United States General Accounting Office

GAO

Report to the Chairman, Subcommittee on the Civil Service, Committee on Government Reform, House of Representatives

May 1999

YEAR 2000 COMPUTING CHALLENGE

OPM Has Made Progress on Business Continuity Planning

GAO/GGD-99-66

GAO

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

General Government Division

B-281298

May 24, 1999

The Honorable Joe Scarborough
Chairman, Subcommittee on the Civil Service
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

The Office of Personnel Management (OPM), like other federal agencies, has been working to safeguard its critical computer systems against failures caused by what is known as the Year 2000 computing problem. Computer systems could malfunction or generate incorrect results after December 31, 1999, given that in many systems developed over the past several decades, the year 2000 is indistinguishable from the year 1900 because both are represented as "00." OPM's preparation for the Year 2000 problem is vital to ensuring the continuation of its important agency functions, such as processing annuity payments to federal retirees and their survivors. Given the potential for serious governmentwide disruption to critical functions and services, we have designated the Year 2000 computing problem as a high-risk area in the federal government.[1]

In addition to preparing critical computer systems for the year 2000, federal agencies need to develop plans to ensure the continuity of their operations should systems fail to operate as intended. Agencies must also prepare for possible disruptions to critical infrastructure services like power, water, and telecommunications. Given our concerns about the readiness of federal agencies to prepare for possible disruptions to critical operations, we initiated a review of OPM's business continuity and contingency planning efforts for managing and mitigating the risks of Year 2000-related business failures. Because of your interest in this issue, you asked that we address this report to you.

In reviewing OPM's Year 2000 business continuity and contingency planning activities, our objectives were to evaluate OPM's efforts to (1) develop an overall planning strategy for ensuring the continuity of agency operations, (2) assess the risk and impact of system failures on the agency's core business processes, (3) prepare contingency plans that include procedures and timetables for continuing agency operations in the event that critical systems fail, and (4) test the contingency plans to

[1] High-Risk Series: Information Management and Technology (GAO/HR-97-9, Feb. 1997); and High-Risk Series: An Update (GAO/HR-99-1, Jan. 1999).

determine their effectiveness. Guidance on these four steps is detailed in our Year 2000 business continuity planning guide,[2] which presents a structured approach to aid federal agencies in managing and mitigating risks associated with the century date change. This structured approach helps to ensure that agencies have, at a minimum, addressed the important components of a well-developed business continuity plan for the Year 2000 problem.

Results in Brief

OPM has made progress in its business continuity planning efforts in preparation for the Year 2000 computing problem. Using our guidance on Year 2000 business continuity planning for federal agencies, OPM developed a strong planning strategy for ensuring the continuity of critical agency operations in the event of Year 2000-induced system failures. To develop its planning strategy, OPM created a project structure involving representatives from the agency's major business units. Through the coordination of this project work group, OPM developed a master schedule and milestones for continuity planning activities, identified business processes that are critical to agency operations, established key reporting requirements, and obtained the concerted support and involvement of the agency's senior management.

Our review raised concerns, however, about OPM's implementation of its business continuity planning strategy. We identified these concerns after reviewing key planning documents that OPM had developed according to critical milestones established by the agency in its Year 2000 business continuity planning process. Specifically, our concerns involved the approach that OPM used for (1) assessing the risk and impact of system failures on the agency's core business processes, (2) preparing contingency plans to be used in the event of critical system failures, and (3) developing plans to test the contingency plans to determine whether they would be effective if implemented.

When OPM presented us with its written comments on a draft of this report, it provided us with supplemental documentation that demonstrated that the agency had taken additional actions to address our concerns. By taking these additional actions, OPM has improved the implementation of its business continuity planning strategy and increased the likelihood that critical agency functions can be carried out even if Year 2000-induced failures occur in key computer systems. Thus, we are not making recommendations to address the concerns we originally observed.

[2] Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, issued as an exposure draft in Mar. 1998 and in final form in Aug. 1998).

Background

For the past several decades, automated information systems have typically used two digits to represent the year, such as "98" for 1998, in order to conserve electronic data storage space and reduce operating costs. In this format, however, the year 2000 is indistinguishable from the year 1900 because both are represented as "00." As a result, if not modified, computer systems or applications that use dates or perform date-sensitive calculations could malfunction or generate incorrect results when working with years after 1999. To mitigate this risk, organizations—public and private—must repair or replace their mission-critical systems, test the systems for Year 2000 compliance, and develop plans to ensure continued operations in the event of Year 2000-induced system failures.

To assist agencies in addressing the Year 2000 computing problem, we prepared guidance that presents structured approaches for assessing an agency's Year 2000 conversion effort,[3] testing systems and system components for Year 2000 compliance,[4] and developing business continuity and contingency plans.[5] Our guide on business continuity and contingency planning, which the Office of Management and Budget (OMB) has adopted as a standard for federal agencies, describes four phases of implementation, each representing a major Year 2000 business continuity planning activity. These four phases are described in the following paragraphs.

Initiation: This critical first step involves establishing an overall strategy for ensuring the continuity of agency operations in the event of Year 2000-induced system failures. The agency convenes a planning team of agency officials to work with the agency's Year 2000 program management in developing a master schedule and milestones, documenting the agency's core business processes, establishing key reporting requirements, and obtaining executive-level support for the planning effort.

Business impact analysis: In this phase, the agency assesses the risk and impact of systems failures on the viability and operations of the agency's core business processes. By defining possible failure scenarios associated with the Year 2000 problem, the agency identifies threats to its core business processes. The agency then analyzes the risk and impact of these

[3] Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, issued as an exposure draft in Feb. 1997 and in final form in Sept. 1997).

[4] Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, issued as an exposure draft in June 1998 and in final form in Nov. 1998).

[5] GAO/AIMD-10.1.19, August 1998.

potential threats and develops strategies to mitigate the impact of these threats prior to potential system failure.

Contingency planning: This phase entails developing and documenting contingency plans that specify the agency's response to system failures in order to ensure the continued operation of the agency's core business processes. These plans provide a description of the resources, staff roles, procedures, and timetables needed for implementation.

