

December 3, 1999

CLARENCE E. LEWIS, JR.
CHIEF OPERATING OFFICER
AND EXECUTIVE VICE PRESIDENT

NORMAN E. LORENTZ
SENIOR VICE PRESIDENT,
CHIEF TECHNOLOGY OFFICER

SUBJECT: Year 2000 Business Contingency and Continuity Planning:
Plan Development and Testing (Report Number TR-AR-00-001)

This report presents the results of the Office of Inspector General's second review of the United States Postal Service's Year 2000 (Y2K) Business Contingency and Continuity Planning Initiative (Project Number 00PA016TR000). During this review, we noted that while the Postal Service had made significant progress in documenting plans, a contingency plan had not been developed for one critical system. Also, contingency and continuity plans were often not complete, well integrated, or adequately tested. To the extent that corrective actions are not taken to address these issues, the Postal Service may increase the risk of disruptions to core business processes in the event of Y2K disruptions. Management agreed with two recommendations, agreed in part with two more, and disagreed with one recommendation. Management has initiatives in progress, completed, or planned addressing the issues in this report. Management's comments and our evaluation of these responses are included in the report.

We appreciate the cooperation and courtesies provided by your staff during the audit. If you have any questions, please contact Debra Ritt, director, Transportation, at (703) 248-2198 or me at (703) 248-2300.

Richard F. Chambers
Assistant Inspector General
for Performance

Attachment

cc: Richard D. Weirich
Nicholas F. Barranca
Jim Golden
John R. Gunnels

TABLE OF CONTENTS

Part I

Executive Summary	i
-------------------	---

Part II

Introduction

Background	1
Objective, Scope, and Methodology	2
Prior Audit Coverage	3

Audit Results

Plan Inventory	4
Recommendation	4
Management's Comments	5
Evaluation of Management's Comments	5

Adequacy of Plans	6
Contingency Plans	6
Continuity Plans	8
Recommendations	10
Management's Comments	10
Evaluation of Management's Comments	10

Testing	12
Recommendation	13
Management's Comments	13
Evaluation of Management's Comments	13

Quality Assurance Process	14
Recommendation	15
Management's Comments	15
Evaluation of Management's Comments	15

Appendices

Appendix A. Results of Contingency Plan Reviews	16
Appendix B. Prior Inspector General Y2K Reports	19
Appendix C. Statistical Sampling and Projections for Review of Year 2000 Continuity Plans	21
Appendix D. Contingency and Continuity Plans with Inadequate Testing Justification	22
Appendix E. Management's Comments	24

EXECUTIVE SUMMARY

Introduction

This is the Office of Inspector General's (OIG) second report on the status and quality of the United States Postal Service's (Postal Service) business contingency and continuity plans,¹ and the eleventh in a series of reports² regarding the Postal Service Year 2000 (Y2K) initiative. This report addresses whether contingency and continuity plans: (1) exist for all high-impact areas, (2) are adequate for successful implementation, and (3) have been sufficiently tested.

Results in Brief

The Postal Service has made significant progress in developing business contingency and continuity plans. To date continuity plans have been prepared for 32 high-impact disruptions and contingency plans have been prepared for 173 severe or critical systems and equipment. However, a contingency plan has yet to be developed for the Equal Employment Opportunity Complaint Tracking System. Without a plan, should a disruption occur, the Postal Service might not be able to process complaints within legal time requirements. Additionally, although the Postal Service has continuity plans for high-impact areas, it has not yet developed contingency plans for all external suppliers. If these plans are not completed, managers may not have alternative suppliers to rely on in the event that primary suppliers encounter Y2K disruptions.

Furthermore, while the Postal Service had developed plans for its high-impact areas, plan quality varied. Specifically, contingency plans did not adequately address at least 4 to as many as 11 of 12 key elements recommended by Postal Service standards. While plan elements vary in importance, each element increases Postal Service preparedness to handle disruptions. Therefore, to the extent that plans exclude some of the elements, the Postal Service may encounter delays in recovering from disruptions in critical business functions and information processing. Finally, we noted that 16 contingency plans did not adequately identify other supporting plans. As a result, users may not be able to access information needed to fully implement contingency plans.

¹ Continuity plans address potential failures primarily caused by errors in business partner or public infrastructure systems, while contingency plans address potential failures in systems internal to the Postal Service.

² See Appendix B for a list of these reports.

Similar to our review of contingency plans, our review of continuity plans disclosed incomplete areas. Continuity plans generally did not include well-defined operating procedures for 17 of 32 disruption scenarios, nor were resource requirements fully developed for the 32 scenarios. As a result, the Postal Service may not have a well-defined response to disruptions and staff may not be fully prepared to manage them.

We also found that the Postal Service was identifying roles and responsibilities for Y2K business resumption activities under an initiative separate from its business contingency and continuity planning initiative. Accordingly, Postal Service management should ensure that these areas are integrated into continuity plans and that plans adequately reference activities that support them.

Key to preparing for Y2K, is the testing of contingency and continuity plans. Testing is particularly needed to determine whether incomplete plans are capable of supporting the agency's core business processes and can be implemented within a specified period of time. However, the Postal Service does not plan to test 124 (60 percent) of its plans, all of which were incomplete in some manner. In addition, the Postal Service did not adequately justify its reasons for not testing at least 44 of the 124 plans. Further, we could not determine whether the Postal Service considered testing all plan scenarios relating to severe or critical Finance systems.

Since our last report,³ the Postal Service has proposed steps to enhance quality assurance over its contingency and continuity planning efforts. While these proposed steps are commendable, greater oversight and testing of plans is needed to ensure they are consistent, properly integrated and sufficiently tested across organizational initiatives. In addressing the deficiencies we noted, the quality assurance process should consider the time remaining before the calendar year rollover, possible leap year disruptions, and operational disruptions from computer security failures that may interrupt mail services.

³ See Appendix B for a listing of reports.

**Summary of
Recommendations**

While it may not be practical to refine all contingency and continuity plans by the end of the year, the Postal Service should concentrate on those of highest impact to its operations. At a minimum, we recommend that the Postal Service develop a plan for the Equal Employment Opportunity Complaint Tracking System and expand testing to those areas where plans are not fully developed. We also recommend that management ensure that proposed quality assurance steps be taken to ensure that plans are adequately integrated with other supporting plans and organizational initiatives, and are properly tested. In the long-term, we believe the Postal Service needs to consider not only possible leap year disruptions, but also operational disruptions from computer security failures that may interrupt mail services. For these reasons, comprehensive plans for all severe or critical systems and for all high-impact failure scenarios should be pursued.

