to take these additional risk mitigation actions..

We would like to clarify two issues of fact.

- **M/FM did analyze the test results and incorporate those results into a revised plan.** The mission contingency plan was tested in one mission (PERU). The plan largely worked, as developed. Those minor issues that were identified in PERU were used as a

basis for improving the plan. After the test was completed, each mission was required to rehearse the procedures stated in the plan. The primary purpose of these rehearsals was to educate each mission on how to execute the plan, not to test it further. In analyzing the extensive documentation of the results of the rehearsals, M/FM did not find any problems that do not have easy solutions without changes to the plan, as written.

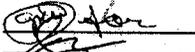
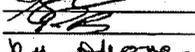
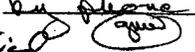
- **M/FM named its initial business resumption team in May.** Moreover, it has recently adjusted the staff assigned to the team, and made the assignments more detailed. The team is already scheduled to meet next week to make final preparations.

M/FM will take the following actions in the time before Y2K to mitigate business risk to the Agency:

- Analyze the detailed correspondence from the mission rehearsals to ensure that each mission did confirm that it can implement the plan as written. A summary of this information will be provided.
- Document the evidence for the conclusion that problems encountered in the rehearsals are manageable by describing examples of the more serious problems and how they can be resolved under the existing plan. This will provide ready answers to missions, and thus help assess the level of risk.
- Conduct tests of the transaction types not previously tested in Washington, and make any necessary adjustments to the plan.
- Document an analysis of M/FM's operational capacity to handle the required volume of work based on the time required to perform the test transactions. (As noted in the plan, M/FM will manually process all mission critical transactions, and others it has the capacity to manage manually, but does not expect to be able to process the normal volume of work under the contingency plan.)

We have discussed these actions with OIG staff and have concluded that they are responsive to the audit findings and recommendation. We will propose that the recommendation be closed when these steps are completed.

CLEARANCES:

M/IRM/OD:W. Van Vechten		Date 12/10/99
M/IRM/SDM:G. Moore *		Date 12/10/99
M/AA:P. Benedict		Date 12/10/99
M/FM/CONT:E. Klosky		Date 12/10/99

* facts not verified.


M/IRM:PBenedict:PB:712-4948:12/10/99:U:/IRM.OD/Audit
Response

APPENDIX III

THE GAO GUIDE PROCESSES

INITIATION

- 1.1 Establish a business continuity project work group
- 1.2 Develop/document a high-level business continuity planning strategy
- 1.3. Identify core business processes
- 1.4. Define roles and responsibilities
- 1.5. Develop a master schedule and milestones
- 1.6 Implement a risk management process and establish reporting system
- 1.7 Assess existing business continuity, contingency, and disaster recovery plans and capabilities
- 1.8 Implement quality assurance reviews

BUSINESS IMPACT ANALYSIS

- 2.1 Define/document information requirements, methods, and techniques to be used in developing the business continuity plan
- 2.2 Define/document Year 2000 failure scenarios
- 2.3 Perform risk and impact analyses of each core business process
- 2.4 Assess and document infrastructure risks
- 2.5 Define the minimum acceptable level of outputs and services for each core business process

CONTINGENCY PLANNING

- 3.1 Assess the cost and benefits of identified alternatives and select the best contingency strategy for each core business process
- 3.2 Identify and document contingency plans and implementation modes
- 3.3 Define and document triggers for activating contingency plans
- 3.4 Establish a business resumption team for each core business process
- 3.5 Develop/document "zero day" strategy and procedures.

TESTING

- 4.1 Validate business continuity strategy
- 4.2 Develop and document contingency test plans
- 4.3 Establish test teams and acquire contingency resources
- 4.4 Prepare for and execute tests
- 4.5 Validate the capability of contingency plans
- 4.6 Rehearse business resumption teams
- 4.7 Update the business continuity plan based upon lessons learned and re-test if necessary
- 4.8 Update disaster recovery plans and procedures