Testing: In this phase, the agency develops and executes test plans to determine whether the contingency plans are capable of providing the desired level of support to the agency's core business processes and whether the plans can be implemented within a specified period of time. The agency then updates its contingency plans based on lessons learned and retests if necessary.

In planning for possible Year 2000-related problems, agencies need to consider not only the potential failures of their internal systems but also disruptions related to the agencies' external dependencies. Many agencies depend on information and data from business partners, including other federal agencies, state and local agencies, and private sector entities. In addition, agencies need to consider the risks to public infrastructure services, such as power, water, and voice and data telecommunications.

We conducted our review from November 1998 through April 1999 in accordance with generally accepted government auditing standards. Details of our objectives, scope, and methodology are presented in appendix I. We requested comments on a draft of this report from the Director of OPM or her designee. On April 2, 1999, we met with OPM officials to obtain and discuss the agency's written comments, which are summarized in the Agency Comments section and reprinted in appendix IV.

OPM Developed a Strong Planning Strategy for Its Year 2000 Continuity Efforts

The first phase of business continuity planning—referred to herein as initiation—involves developing a planning strategy for ensuring the continuity of agency operations in the event of Year 2000-induced failures. As noted in our guidance on business continuity planning, during this initiation phase, agencies need to create an organizational structure for the planning project and establish a master schedule and key milestones for completing the planning effort. Our guide recommends creating a business continuity work group that reports to senior agency management and includes representatives from the agency's major business units. Through the coordination of this work group, agencies would identify their core

business processes, establish key reporting requirements, and obtain executive support for the planning effort.

Our review showed that OPM developed a strong planning strategy for its Year 2000 business continuity efforts. In developing this planning strategy, OPM established a project structure and milestones for carrying out the planning effort, identified the agency's core business processes, established key reporting requirements, and obtained the concerted support and involvement of senior managers in the agency.

OPM Created a Project Structure and Milestones for Its Planning Activities

OPM's Year 2000 business continuity planning efforts began in April of 1998. At that time, OPM's Director designated the agency's Chief of Staff to oversee the agency's continuity planning process. The Chief of Staff formulated an executive committee to select an OPM official to serve as the project manager in directing the day-to-day activities of the agency's Year 2000 continuity planning effort. As recommended in our business continuity planning guide, OPM assembled a business continuity work group to coordinate the agency's planning efforts. The work group, which began meeting in June 1998, is led by the business continuity project manager and is composed of officials from each of OPM's 17 major business units. (See app. II for a list of the units represented on the work group.) The designated role of the work group was to coordinate the agency's planning efforts through their respective OPM units and report to the continuity project manager on the status of units' planning activities.

Our business continuity planning guide states that agencies should also develop a master schedule and milestones for the continuity planning effort. OPM developed a master schedule that called for the preparation of all the agency's draft[6] contingency plans by December 1998. To determine whether the plans would be effective if implemented, OPM established milestones to develop and test the contingency plans by May 1999. The schedule called for OPM to prepare its final contingency plans by June 1999.

OPM Identified Core Business Processes to Be Used in Its Planning Process

In the early phase of the business continuity planning effort, each agency also needs to identify those processes or functions that are critical to the agency's ability to deliver important services to its customers. These core business processes are to serve as the foundation of the agency's Year 2000 continuity planning efforts. OPM identified the following five core business processes for the agency:

[6] Until the contingency plans are tested to determine their effectiveness, OPM officials refer to the plans as "draft."

- Provide retirement and survivor annuity payments.
- Process retirement and survivor claims.
- Administer health benefit and life insurance programs and payments.
- Provide examining services to agencies.
- Provide communications to agencies and employees on critical human resources issues.

In addition, OPM identified two key support functions that the continuity work group would consider in its planning process: (1) provide administrative and management information systems and (2) provide information technology infrastructure.

When identifying core business processes, it is important that agencies consider the critical agency systems that support these core processes. Because the agency's mission-critical systems support its core processes, these critical systems should receive priority in the agency's Year 2000 program. At the time of our review, OPM had designated 109 of its information systems as mission-critical. Included in OPM's inventory of mission-critical systems are complex retirement and insurance support systems that process monthly annuity payments and collect funds withheld by federal employees for retirement, health benefits, and life insurance premiums. OPM officials told us that when they assessed their systems to determine which ones to designate as mission critical, they decided to take the broad approach of including more rather than fewer systems. OPM officials said that this approach would help to ensure that important systems received agencywide attention.

OPM Established Reporting Requirements for Its Planning Effort

In developing a sound continuity planning approach, agencies also need to establish key reporting requirements. Within OPM, business continuity and contingency planning is one of 14 components in the agency's overall Year 2000 program. Under OPM's Year 2000 program management approach, agency officials responsible for each of these 14 components are to report monthly on their progress in meeting Year 2000-related goals. (See app. III for a list of the 14 components and the responsible OPM units.) OPM initiated this program management approach in August 1998 in response to our earlier review of OPM's initial Year 2000 system conversion efforts. In a July 1998 briefing with OPM officials, we raised concerns that OPM had not developed a comprehensive Year 2000 plan with scheduled tasks as specified in our Year 2000 assessment guide[7] and that the lack of such a plan could affect OPM's ability to achieve Year 2000 compliance. OPM

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

agreed with these observations and developed a Year 2000 plan with scheduled tasks and a more structured reporting and control mechanism.

OPM also established a reporting format for its business units to use when preparing their Year 2000 contingency plans. In June 1998, OPM's continuity work group adopted the contingency plan reporting format that the Social Security Administration (SSA) had used for its contingency planning efforts. We had reported[8] earlier that SSA was generally regarded as a federal leader in addressing the century date change. Additionally, in its May 1998 quarterly report on the status of the federal government's Year 2000 progress, OMB reported that SSA's business continuity and contingency plan had been circulated as a model to other federal agencies.

OPM Obtained Senior Managers' Support for Its Continuity Planning Efforts

Our business continuity planning guide stresses the importance of promoting executive ownership of the Year 2000 continuity planning effort. Since the commencement of OPM's contingency planning activities, OPM has made a concerted effort to obtain the support and involvement of the agency's senior managers. For example, OPM's Chief of Staff oversaw the business continuity work group's initial efforts to coordinate the agency's Year 2000 continuity planning activities. OPM's Deputy Director, newly appointed in November 1998, has also taken an active role in the agency's efforts to address the Year 2000 problem. In December 1998, the Deputy Director assumed responsibility for overseeing the business continuity work group's efforts to coordinate the agency's Year 2000 continuity planning activities.