**Summary of
Management's
Comments**

Management agreed with our findings and recommendations to develop a plan for the Equal Opportunity Complaint Tracking System and to require that quality assurance steps be taken to ensure that plans are adequately integrated and properly tested. In addition, management agreed with our finding and recommendation to integrate supporting contingency and continuity plans, but did not agree to integrate other organizational initiatives. They stated there was less value in integrating plans with other initiatives such as deployment, assignment of roles and responsibilities, and change configuration management because overall year 2000 program interdependencies are actively monitored by the senior executive council. Management also agreed that they needed to update and improve plans and directed business owners to conduct additional reviews. Any plans found lacking would be updated and republished.

Management disagreed with our recommendation, as stated, to expand the testing of contingency and continuity plans. However, management plans to require, where appropriate, business owners to either provide adequate justification for not testing plans or conduct tests.

We have summarized management's comments in the report and included the full text of their comments in Appendix E.

**Overall Evaluation of
Management's
Comments**

Management's comments were generally responsive to our findings and recommendations. Planned and on-going actions should further mitigate the risk of potential year 2000 disruptions. While we found management comments generally responsive, we continue to believe that organizational integration is critical to ensure adequate coordination between related initiatives. Because the Postal Service used a fragmented approach to planning and lacked an adequate quality assurance process, we are not confident that the monitoring performed by the senior executive council is sufficient to ensure interdependencies are adequately coordinated.

Although management disagreed with our recommendation relating to the testing of plans as stated, we found management's action to ask business owners to either further justify not testing or conduct tests, responsive to our findings. Such actions further validate management's efforts to mitigate year 2000 disruptions.

INTRODUCTION

Background

The Y2K computing problem poses significant risks that, if not adequately addressed, could have serious consequences for the Postal Service. For example, the timely delivery of the nation's mail could be at risk if Postal Service systems and equipment do not function properly. Ensuring that mail delivery is not disrupted at the turn of the century is no small undertaking in such a large and diverse organization as the Postal Service.

In June 1999, the Postal Service headquarters developed a continuity plan that addressed 32 external failure scenarios, which could occur primarily due to disruptions in business partner or public infrastructure systems. This plan was subsequently distributed to the field for local adaptation, and 508 local plans were generated from the master plan. The scenarios within this plan comprise disruptions to:

- Public infrastructure (e.g., banking, telecommunications, and electrical power);
- Postal Service supply chain (e.g., air transportation, and surface transportation);
- Critical inventory (e.g., mail transport equipment, stamps, and supplies);
- Mailing patterns resulting from changes in mailer behavior; and
- Services provided by high-impact, critical business partners.

In addition, as of September 1999, the Postal Service reported that it had developed contingency plans to mitigate potential Y2K disruptions for 220 internal systems, including 137 classified as severe⁴ or critical⁵ information systems and another 38 pertaining to mail processing systems. These plans were developed by each of the five core business areas--Processing and Distribution, Finance, Marketing, Mail Operations, and Enabling.

There are several offices within the Postal Service responsible for completing Y2K program initiatives. The chief operating officer and executive vice president serves

⁴ Severe systems are those that are crucial to core business activities.

⁵ Critical systems are those which, in the event of failure, will have significant impact on Postal Service's operations.

as the lead executive for business continuity planning. The senior vice president, chief technology officer is responsible for contingency plans relating to internal system failures.⁶

Objective, Scope, and Methodology

The overall objective of our continuing audit coverage is to report on the status and quality of Y2K business contingency and continuity plans. This report addresses the last two phases of business contingency and continuity planning recommended by GAO⁷—plan development and testing. Our specific objectives were to determine whether contingency and continuity plans (1) exist for all high-impact areas, (2) are adequate for successful implementation, and (3) have been sufficiently tested.

To determine whether contingency and continuity plans exist for all high-impact areas, we reconciled Postal Service plans to progress reports and to its inventory of severe or critical systems as of September 30, 1999.

In assessing the completeness of contingency plans for information and mail processing systems, we compared them to standards developed by the Postal Service. Postal Service standards highlighted 12 elements of a successful plan. A consultant engaged in auditing Y2K business contingency and continuity plans also validated our evaluation criteria. To the extent that contingency plans supported continuity plans or other contingency plans, we considered the adequacy of both plans in our assessments.

To evaluate the adequacy of Postal Service plans, we assessed the completeness of plans and level of integration between contingency and continuity plans. In assessing plan completeness, we compared the master continuity plan to standards issued by the Mitre Corporation, Information Systems Audit and Control Association, and the Federal Financial Institutions Examination Council. In addition, to determine the level of customization of the master plan that was performed by 508 field units for the 32 failure scenarios, we reviewed a statistically selected sample of 115 field continuity plans.

To assess the sufficiency of plan testing, we reviewed

⁶A system comprises several components or subsystems.

⁷Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, August 1998).

planned tests as well as the first round of testing results. In addition, where available, we analyzed test decisions to determine whether the Postal Service adequately supported decisions not to test.

Our audit work was accomplished during the period August 1999 to November 1999 in accordance with generally accepted government auditing standards and included tests of internal controls as were considered necessary under the circumstances.

Prior Audit Coverage

During our continuing coverage of the Postal Service Y2K initiative, we issued ten reports⁸ covering remediation, validation, reporting quality, budgeting, contracting, and business continuity planning. In our previous audit of business contingency and continuity planning, we noted several areas where management needed to strengthen its strategy and business impact analysis. We recommended that the chief operating officer and executive vice president (1) specify the extent of testing for contingency plans and monitor remaining milestones, (2) ensure sufficient funding for plan execution, (3) establish a more comprehensive quality assurance process, (4) revise supplier assessments and make adjustments to plans accordingly, and (5) communicate service commitment expectations to the field. Management agreed with our findings and recommendations. Their planned or completed actions were responsive to our recommendations.

⁸ See Appendix B for a listing of reports.

AUDIT RESULTS

Plan Inventory

The Postal Service has made significant progress in developing contingency and continuity plans. Continuity plans have been developed for 32 high-impact disruptions and contingency plans have been prepared for 173⁹ severe or critical information systems and equipment. However, a contingency plan has not yet been developed for one critical system--the Equal Employment Opportunity Complaint Tracking System,¹⁰ within the Enabling business area. This system is used to track complaints filed and the timeliness of complaint investigation and processing. Without a plan for this system, the Postal Service may not be able to process complaints within legal time requirements should Y2K disruptions occur.

Although the Postal Service has continuity plans for high-impact areas, including business partner and public infrastructure systems, plans have not been developed in the event that critical external suppliers are not Y2K compliant. The Postal Service stated that it was developing supplier contingency plans; however, because there is less than two months remaining before the end of the year, we are concerned they may not have sufficient time to complete these plans. As a result, if suppliers cannot perform, managers may not have alternative suppliers to turn to on short notice. This issue and related recommendations are discussed in greater detail in our November 1999 report.¹¹

Recommendation

We recommend that the chief operating officer and executive vice president, in conjunction with the senior vice president, chief technology officer :

1. Ensure that a plan is developed for the Equal Employment Opportunity Complaint Tracking System.

⁹ Contingency plans relating to two of the severe or critical information and mail processing systems (the Equal Employment Opportunity Complaint Tracking System and the Address Management System - Personal Computer) were not reviewed

¹⁰ Index number 1012.00 in Postal Service's inventory.

¹¹ Year 2000 Initiative: Suppliers, Mail Processing Equipment, Facilities, and Embedded Chips (Report No. IS-AR-00-001).

Management's Comments	Management agreed with our finding and recommendation to develop a plan for the Equal Opportunity Complaint Tracking System. They stated that although the original plan could not be located, a new plan has been developed for this system.
Evaluation of Management's Comments	Management's comments are responsive to our finding and recommendation. The development of a contingency plan for the Equal Opportunity Complaint Tracking System completes the Postal Service requirement to have plans for all severe or critical systems.

Adequacy of Plans

Because of the risk of Y2K failures, comprehensive business contingency and continuity plans are essential to continuing core operations. Without well-defined plans, the Postal Service may not be able to respond appropriately or have sufficient time to develop alternatives if unpredicted failures occur.

Contingency Plans

Contingency plans for 173 severe or critical information and mail processing systems we reviewed did not adequately address at least 4 to as many as 11 of the 12 elements recommended by Postal Service standards. According to these standards,¹² plans should address the following 12 key elements:

- Objective or scenario,
- Criteria/trigger for invoking the plan,
- Expected life of the plan,
- Procedures for operating in contingency mode,
- Roles assigned to actions,
- Responsibilities assigned to individuals,
- Authority to execute plans,
- Personnel required to execute plans,
- Scheduling of labor,
- Tools --e.g., materials, supplies, facilities, communications equipment,
- Funding requirements, and
- Criteria and procedures for returning to normal operations (normalization procedures).

According to Postal Service officials, these standards vary in importance and the absence of any one element may not render the plan ineffective. However, industry standards acknowledge that the 12 elements are all important for successful plan implementation. The absence of one or more of these elements increases the risk that the plan may not work as intended. The quality of plans varied by the five business areas. Plans in the Processing and Distribution Systems area were most complete, while those in the Enabling area were least complete.

¹² USPS standards are consistent with industry standards such as the Mitre Corporation, Information Systems Audit and Control Association, and the Federal Financial Institutions Examination Council.

The 38 plans addressing processing and distribution systems were generally missing parts of four key elements (objectives, assigning responsibility to individuals, scheduling, and tools) needed for successful plan implementation. For example, individuals responsible for implementing the plan were not identified. This element is needed to ensure that accountability for all plan steps has been assigned. Further, under the areas of scheduling and tools, current software versions are to be installed and hardware configurations checked before the contingency plan can be implemented. However, none of the contingency plans showed whether or when these steps had to be done. As stated in our November 1999 Y2K report,¹³ while the Postal Service has an adequate process in place to ensure critical mail processing equipment functions properly, it also needs to closely monitor deployment of Y2K remediated software to ensure the correct versions are being installed prior to Y2K.

Following processing systems, 43 Finance and 28 Marketing plans generally did not adequately address seven elements from the standards. For Finance plans, four of the seven elements related to general resource requirements: personnel, scheduling, tools, and funding. The remaining three elements included assigning individual responsibilities, associating roles with actions, and including procedures for returning to normal operations. We noted that while these elements often were not addressed in contingency plans, they were at times stated in separate communications plans. Similarly, Marketing plans did not adequately address roles, responsibilities, and resource requirements. In addition, Marketing plans did not adequately address the life of plans.

Furthermore, 31 Mail Operations plans generally did not adequately address nine elements including triggers, plan life, roles, responsibilities, personnel requirements, scheduling, tools, funding, and well-defined objectives.

Finally, 33 plans in the Enabling business area generally did not adequately address 11 key elements. The only key element that was complete was contact information for personnel with authority to invoke the plans.

¹³ Year 2000 Initiative: Suppliers, Mail Processing Equipment, Facilities, and Embedded Chips (Report No. IS-AR-00-001).

Contingency plans were incomplete because they were developed by several different business areas that were given maximum latitude to design plans as they saw fit. While this approach ensured plans were developed by those most knowledgeable of the severe or critical systems, it resulted in inconsistent plan development. In addition, a centralized quality assurance process was not in place to ensure that plans were revised in accordance with Postal Service standards. Without comprehensive contingency plans, the Postal Service may encounter delays in recovering critical business functions and information processing.

We also noted that 16 contingency plans cited dependencies on other plans, but did not adequately refer to those plans. For example, the contingency plan for the Intra-Alaska Dispatch System referred to a group of Process Accounts Payable plans, but did not reference a specific plan under this grouping. In another example, key elements for the Finance area were spread between contingency plans and communications plans. Providing minimal reference information and dividing key elements among separate plans makes it more difficult for users to readily access information needed for operating in a contingency mode.

Detailed results of our review of each business area are provided in Appendix A.

Continuity Plans

Continuity plans were incomplete for the 32 high-impact disruption scenarios. Specifically, plans did not include well-defined operating procedures for 17 of the 32 scenarios, nor were resource requirements fully developed for the 32 scenarios. Although headquarters expected procedures and resource requirements to be further defined by field units, we estimated that at least 91 percent of 508 field plans¹⁴ were not modified beyond providing additional contact information. As a result, the Postal Service may not have a well-defined response and staff may not be fully prepared to manage disruptions. Prolonged business disruptions could jeopardize the Postal Service's image as a reliable provider of mail services.

¹⁴ See Appendix C for the basis of our statistical analysis.

In 6 of 17 scenarios, we also noted that procedures would not be developed until the time of disruption or were to be addressed under a separate initiative. For example, in the event of a Customs failure impacting the flow of international mail, the Postal Service's plan is to work with Customs to determine the best plan for either holding the mail or manually processing selected items. In another example, procedures for restoring data communications were being developed under a separate information technology initiative. While this may be true, the Postal Service was unable to demonstrate that these procedures had been developed or reconciled to business continuity scenarios to ensure organizational readiness in these areas. We believe the absence of procedures may contribute to unnecessary delays in moving the mail.