OPM Developed Information to Assess the Risk of System Failures

After developing a business continuity strategy for the Year 2000 problem, agencies need to determine the risk and impact of internal and external system failures on the viability and operations of the agency's core business processes. During this phase—referred to herein as business impact analysis—the agency identifies Year 2000-related threats to the agency's core processes. The agency then assesses the risk and impact of these threats and identifies strategies to eliminate or reduce the impact of the threats prior to potential system failures.

Our review of OPM's business impact analysis found that OPM identified potential threats to the agency's critical functions and identified strategies to mitigate these threats. We found during our review, however, that when OPM analyzed the impact of system failures on its core business processes, it had not estimated and assigned risk to its mission-critical

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

systems. After reviewing a draft of this report, OPM provided us with documentation that showed that the agency had taken additional action to develop a Year 2000 risk assessment for each of its 109 mission-critical systems. This assessment should assist in providing OPM with vital information about the likelihood of system failures and the risk of such failures to the agency's core business functions.

OPM Identified Threats to Its Core Business Processes

In conducting a risk and impact assessment of core business processes, agencies first need to identify potential Year 2000-related threats, which represent circumstances or events that could harm critical agency functions. As noted in our business continuity planning guide, agencies identify these potential threats by considering various Year 2000 failure scenarios. These failure scenarios assume the loss of the agency's internal mission-critical systems as well as potential failures related to exchanging electronic data with business partners. The failure scenarios should also address the potential disruption of essential infrastructure services, including power and telecommunications.

OPM identified potential threats to its critical functions through its Year 2000 business continuity work group. Members of this work group coordinated with their respective units in considering possible Year 2000 failure scenarios and identified specific threats to the provision of uninterrupted critical services to OPM customers. For example, in identifying threats to its critical process of providing retirement and survivor annuity payments, OPM noted that some banks might not be able to receive electronic funds transfer (EFT) payments, thus preventing customers from receiving their retirement benefits.

OPM Assessed Risk to Its Mission-Critical Systems

After identifying potential Year 2000-related threats, agencies need to assess the risk and impact of these threats on the agency's core business processes. As noted in our business continuity planning guide, the risk management process for continuity planning calls for agencies to estimate and assign risk to each of their mission-critical systems. This risk could be related to the system's environment, hardware, software interfaces, or other circumstances unique to the particular system. For example, factors could include the number of interfaces that the system has with external entities and the current status of repairing and testing the system for Year 2000 compliance.

During our review, we found that when OPM assessed the risk of Year 2000-induced failures for its core business processes, it had not estimated and assigned risk to its mission-critical systems. Therefore, OPM units that were assessing the risk of Year 2000 failures on core business processes

lacked critical information on the risk of failure associated with each of the mission-critical systems. This lack of information hindered OPM's ability to develop a complete assessment of the risk to its core processes. Such an assessment is important to providing OPM with information on which processes are more likely to be affected by system failures and to allowing OPM to concentrate its resources on mitigating and managing those risks that are more likely to endanger agency operations. OPM systems at greater risk for failure may need increased management attention because these systems will likely require more detailed contingency plans and longer time frames for testing the plans.

OPM has engaged a contractor to independently verify OPM's Year 2000 compliance effort. As part of its quality review, the contractor was tasked with identifying risks in OPM's Year 2000 methodologies and processes. Contractor representatives we interviewed said that they planned to provide OPM with information about the degree of risk associated with each of OPM's critical systems; however, they did not plan to provide this information to OPM until October or November 1999, when all system testing is expected to be completed. The contractor representatives said that the scope of their work did not include verifying the appropriateness of OPM's business continuity and contingency planning efforts. They said that OPM would have to determine on its own how contingency planning efforts should be prioritized, based on its knowledge of the importance of its systems for maintaining essential agency operations.

If OPM waited to develop a complete risk assessment of its mission-critical systems and associated core processes until October or November 1999, it would likely not have sufficient time to reassess and implement appropriate risk mitigative actions prior to January 1, 2000. Although factors affecting risk and impact could change after the agency developed its risk assessment, OPM could update its assessment as it became aware of additional information that altered the risks associated with its systems and processes. If necessary, OPM could then develop additional mitigative strategies or revised contingency procedures on the basis of this new information.

At our April 2, 1999, meeting with OPM to obtain and discuss the agency's written comments to our draft report, OPM provided us with information that demonstrated that the agency had taken additional action to develop a Year 2000 risk assessment of its mission-critical systems. OPM stated that after we raised concerns about the timing of its verification efforts, it accelerated the schedule for the independent contractor to provide it with information about the risk associated with its mission-critical systems.

OPM said that with this assistance from its verification contractor, the agency developed a Year 2000 risk assessment for each of its 109 mission-critical systems. OPM officials provided us with supplemental documentation that showed the criteria OPM used to assess the systems and the results of the risk assessment for each system. OPM officials told us that they are using this newly developed risk assessment in their planning efforts to focus on those risks that are more likely to endanger the agency's core business functions.

OPM Identified Risk Mitigation Strategies

As part of the business continuity planning process, agencies also need to identify strategies to eliminate or reduce the impact of the Year 2000-related threats prior to potential system failures. With the identification and implementation of risk mitigation strategies, agencies can reduce the level of risk and lessen the potential need to implement the contingency plan.

Our review of OPM's planning documents found that 16 of OPM's 17 business units identified clearly stated risk mitigation strategies for the threats that OPM had identified. For example, in the case of ensuring the provision of EFT payments to federal retirees, one of the risk mitigation strategies included developing a computer program that would immediately recognize EFT payments that were not accepted by banks and reauthorize a hard-copy check to be sent to the retiree's current correspondence address. With the recent development of its Year 2000 risk assessment, OPM can focus its efforts on ensuring that its inventory of risk mitigation strategies is sufficient. Given the time constraints as the century date change approaches, OPM—like other government agencies and private organizations—will need to focus its resources on developing and implementing risk mitigative actions for those systems and processes that are at greater risk for failure.