In addition, other factors critical to successful plan implementation were being addressed under separate organizational initiatives and were not integrated into continuity plans. For example, Postal Service representatives stated that assigning roles and responsibilities for business resumption activities is being addressed under the recovery management initiative. While this may be true, recovery management is not responsible for assigning roles and responsibilities. Field units are ultimately responsible for this activity, but currently there is no process in place to ensure this occurs. As a result, a single continuity plan, by itself, does not contain all of the elements needed for successful implementation, which creates challenges for the field if plans are to be implemented.

In addition, plans did not refer to supporting activities or to other plans that support them. For example, in 11 of 32 scenarios, continuity plan procedures included executing contingency plans; however, they did not refer to specific contingency plans.

With little time remaining before the calendar year rollover, the Postal Service will need to determine how best to address plan deficiencies. While it may not be practical to complete development of all contingency and continuity plans by the end of the year, the Postal Service will need to concentrate on those highest impact plans. However, in the long-term, the Postal Service needs to consider not only

possible leap year disruptions, but also operational disruptions from computer security failures that disrupt mail services. For these reasons, comprehensive plans for all severe or critical systems and for all high-impact failure scenarios should be pursued.

Recommendations

We recommend that the chief operating officer and executive vice president, in conjunction with the senior vice president, chief technology officer:

2. Integrate supporting contingency and continuity plans and other organizational initiatives.

**Management's
Comments**

Management agreed with our finding and recommendation (number 2) to integrate supporting contingency and continuity plans but did not agree to integrate other organizational initiatives. They stated there was less value in integrating plans with other initiatives such as deployment, assignment of roles and responsibilities, and change configuration management because overall year 2000 program interdependencies are actively monitored by the senior executive council. Moreover, management implied that the Office of Management and Budget has endorsed their decision not to include individual roles and responsibilities in business contingency and continuity plans.

**Evaluation of
Management's
Comments**

Management's comments were not fully responsive to our findings and recommendation regarding plan integration. While management agreed to better integrate contingency and continuity plans, they did not agree to integrate plans with other organizational initiatives. We continue to believe that this type of integration is critical to ensure adequate coordination between related initiatives. Because the Postal Service used a fragmented approach to planning and lacked an adequate quality assurance process, we are not confident that the monitoring performed by the senior executive council is sufficient to ensure interdependencies are adequately coordinated. In addition, we believe management has taken the Office of Management and Budget's statement regarding the assignment of roles and responsibilities out of context. The Office of Management and Budget's statement related to the Postal Service's Day One Strategy Guide, and not its continuity or contingency plans. Contrary to management's assertion, industry

guidance suggests that plans should describe the assignment of roles and responsibilities of key individuals. This is needed to ensure that these individuals are familiar with their roles and responsibilities for executing plan steps.

In the long-term we recommend that the chief operating officer and executive vice president, in conjunction with the senior vice president, chief technology officer direct business areas to:

3. Further complete business contingency and continuity plans, beginning with those areas of greatest risk.

**Management's
Comments**

Management agreed with recommendation 3 that they needed to update and improve plans but stated that they considered all elements and only included those they believed was appropriate. Nevertheless, in light of our findings, management is directing business owners to conduct additional reviews of plans and update and republish any plans found lacking.

**Evaluation of
Management's
Comments**

Management's actions to conduct additional reviews of plans and update where necessary are responsive to our findings and recommendation. Additional reviews focusing on the completeness of plans should further strengthen management's efforts to mitigate year 2000 disruptions.

Testing

Key to preparing for Y2K is the testing of contingency and continuity plans. Testing is needed to determine whether plans are capable of providing the level of support to the agency's core business processes and can be implemented within a specified period of time. Integration testing across multiple departments, including external business entities as appropriate, must also be conducted where needed. Thus, testing should uncover operational elements requiring adjustments to assure successful plan execution and assure that individuals understand the procedures and their roles.

We found that the Postal Service does not plan to test 124 (60 percent),¹⁵ of its business continuity and severe or critical contingency plans, although testing is encouraged by GAO and industry standards and, as discussed previously, plans are generally incomplete. According to the Postal Service, the 124 plans comprise standard operating procedure or are so simple they do not require rehearsal. Specifically, 49 plans address standard operating procedures and 75 plans were considered to be simple to execute. We believe the importance of testing cannot be overemphasized because in 19 cases where the Postal Service conducted pre-tests, plans delivered unanticipated results and required adjustments. Specifically, Y2K representatives for the Forwarding Control System re-wrote the related contingency plan after initial attempts to test the plan showed that it was not executable. In addition, 18 contingency plans in the Mail Operations business area underwent significant revisions after a review of the soundness of the proposed contingency strategy revealed significant weaknesses.

The Postal Service prepared justifications for not testing the 124 plans and while we agree that all plans do not require comprehensive testing, we believe that the Postal Service did not sufficiently justify its decision for at least 44 of the 124 plans. For example, the Postal Service decided not to test several plans in the Marketing area because the probability of disruption was low and confidence in the plan was high. These high confidence levels may not be justified

¹⁵ Sixty percent (124 of 205) plans will not be tested. The 205 include 32 failure scenario plans, 135 information system plans, and 38 mail processing equipment plans.

Considering the extreme uncertainty of potential Y2K problems. A listing of the 44 plans lacking adequate justification is provided in Appendix D.

Further, we were also unable to determine whether the Postal Service plans to test all severe or critical scenarios within the Finance business area. The Postal Service test decisions did not specify which scenarios within each plan were considered.

Due to deficiencies existing in contingency and continuity plans and current time constraints, additional testing of plans would provide more assurance that the Postal Service can effectively manage disruptions. In particular, plan walk-throughs, at a minimum, would ensure that applicable personnel, at all levels of the organization, understand plan procedures, their roles, and responsibilities.

Recommendation

Although little time remains before the calendar year rollover, we recommend that the chief operating officer and executive vice president, conjunction with the senior vice president, chief technology officer:

4. Expand testing of contingency and continuity plans to the maximum extent possible. At a minimum, conduct walk-throughs for those plans that are incomplete.

**Management's
Comments**

Management disagreed with our recommendation to expand the testing of contingency and continuity plans. It stated that the level of testing performed to date coupled with the dress rehearsal conducted in late November 1999 is more than adequate to ensure that the Postal Service is ready to effectively implement contingency and continuity plans. Rather management plans to require, where appropriate, business owners to either provide adequate justification for not testing plans or conduct tests.

**Evaluation of
Management's
Comments**

Although management disagreed with our recommendation, as stated, we found management's action to ask business owners to either further justify not testing or conduct tests, responsive to our findings. Such actions further validate management's efforts to mitigate year 2000 disruptions.