OPM Prepared Contingency Plans for Its Organizational Units

Agencies need contingency plans for responding to the loss or degradation of essential services as the result of a Year 2000 problem in an automated system. In this contingency planning phase of the business continuity planning process, agencies are to prepare plans that describe the fallback procedures the agency would employ—including the activation of manual or contract processes—to ensure the continuity of core business processes in the event of Year 2000-induced system failures. As noted in our business continuity planning guide, contingency plans should also include a description of the resources, staff roles, and timetables needed for implementation.

To prepare for possible disruptions to its core business processes, OPM developed its Year 2000 contingency plans by organizational unit. We reviewed the 27 contingency plans that OPM's 17 units prepared in response to possible Year 2000-induced failures.[9] Our review of these contingency plans initially showed that they did not fully address three areas of key information that are essential for ensuring the continuity of agency operations in the event of critical system failures. Specifically, OPM's plans (1) did not demonstrate that the agency considered all its mission-critical systems in the planning process, (2) lacked clear procedures and assignment of responsibilities for activating and implementing the plans, and (3) did not include a risk-reduction strategy and procedures for the critical days before and after the century date change. When it provided written comments on our draft report, OPM gave us supplemental documentation that demonstrated that the agency had taken additional actions to address our concerns. With this additional attention to its contingency plans, OPM will be better positioned to have timely and well-defined responses in the event that system failures occur.

Plans Considered All of OPM's Mission-Critical Systems

When developing Year 2000 contingency plans, agencies should determine the effect of mission-critical system failures on agency operations by documenting which systems affect the agency's core business processes. Moreover, because the agency's mission-critical systems support its core business processes, all the critical systems should be considered in the contingency planning process. Our review found that 23 of OPM's 27 contingency plans did not identify the mission-critical systems associated with the threats that had been identified. Because most of OPM's plans did not link identified threats to mission-critical systems, OPM would not be able to readily determine whether its inventory of critical systems was considered or included in the planning process.

OPM officials initially told us that they could not confirm whether all of OPM's 109 mission-critical information systems were considered or included in the agency's contingency plans. They told us, however, that OPM would work to ensure that all critical systems are linked to core processes in the plans and that this linkage would verify that OPM's entire inventory of 109 critical systems was considered. In its written comments on a draft of our report, OPM said that it had considered all the automated systems supporting its core business functions in its continuity planning process. In response to our concerns about this issue, OPM created and

[9] Fourteen of the 17 units prepared and submitted one plan each. The remaining three units submitted plans for their subunits. The Retirement and Insurance Service submitted six plans; the Office of Contracting and Administrative Services, five plans; and the Office of Executive Resources, two plans.

provided to us a crosswalk that linked each of its critical systems to the relevant sections of its contingency plans. By linking its critical systems to its contingency plans, OPM was able to ensure that it had considered all its critical systems in the planning process.

Plans Included Procedures and Responsibilities for Activation and Implementation

As noted in our business continuity planning guide, each Year 2000 contingency plan should provide a description of the resources, staff roles, procedures, and timetables needed for its implementation. As part of this description, agencies need to define and document the triggers for activating contingency plans as well as the actions to be taken if and when the plans are activated. Each of the agency's contingency plans should also identify the individuals responsible for managing the plan's activation and implementation.

Our review found that 26 of OPM's 27 contingency plans were missing one or more of these important elements. Only 1 of the 27 plans we reviewed identified the OPM official responsible for managing the activation and implementation of each contingency plan. Seven of the plans did not specify the trigger for plan activation, and nine did not clearly state the procedures needed for operating in contingency mode. This lack of accountability could generate confusion over who is responsible for notifying agency personnel when a contingency plan is activated and for carrying out contingency mode procedures until the agency's normal operating mode can be resumed. Similarly, for those plans that did not specify requirements for activation and implementation, agency officials will not know in advance when contingency procedures should be invoked and what actions should be taken if and when the plan is activated. Specification of triggers and implementation actions in contingency plans allows the agency to have predetermined criteria and thus avoid the time-consuming process of reaching agreements if a system failure occurs.

At our April 2, 1999, meeting with OPM officials to discuss OPM's comments on our draft report, agency officials provided us with documentation that showed the agency had taken additional actions to address these concerns. Specifically, OPM's documents showed that it had (1) identified the officials responsible for activating and implementing the contingency plans, (2) specified the triggers for plan activation, and (3) articulated the procedures needed for operating in contingency mode.

Plans Included Zero Day Strategy

As part of the contingency planning process, agencies also should develop and document a risk-reduction strategy for the critical days before and after the century date change. This strategy—called the "zero day" or "day one" strategy—articulates the procedures and resources that the agency

will need for the period from late December 1999 to early January. Such a strategy may include, for example, an agencywide shutdown of all agency information systems on Friday, December 31, 1999, and a phased power-up on Saturday, January 1, 2000.

OPM's initial plans did not include a risk-reduction strategy and procedures for these critical days before and after the century date change. During our review, OPM officials told us that they recognized that they needed to develop a zero day strategy and procedures for the agency's critical operations. OPM's business continuity project manager initially said, however, that he did not know when the agency would develop its zero day plans.

At our April 2, 1999, meeting to obtain and discuss OPM's written comments on a draft of this report, the agency gave us documentation that showed that it had taken additional action to develop zero day plans for its business units. In its written comments, OPM said that from the outset of its business continuity planning process, the agency had intended for OPM units to submit their zero day plans in April 1999. Prior to receiving OPM's written comments, however, we had not been provided with any information that specified when the agency's zero day strategy and procedures would be completed.

The zero day plans that OPM provided to us showed that the agency's units had detailed their planned procedures and activities for the 6-day period from Wednesday, December 29, 1999, to Tuesday, January 4, 2000. OPM's plans included the designation of agency employees who would serve on business resumption teams. These teams would be responsible for assisting in carrying out the contingency plans and dealing with a wide range of operational problems that could occur. Now that OPM has developed zero day plans, the agency can periodically review these plans to determine what changes, if any, should be made to reduce risk and ensure a smooth transition during the critical days before and after the century date change. OPM officials said that they expect that their zero day plans may change between April and the fall of 1999, as OPM's units review their plans and respond to any changes in risks associated with the agency's core business processes or mission-critical systems.

OPM's Test Plans Included Important Elements Needed to Determine Effectiveness

The fourth phase of business continuity planning involves developing and executing tests of the contingency plans to determine whether the plans are likely to be effective if implemented. As noted in our business continuity planning guide, these tests allow the agency to evaluate whether the contingency plans are capable of providing the desired level of support to the agency's core business processes and whether the plans can be implemented within a specified period of time. The contingency test plans developed by agencies are to include elements that will allow the agency to test the basic assumptions under which the contingency plans were developed.

Our review of the contingency test plans that OPM made available to us showed that important elements were often lacking, including clearly defined test objectives, necessary personnel and their roles, the duration and location of tests, and expected test results. Along with its written comments on a draft of our report, OPM provided documentation that showed that the agency had taken additional action to incorporate these elements into its test plans. With these elements now added, OPM's tests of its contingency plans can provide greater assurance that the contingency plans would be effective in the event of Year 2000-induced business failures.

OPM Developed Plans to Test Contingency Procedures

According to OPM's monthly Year 2000 management reports, OPM began developing its contingency plan testing strategy in August 1998. Members of the continuity work group were to coordinate the development of the test plans through their respective units. As with the preparation of OPM's Year 2000 contingency plans, the business continuity project manager instructed the OPM units to refer to our business continuity planning guide when developing their contingency test plans.

OPM initially made available five of its contingency test plans for us to review. At the time we reviewed these five test plans, OPM had not completed development of all its test plans. The five test plans that we reviewed were prepared and submitted by three OPM offices: the Employment Service, the Office of Communication, and the Retirement and Insurance Service.[10] OPM's business continuity project manager said that these offices included the most critical of the agency's core processes.

[10] We reviewed three contingency test plans from the Retirement and Insurance Service—one each from the Office of Retirement Programs, the Office of Insurance Programs, and the Office of the Actuaries.

We used our business continuity planning guide as a framework to review the five contingency test plans. Our review of these test plans showed that important elements were often not addressed. Elements missing from the test plans included clearly defined test objectives, necessary personnel and their roles, the duration and location of tests, and expected test results. These elements are important because they allow the agency to evaluate whether individual contingency plans are capable of providing the desired level of support to the agency's core business processes and whether the plans can be implemented within a specified period of time.

At our April 2, 1999, meeting with OPM to discuss its written comments on our draft report, agency officials provided us with documentation that demonstrated that the agency had taken additional action to incorporate these missing elements into its test plans. This additional information showed that its test plans included the important elements needed for testing, such as test objectives, necessary personnel, the duration and location of tests, and expected test results. With these elements now included in its test plans, OPM's testing of its related contingency plans can provide greater assurance that OPM's proposed contingency responses would be effective in the event of Year 2000-induced failures.

OPM's Testing of Its Contingency Plans Had Recently Begun

At the time of our review, OPM was planning to complete its evaluation of the results of its contingency plan testing by May 1999 and prepare the final contingency plans by June 1999. Because OPM had newly begun the process of testing its individual Year 2000 contingency plans at the time of our review, we focused our review on OPM's development of these test plans and did not address the execution or results of the tests.

Conclusions

OPM has made progress in its business continuity and contingency planning efforts for the Year 2000 computing problem. OPM developed a strong planning strategy for its business continuity planning efforts by creating a project structure and milestones for the planning effort, identifying core business processes, establishing key reporting requirements, and obtaining solid support for the planning effort from the agency's senior managers. Once a Year 2000 continuity strategy is developed, successful implementation becomes crucial to providing reasonable assurances that the agency has reduced the risk and potential impact of Year 2000-induced information system failures.

In response to concerns we raised during our review, OPM undertook actions to improve the implementation of its Year 2000 business continuity planning strategy. OPM's Year 2000 risk and impact assessment now includes the assignment of risk to each of its mission-critical information

systems. OPM's Year 2000 contingency plans now address key information that is essential for ensuring the continuity of agency operations. Finally, OPM's contingency test plans now include important elements for determining the effectiveness of its contingency plans. By taking measures to improve these components of its overall business continuity planning effort, OPM will be better positioned to deal with unexpected problems and delays that may be caused by the Year 2000 computing problem.

Agency Comments and Our Evaluation

We provided a draft of this report to the Director of OPM for comment. On April 2, 1999, we met with OPM officials to obtain and discuss the agency's written comments on our draft report. At this meeting, OPM provided us with its written comments as well as supplemental documentation that showed that the agency had taken additional actions to respond to our concerns. Descriptions of the additional actions that OPM undertook were incorporated throughout this report. OPM's written comments, which were provided by OPM's Deputy Director, are reprinted in appendix IV and summarized and evaluated here.

In its written comments, OPM stated that during our review we made a number of good suggestions that were helpful to the agency in its ongoing Year 2000 business continuity planning efforts. Although OPM commended our effort, the agency said that it disagreed with various statements in our draft report. OPM's overall disagreement with the conclusions and recommendations in our draft report focused primarily on the timing of our review. OPM stated that our review occurred in the middle of the agency's Year 2000 business continuity planning efforts, and as a result, the material we reviewed was preliminary and incomplete. Although we recognized that OPM's preparation for the Year 2000 computing problem was an ongoing effort, we based the timing of our review on the schedule that OPM had established for completing various milestones in its business continuity planning process. For example, OPM's schedule called for the completion of its initial Year 2000 contingency plans by December 2, 1998; we began our review of these plans later in that month. Additionally, in response to OPM's request, we delayed completion of our scheduled audit work so that the agency could provide us with contingency test plans from various OPM units.

In commenting on a recommendation in our draft report that OPM complete a Year 2000 risk assessment for the agency's mission-critical systems, OPM stated that after we raised concerns about the timing of its verification efforts, it accelerated the schedule for the independent verification contractor to provide it with information about the risk associated with its mission-critical systems. OPM stated that with

assistance from its verification contractor, the agency developed a risk assessment for each of its 109 mission-critical systems. At the April 2, 1999, meeting with OPM to discuss the agency's written comments on our draft report, OPM officials provided us with documentation that showed the criteria OPM used to assess the systems and the results of the risk assessment for each system. OPM officials told us that they would use this assessment to prioritize the agency's Year 2000 business continuity planning efforts. To recognize the additional action that OPM undertook in developing the risk assessment, we made changes to the relevant sections of our report, including the removal of our recommendation that OPM develop a Year 2000 risk assessment of its mission-critical systems.