**Quality Assurance
Process**

In our previous report on business continuity planning,¹⁶ we recommended that the Postal Service enhance its quality assurance process to provide needed oversight of business contingency and continuity planning efforts. In response to our findings, the Postal Service stated that integration of business contingency and continuity plans is being undertaken to ensure that all cross-references between the plans are clear and easy to follow. Further, a dress rehearsal, scheduled for late November, has been added to the project plan to test the readiness of the field, as well as their understanding of how and when to use business contingency and continuity plans. Finally, the chief operating officer and executive vice president has mandated that individuals, throughout the organization, be assigned accountability for the roles and responsibilities and the implementation of plans, should the need arise. Thus, accountability will be monitored through a certification process.

While we believe these proposed actions should further strengthen business contingency and continuity plans, adequate oversight is needed to ensure that gaps in planning are addressed and that plans are properly integrated and sufficiently tested across multiple organizational initiatives. Further, relying on business managers alone to certify that plans are complete or that roles and responsibilities have been assigned will not provide adequate assurance that these steps have been taken. For instance, business areas certified that continuity plans were sufficient for local implementation; however, little or no changes were made to adapt the continuity plans. According to the manager for business continuity planning, the field did not sufficiently develop procedures for at least two scenarios (facility closures and inability of employees to get to work), although managers had given their assurances that plans were complete.

In addressing any quality assurance process deficiencies, the Postal Service should consider the time remaining before the calendar year rollover, possible leap year disruptions, and operational disruptions from computer security failures that interrupt mail services.

¹⁶ See Appendix B for a listing of reports.

Recommendation	<p>We recommend that the chief operating officer and executive vice president:</p> <p>5. Require that the proposed quality assurance steps be taken to ensure that plans are adequately integrated with other supporting plans and organizational initiatives, and are properly tested.</p>
Management's Comments	<p>Management agreed with our finding and recommendation to require quality assurance steps be taken to ensure that plans are adequately integrated and properly tested. They stated that plans would be reviewed, tests concluded, dress rehearsals conducted, and plans updated and republished, where required.</p>
Evaluation of Management's Comments	<p>Management's comments are responsive to our finding and recommendation. A continual quality assurance process increases confidence that plans will work as intended.</p>

APPENDIX A

RESULTS OF CONTINGENCY PLAN REVIEWS

The following tables summarize by business area the number and percentage of contingency plans lacking key elements recommended for successful implementation.

Processing and Distribution Contingency Plans

	<i>Elements of a Successful Plan</i>	<i>Severe and Critical Systems (38 Plans)</i>	
		<i>Number Plans with Incomplete Key Elements</i>	<i>% Plans Key with Incomplete Key Elements</i>
1	Objectives (Scenario)	38	100%
2	Trigger event	0	0%
3	Life of plan	0	0%
4	Procedures (actions)	0	0%
5	Roles assigned to actions	0	0%
6	Responsibilities assigned to individuals	28	74%
7	Contact information provided for personnel with authority to execute plans	0	0%
8	Personnel requirements	4	11%
9	Scheduling requirements	38	100%
10	Tools requirements	36	95%
11	Funding requirements	5	13%
12	Procedures and criteria for normalizing operations	0	0%

Finance Contingency Plans

	<i>Elements of a Successful Plan</i>	<i>Severe and Critical Systems (43 Plans)</i>	
		<i>Number Plans with Incomplete Key Elements</i>	<i>% Plans Key with Incomplete Key Elements</i>
1	Objectives (Scenario)	0	0%
2	Trigger event	0	0%
3	Life of plan	6	14%
4	Procedures (actions)	0	0%
5	Roles assigned to actions	17	40%
6	Responsibilities assigned to individuals	34	79%
7	Contact information provided for personnel with authority to execute plans	0	0%
8	Personnel requirements	29	67%
9	Scheduling requirements	29	67%
10	Tools requirements	32	74%
11	Funding requirements	7	16%
12	Procedures and criteria for normalizing operations	25	58%

Marketing
Contingency Plans

	<i>Elements of a Successful Plan</i>	<i>Severe and Critical Systems (28 Plans)</i>	
		<i>Number Plans with Incomplete Key Elements</i>	<i>% Plans Key with Incomplete Key Elements</i>
1	Objectives (Scenario)	1	4%
2	Trigger event	4	14%
3	Life of plan	5	18%
4	Procedures (actions)	0	0%
5	Roles assigned to actions	6	21%
6	Responsibilities assigned to individuals	14	50%
7	Contact information provided for personnel with authority to execute plans	0	0%
8	Personnel requirements	10	36%
9	Scheduling requirements	23	82%
10	Tools requirements	9	32%
11	Funding requirements	9	32%
12	Procedures and criteria for normalizing operations	2	7%

Mail Operations
Contingency Plans

	<i>Elements of a Successful Plan</i>	<i>Severe and Critical Systems (31 Plans)</i>	
		<i>Number Plans with Incomplete Key Elements</i>	<i>% Plans Key with Incomplete Key Elements</i>
1	Objectives (Scenario)	13	42%
2	Trigger event	8	26%
3	Life of plan	16	52%
4	Procedures (actions)	4	13%
5	Roles assigned to actions	17	55%
6	Responsibilities assigned to individuals	30	97%
7	Contact information provided for personnel with authority to execute plans	0	0%
8	Personnel requirements	25	81%
9	Scheduling requirements	31	100%
10	Tools requirements	20	65%
11	Funding requirements	23	74%
12	Procedures and criteria for normalizing operations	4	13%

Enabling
Contingency Plans

	<i>Elements of a Successful Plan</i>	<i>Severe and Critical Systems (33 Plans)</i>	
		<i>Number Plans with Incomplete Key Elements</i>	<i>% Plans Key with Incomplete Key Elements</i>
1	Objectives (Scenario)	6	18%
2	Trigger event	5	15%
3	Life of plan	8	24%
4	Procedures (actions)	11	33%
5	Roles assigned to actions	21	64%
6	Responsibilities assigned to individuals	33	100%
7	Contact information provided for personnel with authority to execute plans	0	0%
8	Personnel requirements	20	61%
9	Scheduling requirements	28	85%
10	Tools requirements	21	64%
11	Funding requirements	21	64%
12	Procedures and criteria for normalizing operations	10	30%

APPENDIX B

PRIOR INSPECTOR GENERAL Y2K REPORTS

In November 1999, we issued a report entitled Year 2000 Initiative: Suppliers, Mail Processing Equipment, Facilities, and Embedded Chips (Report No. IS-AR-00-001 dated November 30, 1999), which noted that the Postal Service needs to place more emphasis on the issue of alternative suppliers. Specifically, we recommended that the Postal Service needs to develop supplier contingency plans and establish a no-later-than date when it will look to these alternative suppliers to take over for its at-risk critical suppliers, i.e., suppliers who may not be Y2K ready or who have already reported their inability to become Y2K ready.

In September 1999, we issued a report entitled Business Contingency and Continuity Planning: Initiation and Business Impacts, (Report No. TR-AR-99-002 dated September 29, 1999), that noted several areas in which management had taken positive steps to mitigate Y2K disruptions. In addition, our audit identified several areas in which management needs to strengthen its strategy and business impact analysis.

In September 1999, we issued a report entitled Year 2000 Initiative: Review of Administration: Status Report on Postal Service Year 2000 Readiness, (Report No. IS-AR-99-002 September 20, 1999), that provided the May 1999 status of postal initiatives relating to information systems, exchanges, contingency plans, mail processing equipment, suppliers, facility sites, continuity plans, and testing.

In July 1999, we issued Year 2000 Initiative: Review of Administration, (Report No. FR-MA-99-002 dated July 7, 1999). Among the more significant issues, we noted that adequate controls often were not in place to monitor contractor activities, information often had not been provided to Integrated Business Systems Solutions Center personnel to help in controlling Y2K resources, and work products provided by contractor personnel were not timely or adequate.

The OIG and General Accounting Office established a joint partnership in the fall of 1998, to work on Y2K issues which led to February 1999 testimony before several House subcommittees. The Inspector General testimony on the Postal Service Y2K Initiative, (Report No. IS-TR-99-001 dated February 23, 1999), addressed major challenges facing the Postal Service. These included: developing and implementing a business contingency and continuity plan; determining whether external suppliers and Postal facilities are Y2K ready; deploying solutions and testing mail processing equipment; and reviewing, correcting, and testing information systems, data exchanges, and information technology infrastructure. The GAO delivered testimony entitled "Year 2000 Computing Crisis: Challenges Still Facing the U.S. Postal Service (GAO/T-AMID-99-86, dated February 23, 1999) which addressed Y2K operational issues similar to those presented in the IG testimony.

In February 1999, we issued a Y2K report entitled Year 2000 Initiative: Program Management Reporting (Report No. IS-AR-99-001, dated February 18, 1999) that addressed quality and reliability of Y2K information reported to senior managers. We found that Y2K briefings and reports to senior management were not often complete, consistent, or clear. Y2K briefings did not include a standard report on the overall status of Y2K progress and were not provided at regularly scheduled intervals. As a result, senior managers were not always able to use the information to monitor Y2K progress and make informed decisions.

In September 1998, we issued a Y2K report entitled Year 2000 Initiative: Post Implementation Verification, (Report No. IS-AR-98-003, dated September 29, 1998), that involved an assessment of the efficiency and effectiveness of the process implemented as an independent check on Postal Service remediation efforts. This report recommended that the Postal Service modify its system certification and post implementation verification procedures to improve the quality of systems sent to verification as well as the process itself. Postal Service management fully concurred with our findings and recommendations.

In July 1998, we issued a Y2K report, entitled Year 2000 Initiative: Status of the Renovation, Validation, and Implementation Phases, (Report No. IS-AR-98-002, dated July 21, 1998), that involved a preliminary assessment of the renovation, validation, and implementation phases of the Postal Service Y2K initiative. It contained recommendations for improvement in several areas including accurately reporting the compliance status of systems applications. Postal Service management fully concurred with our findings and recommendations.

In July 1998, we issued a letter report, entitled Year 2000 Contract Indemnification Advisory Letter (Report No. CA-LA-98-001, dated July 7, 1998), that addressed negotiations between the Postal Service and a consulting firm regarding the Y2K program management contract's indemnification clause. That letter contained suggestions to Postal Service management regarding the indemnification issue.

Our first Y2K report entitled Year 2000 Initiative, (Report No. IS-AR-98-001 dated March 31, 1998). During this review, we examined the awareness and assessment phases of the Postal Service Y2K initiative and made recommendations for improvement in several areas including assigning accountability to responsible managers. Postal Service management fully concurred with our findings and recommendations.

APPENDIX C

STATISTICAL SAMPLING AND PROJECTIONS FOR REVIEW OF Y2K CONTINUITY PLANS

Purpose of the Sampling

One of the objectives of this review was to assess the degree to which the Y2K business continuity plans submitted were tailored for local conditions. In support of this objective, the audit team employed a simple random attribute sample design that allows statistical projection of the plans received from individual facilities.

Definition of the Audit Universe

The audit universe consisted of 508 submitted plans. No projection is made to facilities that should have submitted plans but did not do so.

Sample Design

The audit used a simple random sample design. We randomly selected 115 plans for review, to provide a one-sided 95 percent confidence interval with 6.5 to 7 percent precision for the assumed condition of 50 percent of tailored plans in the sample.

Statistical Projections of the Sample Data

The tested attribute, e.g., whether business continuity plans were substantially tailored as compared to the template plan provided by Postal management, is projected to the universe of 508 plans.

Based on projection of the sample results, we are 95 percent confident that at least 90.7 percent or 461 plans, were not substantially tailored. The unbiased point estimate is 93.9 percent, or 477 plans.

APPENDIX D

Contingency and Continuity Plans With Inadequate Testing Justification

Business Area	Plan ID--Title/Scenario	Criticality/Impact Probability Rating
Business Continuity	Mail Transport Equipment (MTE) Availability	High
Business Continuity	Surface Transportation (Long Haul Trucking) Section 2	High
Business Continuity	US Customs Service	High
Business Continuity	Telecommunications – Section 3 Processing	High
Business Continuity	Indianapolis	High
Business Continuity	Local Transportation and Traffic Infrastructure	High
Business Continuity	Surface Transportation (Long Haul Trucking), Section 1	High
Business Continuity	Employees Reporting to Work Section 1: All Processes and Sub-Processes	High
Business Continuity	Emery (PMPC) Operations Section 2: Counts, Assigns Route Tag (CART) Assignment System	High
Business Continuity	Domestic Air Transportation	High
Business Continuity	Potential Facility Closures	High
Business Continuity	Postal Service Products and Supplies	High
Business Continuity	Disruptions to Customer System Create Abnormal Mailing Behavior	High
Business Continuity	Anticipated Disruptions Cause Changes in Mailing Behavior	High
Enabling	Human Resources – Workers Compensation Information System (WCIS)	Critical
Enabling	Tracking and Reduction-In-Force (TARIF)	Critical
Enabling	Human Resources - Safety and Health (S&H)	Critical
Enabling	Drivers Screening System	Critical
Enabling	Strategic National Automated Purchasing System	Severe
Enabling	Human Resources - Risk Management Reporting System	Severe
Enabling	National Crime Information Center/National Law Enforcement Telecommunication System	Severe