In commenting on the conclusion in our draft report that OPM's plans did not demonstrate that the agency considered all its mission-critical systems in the planning process, OPM stated that all the automated systems that support its core business functions had been considered in the business continuity planning process. OPM stated that during our review, it had provided us with a crosswalk that linked each core business process to all mission-critical systems supporting it. Although this process of linking core business processes to mission-critical systems is important to document for planning purposes, this process alone did not demonstrate that OPM considered or included all the agency's mission-critical systems in its Year 2000 contingency plans. After it had given us its written comments on our draft report, OPM provided us with a crosswalk that linked each of its critical systems to the relevant sections of its contingency plans. By creating this crosswalk of its critical systems to its contingency plans, OPM was able to ensure that all critical systems were considered in the agency's planning process. In response to this additional action, we made revisions to the relevant sections of our report, including the removal of our recommendation that OPM ensure its contingency plans demonstrate that all critical systems have been considered in the agency's contingency plans.

Regarding a recommendation in our draft report that OPM revise its Year 2000 contingency plans to provide clear procedures and responsibilities for activation and implementation, OPM stated that this lack of clear procedures and assignment of responsibilities was not an oversight but was the result of our review's being done while OPM was still developing its plans. Our review of OPM's contingency plans, however, occurred in mid-December 1998, after the date by which OPM had requested that its units submit their contingency plans. We based the timing of our review of OPM's contingency plans on the agency's internal schedule for completing its initial contingency plans. At the April 2, 1999, meeting with OPM to

discuss the agency's written comment on our draft report, agency officials provided us with documentation that showed that OPM had taken additional action to address our recommendation concerning clear procedures and responsibilities for plan activation and implementation. This new information showed that OPM had identified the officials responsible for activating and implementing the contingency plans, specified the triggers for plan activation, and articulated the procedures needed for operating in contingency mode. In response to the supplemental documentation that OPM provided to us, we amended our report to reflect OPM's additional work on this issue and removed our recommendation from the report.

As to a recommendation in our draft report concerning the development of a zero day or day one strategy and procedures, OPM stated that after we had completed our audit work, it developed zero day plans for the various OPM units. In its written comments, OPM stated that from the outset of its business continuity planning process, the agency had intended for OPM units to submit their zero day plans in April 1999. OPM stated that the absence of a zero day strategy was not due to an oversight but rather to the fact that these plans were not yet due. During our review, however, OPM's business continuity project manager initially told us that he did not know when OPM would develop its zero day plans. Prior to OPM's written comments on a draft of this report, the plans that OPM had provided to us did not specify when the agency's zero day strategy and procedures would be completed. In response to the additional information that OPM provided to us, we amended our report to reflect that OPM was requiring its units to submit their respective zero day plans in April 1999. Our report now also states that OPM provided us with additional documentation showing that OPM units had developed zero day plans. In addition, we removed our recommendation calling for OPM to develop a zero day strategy and procedures.

As to a recommendation in our draft report that OPM ensure that its Year 2000 contingency test plans include important elements needed to test their effectiveness, OPM stated that it had always intended for this information to be part of the completed test plans. The contingency test plans that OPM made available to us for review in February 1999, however, were often missing elements that our business continuity planning guide states are important. At our April 2, 1999, meeting with OPM, agency officials provided us with information that showed that the agency had taken additional action to document these important elements, including test objectives, necessary personnel, the duration and location of tests, and expected test results. In response to OPM's additional actions on this

issue, we revised our report to reflect that OPM had documented these important elements in its contingency test plans. In addition, we removed our recommendation that OPM ensure that its test plans include the important elements needed to test their effectiveness.

We are sending copies of the report to the Honorable Janice R. Lachance, Director of OPM; the Honorable Jacob J. Lew, Director of OMB; appropriate congressional committees; and other interested parties. Copies will also be made available to others upon request.

Please contact me at (202) 512-8676 if you or your staff have any questions concerning this report. Major contributors to this report are listed in appendix V.

Sincerely yours,

Michael Brostek
Associate Director, Federal Management
and Workforce Issues

Contents

Letter		1
Appendix I Objectives, Scope, and Methodology		22
Appendix II List of OPM Units Represented on Year 2000 Business Continuity Work Group		24
Appendix III OPM's Year 2000 Program Management Approach		25
Appendix IV Comments from the Office of Personnel Management	GAO Comment	26 30
Appendix V Major Contributors to This Report		31
Tables	Table III.1: OPM's Year 2000 Program Components and Responsible OPM Units	25

Abbreviations

EFT	electronic funds transfer
LAN	local area network
OMB	Office of Management and Budget
OPM	Office of Personnel Management
SSA	Social Security Administration

Objectives, Scope, and Methodology

Our overall objective for this review was to evaluate OPM's business continuity and contingency planning efforts for managing and mitigating the risks associated with Year 2000-related business failures. Specifically, we evaluated OPM's efforts to (1) develop an overall planning strategy for ensuring the continuity of agency operations, (2) assess the risk and impact of system failures on the agency's core business processes, (3) prepare contingency plans that include procedures and timetables for continuing agency operations in the event that critical systems fail, and (4) test the contingency plans to determine their effectiveness. To accomplish these objectives, we relied on our Year 2000 business continuity planning guide,[1] which provides a structured approach for helping agencies manage the risk of potential Year 2000-induced disruptions to their operations. This structured approach helps to ensure that agencies have, at a minimum, addressed the important components of a well-developed business continuity plan for the Year 2000 computing problem.

To assess OPM's efforts in developing a Year 2000 business continuity planning strategy, we reviewed key OPM documents related to Year 2000 planning, including internal monthly status reports, minutes of business continuity work group meetings, and monthly and quarterly status reports to OMB. We also interviewed key officials at OPM headquarters in Washington, D.C, including the Deputy Chief of Staff, the Deputy Chief Information Officer, and the project manager for the agency's Year 2000 business continuity planning efforts.