Business Area	Plan ID--Title/Scenario	Criticality/Impact Probability Rating
Enabling	Human Resources – National Accident Reporting System	Severe
Enabling	Financial Exception Reporting System	Critical
Finance	Stamps Application Failure: Stamps Distribution Offices cannot log into the systems	Severe
Finance	Statement of Account Data Entry failure	Severe
Finance	Emergency Pay Adjustment System Failure - Payroll Scenario #20.	Critical
Mail Operations	National Change of Address (NCOA)	Critical
Mail Operations	Fast Forward	Critical
Mail Operations	Management Operating Data System (MODS)	Severe
Mail Operations	Corporate Information System Management Operating Data System (CIS MODS)	Severe
Mail Operations	Computerized Labeling and Address Sequence System (CLASSI)	Critical
Mail Operations	Drop Shipment Appointment System (DSAS)	Severe
Mail Operations	Rail Management Information Systems (RMIS)	Severe
Mail Operations	Address Matching System (AMS-API)	Severe
Mail Operations	Address Change Service (ACS) NCSC	Critical
Mail Operations	Management Operation Data System (PC-MODS)	Critical
Marketing	Meter Accounting and Tracking System (MATS)	Critical
Marketing	CISS IPSS Production Tracking System (IPTS)	Critical
Marketing	Consumer Affairs Messaging System (CAMS)	Critical
Marketing	Centralized Meter Licensing System (CMLS)	Critical
Processing and Distribution	Identification Code Sorting, PICS/SICS	Critical
Processing and Distribution	Vending Activity Reporting System (VARs)	Critical
Processing and Distribution	Delivery Barcode Sorter Input/Output Sub-System	Critical
Processing and Distribution	Computerized Forwarding System II	Critical

APPENDIX E. MANAGEMENT'S COMMENTS

CLARENCE E. LEWIS, JR.
CHIEF OPERATING OFFICER,
EXECUTIVE VICE PRESIDENT



December 3, 1999

RICHARD F. CHAMBERS
ASSISTANT INSPECTOR GENERAL
FOR PERFORMANCE

SUBJECT: Response to Draft Audit Report – Year 2000 Business Continuity and Contingency
Planning: Plan Development and Testing (TR-AR-00-DRAFT)

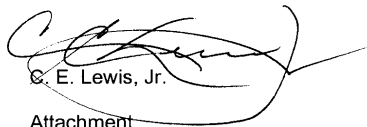
Thank you for providing the opportunity to respond to the Office of Inspector General (OIG) audit report on Year 2000 Business continuity and Contingency Planning: Plan Development and Testing and for recognizing in the report that the Postal Service has made significant progress in developing continuity and contingency plans.

As you are aware, the Postal Service routinely implements contingency plans so that our primary missions – moving the mail, protecting the welfare and safety of our employees, paying our employees and suppliers, and receiving revenue – are achieved. Although we have supplemented our existing procedures with additional plans to accommodate potential difficulties we may face with the rollover to Year 2000, adapting to disruptions such as airport closures, telecommunications outages, and transportation problems are, in fact, "business as usual" for the Postal Service. We are confident that the business areas responsible for each core process have feasible plans in place and have made appropriate decisions with respect to testing.

We had several meetings with members of your staff to discuss the preliminary findings, and although these meetings provided more common understanding in some areas, we were unable to agree on every issue. As the report suggests, there is limited time remaining before the calendar rollover, thus, our efforts must focus on those areas we believe may be at greatest risk to our primary mission.

The Postal Service views the Year 2000 problem as a business problem not a technology problem. Consequently, we have relied heavily upon the business areas to make appropriate decisions to maintain the readiness in their respective areas. However, in view of your concerns, I have asked the business owners to again review their contingency and continuity plans and to provide positive verification that the plans are feasible and tested as they deem appropriate.

If you require additional information in this regard, please feel free to contact James L. Golden, Year 2000 Initiative Executive Program Director, at (703) 526-2888.


C. E. Lewis, Jr.

Attachment

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-0080
202-268-4842
FAX: 202-268-4843

**Response to Recommendations
Draft Audit Report – (TR-AR-00-DRAFT)
Year 2000 Business Contingency and Continuity Planning
Plan Development and Testing**

Summary Comments:

The Postal Service is pleased that the Office of Inspector General (OIG) report recognized the significant progress made in developing the Component Contingency Plans (CCP's) and Business Continuity Plans (BCP's). These plans are vital to our ability to quickly and appropriately address any failures that might arise as a result of the Year 2000 rollover. We recognize and agree that we should prioritize our efforts to concentrate on those areas posing the greatest risk to the Postal Service's core processes. In view of the fact that little over 30 days remain before the end of the year, we have thoroughly examined the report findings and recommendations to determine where we should concentrate these efforts.

While the report highlighted some issues that have been or are being corrected, there are areas of fundamental differences of opinion. At the heart of the matter are two issues: (1) whether it is necessary for each plan to contain all 12 elements the OIG used to audit plan completeness – in particular, detailed procedures for all failure scenarios and the assignment of roles and responsibilities, and (2) whether there is value in conducting, at a minimum, walk throughs for all plans.

All of the 12 elements cited by the OIG were *considered* in the development of plans; however, not all elements are germane to or included in all plans. Where a specific element did not enhance the value of the plan, or was included in other plans or checklists, it was not specifically referenced in the plans the OIG reviewed. Moreover, all elements are not equally important to the plans, nor does the absence of one or more element necessarily increase the risk that the plan may not work as intended.

We believe the elements "Procedures for Operating in Contingency Mode" and "Authority to Execute Plans" are essential to each plan. While the OIG and we agree that these elements were included in the plans, the OIG has concerns about the adequacy of some procedures. Specifically, the OIG raised concerns that certain plans would require further definition depending on the exact circumstances of the failure. Because certain disruptions, such as Domestic Air Transportation, require different responses depending on the location and extent of the disruption, it is not feasible to address each possible combination and permutation in the plan itself. Additionally, the OIG expressed concern that many of the BCP's were not adequately customized by the field organizations. In fact, the BCP work segment owner expected only two plans to have significant field customization. We agree that not enough attention was paid to these two plans; however, additional customization is expected during the preparatory activities detailed in the Recovery Management Resource handbook.



A number of additional elements are important but not critical considerations in the development of the plans.

- 1) The objective or scenario was stated in all of the BCP's, but, in general, was not as clearly stated in the CCP's. Given that the objective of each CCP was to provide a workaround in the event of a component failure, the fact that an objective or scenario was not explicitly stated does not put the plans at risk.
- 2) A criteria/trigger for invoking the plan was generally included in all of the BCP's and generally not included in the CCP's. Given that the trigger for all CCP's was the failure of the component, the fact that this was not explicitly stated does not put the plan at risk.
- 3) A number of capability elements – roles assigned to actions, responsibilities assigned to individuals, personnel required to execute plans, and tools required – were often absent in both BCP's and CCP's. Although these were considered in the development of all plans, the actual determination of roles, responsibilities, personnel and tools has been assigned to the field and the business areas as part of their preparatory activities. These assignments have been detailed in the Recovery Management Resource Handbook, the Postmaster's Kit, the Engineering Year 2000 Recovery Management Kit and in the Finance Communications documents. The Office of Management and Budget (OMB) validated this approach in a review of the Recovery Management Plan by acknowledging that the assignment of roles and responsibilities for an enterprise as large and diverse as the Postal Service is best determined by the field.

The remaining elements are generally unimportant for all but a small number of plans where they are included.

- 1) Expected life of the plan is generally assumed to be until the component is fixed or the disruption is over.
- 2) Funding requirements have been dealt with through a finance directive that allows Year 2000 related extraordinary expenses to be reimbursed to the business area. For the vast majority of the plans, there are no anticipated additional funding requirements.
- 3) Criteria and procedures for returning to normal operations are only required in a small number of cases where a specific backup, rekeying of data, or specialized testing is required before normal operations are resumed. Where special procedures are required, they have been documented. Where they are not documented, they are not required.

Test decisions were based on the following criteria: 1) the extent to which the plan invokes a procedure that is considered "Standard Operating Procedure," or (2) is either so simple or the plan is to do nothing until the disruption is cured. In these instances, testing is not required. If the procedure is neither of the above, testing is conducted via a simple walk through of the plan or as a live test. We believe there is little value in testing procedures that are handled as part of our normal operations, or for which the response is to do nothing, or where the plan is so simple that the test would provide no benefit. However, we have asked the business owners to review the test decision to confirm that additional testing, beyond that which has been conducted, is not required.

Response to Recommendations

Recommendation 1: Ensure that a plan is developed for the Equal Employment Opportunity Complaint Tracking System.

Response: Agree. A plan has been developed for the Equal Employment Opportunity Complaint Tracking System. Although at the time of the audit, the Year 2000 P&R database showed the contingency plan for this system was deployed on September 27, 1999, the plan could not be located. A new plan has been developed for this system.

Recommendation 2: Integrate supporting contingency and continuity plans and other organizational initiatives.

Response: Agree in part. Business Continuity Plans (BCP's) were completed prior to the publication of Component Contingency Plans (CCP's). Because of this, the dependencies between BCP's, CCP's, Recovery Management and Disaster Recovery Plans were not as well integrated as they should have been to enable organizations responsible for implementing the plans to easily identify the referenced documents. The activity to better integrate the BCP's and CCP's to Recovery Management and Disaster Recovery Plans is in progress.

However, we would argue the feasibility and value of integrating other initiatives referenced in the report such as deployment, assignment of roles and responsibilities and change configuration management with CCP's and BCP's. The Year 2000 Program Plan was developed and is being actively monitored at the senior executive level with full consideration of the interdependencies of the 31 work segments.

The audit findings suggest that the successful implementation of CCP's and BCP's may be at risk because the assignment of roles and responsibilities are being addressed in the Recovery Management Plan under the responsibility of the field organizations. In contrast to the OIG's concerns, the Office of Management and Budget (OMB) reviewed our Recovery Management plan and commented as follows on the Postal Service's approach to having the cognizant Areas responsible for assigning appropriate personnel:

"Each Area is responsible for assigning appropriate personnel. Due to the size of the USPS, the level of the plan submitted *does not* and *should not* contain each employee who will be on duty or on call during the rollover period with their contact information." [Emphasis added]

While we agree that such things as the assignment of roles and responsibilities, deployment of correct software versions, and configuration management are important to the overall success of the program, we do not necessarily agree that these elements should be specifically addressed in the plans.

Recommendation 3: Further complete business contingency and continuity plans, beginning with those areas of greatest risk.

Response: Agree in part. We fully concur with the need to constantly update and improve the contingency and continuity plans, and appreciate the recognition that any effort we undertake, particularly on the eve of the Year 2000 rollover, must be prioritized by risk. It is important to note that the plans developed to address potential failures as a result of the Year 2000 rollover have long-term benefit to the Postal Service and will be used going forward to address failures due to other causes. As such, these plans will be reviewed and updated as necessary as a part of our on-going process.

As discussed in the Summary Comments section above, we agree that consideration of the 12 elements is important to successful plan implementation; however, we do not agree with the OIG's findings that elements missing in the plans increase the risk that the plans may not work as intended. We believe that all of the plan elements have been addressed and, where appropriate, have been included in either the plan or in collateral plans for further action by the field.

However, in view of the OIG findings, we have asked the business owners to conduct an additional review of the plans for which they are responsible and to further affirm their confidence that the plans are suitable and adequate for the purpose of protecting the Postal Service from external disruptions or internal component failures. Any plans found lacking by the business owner will be updated and republished.

Recommendation 4: Expand testing of contingency and continuity plans to the maximum extent possible. At a minimum, conduct walk-throughs for those plans that are incomplete.

Response: Disagree. While we agree in principle that testing is better than not testing, it is impractical to conduct walk-throughs for all plans. We believe that the process and criteria established to determine the level of testing required resulted in an appropriate level of testing. The testing performed to date, coupled with the dress rehearsal being conducted in late November, is more than adequate to ensure that the Postal Service is ready to effectively implement contingency and continuity plans, as required.

We do agree, however, that the justification presented in some of the plans may be inadequate for determining that no test is required. Therefore, each of the business owners has been asked to review these plans and either provide adequate justification or conduct tests, all within the parameters of the initial test decision criteria.

Recommendation 5: Require that the proposed quality assurance steps be taken to ensure that plans are adequately integrated with other supporting plans and organizational initiatives, and are properly tested.

Response: Agree. The quality assurance referred to in the OIG findings will be continued, as planned. Plans will be reviewed, tests concluded, dress rehearsals conducted and plans updated and republished, where required.

**Major Contributors to
This Report**

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]