To evaluate OPM's efforts in assessing the risk and impact of system failures on the agency's core business processes, we reviewed OPM planning documents that showed the results of the agency's risk and impact assessments. We also interviewed selected representatives from OPM's business continuity work group to learn how OPM units assessed the risk and impact of system failures on the agency's core business processes. These work group representatives were from the Retirement and Insurance Service and the Office of the Chief Financial Officer. In addition, we interviewed representatives of J.G. Van Dyke and Associates, Inc., a systems contractor that OPM retained to perform independent verification and validation of OPM's Year 2000 activities, including identifying risks in OPM's Year 2000 methodologies and processes.

To assess OPM's efforts in preparing Year 2000 contingency plans, we reviewed the 27 plans that were prepared and submitted by the 17 OPM units represented on the agency's business continuity work group (listed in

[1] GAO/AIMD-10.1.19, August 1998.

app. II). Fourteen of these 17 units submitted one contingency plan each. The remaining three units—the Retirement and Insurance Service, the Office of Contracting and Administrative Services, and the Office of Executive Resources—submitted a total of 13 plans for their respective subunits. In addition, we interviewed the selected representatives from OPM's business continuity work group to learn how these units prepared their contingency plans.

To assess OPM's efforts in determining whether its contingency plans would be effective if implemented, we reviewed five contingency test plans that OPM made available to us. These test plans were prepared and submitted by the Employment Service; the Office of Communications; and three offices within the Retirement and Insurance Service—the Office of Retirement Programs, the Office of Insurance Programs, and the Office of the Actuaries. At the time of our review, OPM had begun some testing of its contingency plans. However, we did not evaluate the execution or results of these tests.

Our review did not include an assessment of OPM's efforts to renovate or test its systems or system components for Year 2000 compliance. We conducted our review from November 1998 through April 1999 in accordance with generally accepted government auditing standards.

List of OPM Units Represented on Year 2000 Business Continuity Work Group

Combined Federal Campaign Operations
Employment Service
Investigations Service
Office of Communications
Office of Congressional Relations
Office of Contracting and Administrative Services
Office of Executive Resources
Office of Human Resources and Equal Employment Opportunity
Office of Merit Systems Oversight and Effectiveness
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of the Director
Office of the General Counsel
Office of the Inspector General
Office of Workforce Relations
Retirement and Insurance Service
Workforce Compensation and Performance Service

OPM's Year 2000 Program Management Approach

In August 1998, OPM established a structured program management approach for its Year 2000 compliance efforts. Under this approach, OPM's Year 2000 program is separated into 14 components. OPM officials responsible for these 14 components are to manage their respective Year 2000-related tasks and report on their progress in meeting their goals. Table III.1 lists the 14 program components of OPM's Year 2000 program and the OPM unit responsible for each component.

Table III.1: OPM's Year 2000 Program Components and Responsible OPM Units

Year 2000 program component	Responsible OPM unit
Overall Year 2000 program management	Office of the Chief Information Officer
Business continuity and contingency planning	Office of the Director
Awareness and publicity	Office of Communications
Mainframe hardware and systems software compliance	Retirement and Insurance Service
Mainframe applications software compliance	Retirement and Insurance Service
Local area network (LAN) and wide area network infrastructure	Employment Service
LAN and personal computer applications software compliance	Employment Service
Date data exchanges for mainframes	Retirement and Insurance Service
Date data exchanges for LAN	Employment Service
Telecommunications	Employment Service
Noninformation technology assets compliance	Office of Contracting and Administrative Services
Vendor management and contracting	Office of Contracting and Administrative Services
Compliance verification program	Office of the Chief Information Officer
Legal rulings and issues	Office of the General Counsel

Comments from the Office of Personnel Management

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
WASHINGTON, D.C. 20415

OFFICE OF THE DIRECTOR

APR 2 1999

Mr. Michael Brostek
Associate Director, Federal Management
And Workforce Issues
General Government Division
General Accounting Office
Washington, DC 20548

Dear Mr. Brostek:

Thank you for the opportunity to respond to the General Accounting Office draft report on the Office of Personnel Management's (OPM) Business Continuity and Contingency Planning (BCCP) for the Year 2000 (Y2K) computing problem. I am very confident that our plans and actions on Y2K, including our BCCP efforts, have us well positioned for the turn of the century.

As you know, OPM has been preparing for the Y2K computing problem in a variety of ways. Under the direction of our Chief Information Officer, we have been carrying out comprehensive and exhaustive Y2K preparations for more than two years. This multi-pronged effort ranges from ensuring that automated systems supporting critical OPM missions are Y2K ready, to developing comprehensive plans for informing OPM's customers and partners of our Y2K plans. In addition, we reported recently to Congress that 100% of OPM's mission-critical systems are now Y2K compliant -- tracking closely the schedule we developed last year. Our BCCP program has also been given a high priority.

See comment 1.

I was deeply concerned that, despite our efforts to provide GAO with thorough and convincing evidence of our overall Y2K readiness, including BCCP, GAO's draft report, particularly its introductory section, conveys a conclusion to the contrary. This conclusion is simply not supported by the facts and could leave an alarming and false impression on our customers that essential OPM services may not be available to them after the century change. Nothing could be further from the truth. Federal annuitants and other OPM customers can be entirely confident that OPM is fully prepared for Y2K.

GAO's conclusions and recommendations have also, unfortunately, been necessarily influenced by the time table required for completion of its report. The result, however, is that one could inaccurately conclude a lesser degree of readiness than is the case when examining the OPM plan, fully implemented under our long-established time line. Because GAO reviewed the implementation of our BCCP plan between November 1998 and March 1999, and OPM's final BCCP is not scheduled for completion until June 1, GAO's review occurred in the midst of our planning effort. As a result, the material GAO reviewed at OPM was preliminary, and in some cases, incomplete -- a fact GAO staff was well aware of. Despite this, the GAO draft report

CON 131-64-4
July 1988

continues to treat these gaps as program oversights, and not as the predictable findings of a review conducted mid-project. Furthermore, because of GAO's review schedule, we had to rely on supporting documentation developed in draft form and ahead of schedule to satisfy GAO inquiries.

We have raised GAO's findings recently, and, with some changes in a BCCP program schedule that had been long established, have now provided the GAO audit team with materials that answer every criticism and recommendation made in the draft report -- all within the two week time period requested in your letter. We trust that this latest information will lead to a reevaluation of the preliminary conclusions reached by GAO in the draft.

As to the draft report's specific comments:

Draft Report: "OPM's risk assessment was not complete because OPM did not estimate and assign risk to its 109 mission-critical information systems that support its core processes. Without a complete risk assessment of each of these critical systems, OPM lacks vital information about the likelihood of system failures and the risk of such failures to the agency's core processes. This information would allow OPM to concentrate its resources on mitigating and managing those risks that are more likely to endanger agency operations". (Pages 4 and 5 of the draft report).

Now on pp. 8-10.

OPM Response: Early in 1997, before any guidance on Y2K had been issued by GAO, OPM identified the mission-critical application systems in each of its business units and supporting organizations. All of these systems were assessed, including technical risk factors such as date data density, computational complexity, and data exchanges. Decisions were made as to which were already Y2K compliant, and which would be retired, repaired, or replaced. Plans were put in place to ensure that OPM's entire inventory of mission-critical systems would be compliant by March 31, 1999. In addition, we launched an independent compliance verification phase to provide extra assurance that these systems were in fact compliant, and which was scheduled to be completed well before the century change.

We planned to incorporate the results of the independent compliance verification process into BCC planning to ensure that any significant risks were addressed and priority given to contingency planning for any system that might have a likelihood of failure. At the time of this GAO review, the compliance verification phase was not yet completed. However, based on discussions with the GAO audit team and with the help of our independent verification contractor, we have accelerated the formal risk assessment for each mission-critical system, and have used that assessment to prioritize our remaining BCCP efforts. The results of this risk assessment have been provided to the GAO audit team. Detailed documentation is available for review upon request.

Draft Report: "OPM's contingency plans did not demonstrate that OPM considered all its mission-critical information systems in its planning process". (page 5)

Now on pp. 11-12.

OPM Response: The comment is misleading because not every automated system originally identified by OPM as "mission-critical" supports an OPM Core Business Function. As mentioned above, OPM identified very early in its Y2K planning effort the automated systems that support important OPM functions. OPM called these its "Mission Critical Systems". Much later, and in conformance with GAO guidance issued after this list was developed, OPM identified its "Core Business Functions". Few of the important OPM functions identified earlier were defined as Core Business Functions. Predictably, many automated systems on OPM's original list of mission-critical systems did not support a "Core Business Function". When the GAO audit team reviewed the contingency plans for OPM's Core Business Functions, it found that only systems supporting them were described and that many of the 109 systems on the original list of mission-critical systems were unaccounted for. This misunderstanding is unfortunate, but is a matter of form, not substance. OPM has, in fact, considered all of the automated systems supporting its Core Business Functions in its BCCP planning process. During the audit, OPM provided a crosswalk to the audit team that links each OPM Core Business Function to all the systems supporting it.

Now on p. 12.

Draft Report: "OPM's contingency plans...lacked clear procedures and assignment of responsibilities for plan activation and implementation." (page 5)

OPM Response: As mentioned in my general remarks, this was not the result of any oversight by OPM but was merely the result of the GAO audit team's review being done while plans were still being developed. OPM's final BCCP would have included this information. Indeed, the BCCP test plan guidance issued by the OPM BCCP management team to all OPM planners was modeled on GAO guidance and includes references to that information. A copy of this guidance was provided to the audit team during their review. In order to immediately address this concern, OPM developed the necessary procedures and assignment lists and provided them to the audit team.

Now on pp. 12-13.

Draft Report: "OPM's contingency plans...did not include a risk-reduction strategy and procedures for those critical days before and after the century date change" (page 5)

OPM Response: OPM incorporated a requirement for "Zero-Day" or "Day-1" plans its BCCP planning process and the original date for their submission was April 1999. Their absence from the draft reviewed by the audit team was not due to an oversight by OPM. Rather, these plans were not yet due at the time of the audit. To respond to this recommendation, OPM substantially amended its BCCP planning schedule and required each OPM component to immediately develop draft "Day-1" plans. These drafts have been submitted to the audit team. Final Day-1 plans will still be required by the original deadline in April.

Now on pp. 14-15.

Draft Report: "On the basis of test plans that OPM made available to us for review, we found that important elements were often missing from the test plans, including clearly defined test objectives, necessary personnel and their roles, the duration and location of tests and the expected test results" (page 6).

OPM Response: OPM intended for this information to be part of its completed BCCP. The test plan standards issued to OPM's offices specified that these elements must be part of a complete BCCP test plan. To respond to the draft report, OPM's BCCP management team has obtained this information from each OPM component. It has been provided to the audit team.

The Y2K crisis presents us all, here and around the world, with wide-ranging and unprecedented managerial challenges. It is with that knowledge that, while we may respectfully disagree with various statements made in your report, we commend your team's effort. They demonstrated a consistent professionalism and commitment to working with us as we develop strategies for continuing our most important functions at the century change. Indeed the GAO team made a number of good suggestions throughout the process that were helpful to us in our ongoing BCCP effort.

If you have any questions concerning OPM's response to this report, please call me or contact Mr. Rick Lowe on (202) 606-1000.

Sincerely,

John U. Sepulveda
Deputy Director

The following is GAO's comment on OPM's letter dated April 2, 1999.

GAO Comment

1. OPM raised concerns that the introductory section in our draft report could present a false impression to OPM's customers that the agency's essential services may not be available after the century change. In response to OPM's concerns, we redrafted the introductory paragraph to continue to emphasize the importance of Year 2000 preparations while not conveying any conclusions about OPM's efforts to renovate or test its systems for Year 2000 compliance.

Major Contributors to This Report

General Government Division

Steven J. Wozny, Assistant Director, Federal Management and Workforce Issues
K. Scott Derrick, Evaluator-in-Charge
Jeffrey W. Dawson, Evaluator

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Order by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touch-tone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER

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

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested