United States General Accounting Office

GAO

Report to the Special Committee on the Year 2000 Technology Problem, U.S. Senate

October 1999

YEAR 2000 COMPUTING CHALLENGE

FBI Needs to Complete Business Continuity Plans

GAO/AIMD-00-11

Contents

Abbreviations

BOP	Bureau of Prisons
CIO	Chief Information Officer
FBI	Federal Bureau of Investigation
IT	information technology
JMD/CSS	Justice Management Division/Computer Services Staff
NCIC	National Crime Information Center
OMB	Office of Management and Budget
PMO	Program Management Office
SSA	Social Security Administration

B-282155

October 22, 1999

The Honorable Robert F. Bennett
Chairman
The Honorable Christopher J. Dodd
Vice Chairman
Special Committee on the Year 2000 Technology Problem
United States Senate

The Federal Bureau of Investigation (FBI) relies on automated information systems to fulfill its mission to investigate violations of federal criminal law, protect the United States from foreign intelligence and terrorist activities, and provide assistance to federal, state, and local agencies. To prevent disruptions to systems caused by the Year 2000 problem, the FBI has taken action to renovate and test its mission-critical systems. Nevertheless, because core business processes may still be disrupted by Year 2000-induced failures in internal systems, business partners' systems, or public infrastructure systems, it is necessary for the FBI to develop and test plans for the continuity of business operations. If done effectively, such plans can help mitigate the risks and mission impacts associated with unexpected internal and uncontrollable external system failures.

At your request, we determined (1) the status of and plans for completing the FBI's contingency planning for continuity of operations and (2) whether the FBI's contingency planning efforts satisfy the key processes in our Year 2000 business continuity and contingency planning guide.[1] This report summarizes the information presented at our August 19, 1999, briefing to your office and provides examples of important business continuity planning steps that the FBI is not fulfilling. This report also includes the briefing slides that we presented to your office because they contain our findings on how well the FBI is satisfying business continuity planning steps. The briefing slides are presented in appendix I, and our objectives, scope, and methodology in appendix II. We requested comments on a draft of this report from the Attorney General or her designee. The Department of Justice provided comments. These comments along with our evaluation are summarized in the "Agency Comments and

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

Our Evaluation" section of this report and are reprinted and addressed in detail in appendix III. We performed our work from March through August 1999 in accordance with generally accepted government auditing standards.

Results in Brief

As of August 1999, the FBI reported that it has renovated, tested, and certified as Year 2000 compliant all but 1of its 43 mission-critical systems and has developed system-level contingency plans for all but 2 of the 43. Also, the FBI has made some progress in its Year 2000 business continuity planning, but this very important effort is running late. To ensure that there will be sufficient time to develop, test, and finalize plans, we recommended[2] in earlier testimony that plans be developed by April 30, 1999, and tested, including addressing problems and retesting, if necessary, by September 30, 1999, in order to allow agencies sufficient time to evaluate whether the plans will provide the level of core business capability needed and whether the plans can be implemented within a specified time frame. However, the FBI had not yet developed division-level business continuity plans or field office plans, and it did not expect to complete the integration of the division plans until September 1999. Further, it had not yet established a target date for completing field office plans or testing both field-level and division-level plans. These delays left the FBI with little time to complete the many planning tasks that remain and ensure that it is ready to minimize the impact of possible Year 2000-induced system failures.

Moreover, the FBI also did not have many of the management controls and processes needed to effectively guide its continuity planning effort through the short time remaining before the Year 2000 deadline. For example, the FBI had not (1) developed a high-level business continuity planning strategy, (2) developed a master schedule and milestones, (3) defined all its core business processes, (4) implemented a complete risk management process for business continuity planning, (5) performed risk and impact analyses of each core business process, (6) assessed the costs and benefits of alternative continuity strategies, or (7) planned for the testing phase of its business continuity planning effort. According to the senior Year 2000 official, the FBI had not implemented these controls and processes because Justice's guidance focuses on system-level contingency plans and does not require business continuity planning. Further, the official stated

[2] *Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions* (GAO/T-AIMD-99-50, January 20,1999).

that the FBI is inherently capable of ensuring continuity of operations because its agents in both headquarters and the field are well trained and prepared for responding to various emergency circumstances, of which potential Year 2000 system failure is just one.

The need for a structured and defined approach to managing Year 2000 programs, including business continuity planning, is widely accepted by both public and private sector organizations, and it is precisely why our Year 2000 guidance has been adopted by the Office of Management and Budget (OMB) as a federal standard. By not employing the management rigor and discipline specified in our Year 2000 business continuity planning guide, the FBI will not be able to ensure that it (1) properly focuses its planning effort on the agency's most critical operations, (2) selects the best strategies to protect these operations, (3) has sufficient resources and staff dedicated to implementing continuity plans, and (4) can efficiently and effectively invoke its continuity plans, if necessary.

To strengthen the FBI's management of business continuity planning, we are recommending that Justice clarify its expectations for Year 2000 business continuity planning for all of its bureaus and that the FBI establish and implement (1) a plan for developing and testing business continuity plans and (2) effective controls and structures for managing Year 2000 business continuity planning. In commenting on a draft of this report, Justice disagreed with our conclusion that it has not required the development and emphasized the importance of business continuity planning. However, it also cited steps that it has recently taken to address our recommendations, including orally clarifying business continuity planning for some bureaus, developing a plan for the timely development and testing of headquarters and field office business continuity plans, and establishing controls and structures for managing business continuity planning. To fully implement all recommendations, Justice must build on these first steps to ensure that all bureaus complete business continuity plans, and that specifically cited plans and management controls for the FBI's business continuity planning are effectively implemented.

Background

The FBI's mission is to investigate violations of federal criminal law, protect the United States from foreign intelligence and terrorist activities, and provide leadership and law enforcement assistance to federal, state, local, and international agencies. The FBI supports its mission with 56 field offices, about 400 satellite offices, and 35 foreign legal attaches. In addition,

classified systems link two computer centers–Washington, D.C. and Clarksburg, West Virginia–and all FBI locations.

To carry out its mission, the FBI depends on information technology (IT) systems that contain information on fugitives, wanted persons, stolen vehicles, etc. and are used by both FBI staff and state and local law enforcement agencies. For example, the FBI has recently implemented its National Crime Information Center (NCIC) 2000 system, which is used by law enforcement agencies in the United States, Puerto Rico, Mexico, and Canada to share information about individuals, vehicles, and property associated with criminal activity.

The FBI has been working to address the Year 2000 problem with its critical IT systems. Under the leadership of a Year 2000 Senior Executive, the FBI identified 43 mission-critical IT systems and hundreds of non-IT assets, such as laboratory equipment and telephone and building systems, to be renovated and tested before the Year 2000. All but one of these systems have been renovated, tested, and certified as Year 2000 compliant. The FBI has also developed system-level contingency plans for all but 2 of its 43 mission-critical systems.

Despite the FBI's or any organization's best efforts to remediate its mission-critical systems; however, core business processes may still be disrupted by Year 2000-induced failures and errors in internal systems, business partners' systems, or public infrastructure systems, such as power, water, transportation, and telecommunications systems. Thus, it is necessary to prepare plans for continuity of business operations to help mitigate the risks and mission impacts associated with unexpected internal and uncontrollable external system failures.

Our Year 2000 business continuity and contingency planning guidance recommends that federal agencies follow a four-phased structured approach to continuity and contingency planning, which is illustrated below. OMB has adopted this guidance as a federal standard for business continuity planning.

- ***Phase 1–Initiation***. Establish a continuity work group and develop a high-level business continuity planning strategy. Develop a master schedule and milestones, and obtain executive support.
- ***Phase 2–Business impact analysis***. Assess the potential impact of mission-critical system failures on the agency's core business processes. Define Year 2000 failure scenarios, and perform risk and impact

analyses of each core business process. Assess infrastructure risks, and define the minimum acceptable levels of output for each core business process.
- ***Phase 3–Contingency planning***. Identify and document contingency plans and implementation modes. Define triggers for activating contingency plans, and establish business resumption teams for each core business process.
- ***Phase 4–Testing***. Validate the agency's business continuity strategy. Develop and document contingency test plans. Prepare and execute tests. Update disaster recovery plans and procedures.

FBI's Continuity of Operations Planning Efforts Are Late

To ensure that agencies have sufficient time to develop, test, and finalize their plans, contingency and continuity plans should have been completed by April 30, 1999, and tested by September 30, 1999. However, the FBI has been running behind our recommended schedule for business continuity planning, and its plans do not contain milestones for completing its remaining tasks. As of August 1999, the FBI

- had not yet developed an integrated set of division-level business continuity plans and did not expect this to be done until September 1999;
- had not yet established a milestone for the completion of field office business continuity plans or instructed field offices on what the content of their contingency plans should be; and
- had not yet established milestones for testing both field-level and division-level continuity plans.

These delays, in part, are attributable to the FBI's late start in undertaking its business continuity planning effort. The agency did not initiate business continuity planning until March 1999, did not instruct its field offices to develop continuity plans until April 1999, and did not instruct divisions to prepare continuity plans until May 1999. The Year 2000 Program Management Office (PMO), in its Contingency Planning Guidebook for Field Offices, stated that it will provide additional guidance to the field offices on business continuity planning, including instructions for the content of plans, in October 1999. According to FBI officials, the FBI started late in business continuity planning because Justice's guidance only requires system-level contingency plans and does not address business continuity planning. Our review of Justice's Year 2000 guidance confirmed this statement.

FBI Lacks Key Controls and Processes Needed to Complete Its Continuity Planning Effort

The delays in the FBI's development of business continuity plans have left the agency with little time to properly test its plans and to update plans based on the results of those tests. As a result, it is exceedingly important for the FBI to have an effective set of management controls in place for managing the remainder of its business continuity planning effort. Nevertheless, the FBI does not have many of the key processes and controls necessary to reduce the risk of Year 2000 business disruptions because, according to the FBI's senior Year 2000 official, Justice's guidance focuses on system-level contingency plans and does not require business continuity planning. Further, the official stated that continuity of operations is embedded in the FBI's normal daily operations, and its agents in both headquarters and the field are well trained and prepared for responding to various emergency circumstances, of which Year 2000 disruption is just one type.

However, the FBI does not have important management controls for effectively managing Year 2000 business continuity planning, controls which OMB has adopted as a federal standard and which public and private sector organizations are employing. Without these controls, the FBI has inadequate assurance that it will be able to effectively address potential internal and external Year 2000-induced system failures.

The following are examples of our recommended business continuity planning steps that, as of August 1999, the FBI had not fully satisfied.

- Develop a high-level strategy for business continuity planning. Our guidance recommends that agencies develop and document a high-level continuity planning strategy during the initiation phase to guide the planning effort. It should include project structure, metrics and reporting requirements, and cost and schedule estimates. Without a planning strategy, agencies cannot ensure that they have sufficient resources and staff dedicated to the contingency and continuity planning effort.
- Develop a master schedule and milestones. Our guidance recommends that agencies develop a master schedule, including milestones for the delivery of interim and final products. These tools help agencies track business continuity planning progress to ensure that important tasks are completed according to defined requirements, and timely corrective actions to address deviations from requirements are taken. While the PMO directed the divisions to develop continuity plans by mid-August and established early September as the milestone for integrating the

division plans, it had not yet established a milestone for the completion of field office business continuity plans or established milestones for testing both field-level and division-level continuity plans.

- Define all its core business processes. The business continuity planning process focuses on reducing the risk of Year 2000-induced business failures. Thus, it is essential for agencies to identify their core business processes and supporting mission-critical systems. Our guidance recommends that this be done during the initiation phase so that in the business impact phase agencies can examine business process composition, priorities, and dependencies and define the minimum acceptable level of outputs and services for each core process. In May 1999, the PMO tasked its headquarters divisions to identify their core business processes and supporting mission-critical systems. As of July 1999, only one of the five divisions we contacted had defined its core processes and supporting systems; the other four reported that they were in the process of doing so.
- Implement a complete risk management process for continuity planning. Our guidance recommends that agencies implement a risk management and reporting process during the initiation phase of the business continuity planning project that includes identifying business continuity project risks, developing measures for tracking planning progress and determining plans' quality, establishing reporting requirements, and assessing system renovation risks. The FBI had not identified project risks, developed measures, or established a reporting system for its business continuity planning project, although it had implemented a risk management process for its mission-critical systems.
- Perform risk and impact analyses for each core business process. To help develop adequate contingency procedures, our guidance recommends that agencies determine the impact of internal and external information system failures and infrastructure services on each core business process. The PMO has directed both headquarters divisions and field offices to assess the impact of internal and external system failures on core functions and to use these analyses in their business continuity planning. One of the five divisions and two of the three field offices we contacted reported that they had not yet begun their impact analyses, although they stated that they plan to do so.
- Assess the costs and benefits of alternative continuity strategies. To select the best contingency strategy for each core business process, our guidance recommends that agencies assess the costs and benefits of identified alternatives as a first step in the contingency planning phase.

The FBI had not assessed the cost and benefits of alternative strategies, and it has not instructed its divisions and field offices to do so.

- Plan for the testing phase of its business continuity planning effort. Agencies need to test their continuity plans to evaluate whether they are capable of providing the desired level of support to core business processes and whether the plans can be implemented within a specified period. To effectively prepare for such tests, our guidance recommends that agencies develop and document test plans and establish teams and acquire contingency resources. Our guidance also recommends that agencies rehearse business resumption teams to ensure that each team and team member is familiar with business resumption procedures and their roles. The FBI had yet to undertake these important planning tasks and, as discussed earlier, has yet to set milestones for completing its testing efforts.

Conclusions

The FBI reports good progress in making its mission-critical systems Year 2000 compliant and in developing system-level contingency plans. However, because Justice has not explicitly required and emphasized the importance of business continuity plans, the FBI started late in undertaking its business continuity planning effort, and it is now faced with a compressed time frame for testing and finalizing its plans. Unless the FBI moves swiftly to implement the management controls and processes it lacks, it is unlikely to have effective business continuity plans in place by the turn of the century, and it runs the serious risk of not being able to sustain the minimal levels of service needed to meet its mission if confronted with Year 2000 system failures.

Recommendations

We recommend that the Attorney General direct the Department of Justice's Year 2000 Program Office to clarify the department's expectations for Year 2000 business continuity planning for all Justice bureaus, emphasizing the need for these plans and discussing OMB's adoption of our guidance as a federal standard. We also recommend that the Attorney General direct the FBI Director to take the following actions:

- establish and implement a plan for the timely development and testing of effective headquarters and field office Year 2000 business continuity plans, including incremental milestones for completing all relevant key processes in our guide associated with business impact analysis, plan development, and plan testing, and

- establish and implement effective controls and structures for managing Year 2000 business continuity planning, including each of the relevant key processes addressed in our Year 2000 contingency planning guide and discussed in this report as not yet being satisfied.

Agency Comments and Our Evaluation

In written comments on a draft of this report, Justice disagreed with our conclusion that it has not required the development and emphasized the importance of business continuity plans. To support its position, Justice (1) cited Year 2000 guidance and information provided to its bureaus in early 1998, (2) noted that three of its eight bureaus currently have plans in place, and (3) stated that it provided OMB a departmentwide business continuity and contingency plan on June 15, 1999.

We do not agree with Justice's position for several reasons. First, guidance cited by Justice does not address business continuity planning per se. Justice's guidance transmitted our Year 2000 guide and a description of the Social Security Administration's (SSA) business continuity planning efforts, but did not direct the bureaus to develop and test business continuity plans. Second, as stated in its response to our report, only three of eight Justice bureaus have developed business continuity plans at this late date, which further supports our conclusion. Third, Justice's department-level plan is not relevant to our conclusion about bureau-level planning, direction and guidance. Moreover, in its comments Justice acknowledges that it has concentrated on system-level contingency plans as opposed to business continuity planning. To its credit, after receiving a draft of our report, Justice held a meeting with selected bureaus that was attended by us, in which it required and explained the importance of business continuity plans; however, Justice provided no evidence that all bureaus were subjected to this requirement.

Justice also stated that the FBI has developed a plan for the timely development and testing of headquarters and field office business continuity plans, and has established controls and structures for managing business continuity planning. We are encouraged by the FBI's first step in responding to our recommendations. To fully implement our recommendations, the FBI must effectively implement its plan, which requires, among other things, that it define reporting requirements and measures of interim progress and effectively act to address any deviations from expectations. Further, the FBI must establish and effectively implement all business continuity key processes, including effectively

monitoring their implementation so that any deviations are identified and corrective action is taken immediately.

Justice's written comments, along with our detailed response, are reprinted in appendix III.

We are sending copies of this report to the Honorable Jacob J. Lew, Director, Office of Management and Budget; the Honorable Janet Reno, Attorney General; the Honorable Louis J. Freeh, Director of the Federal Bureau of Investigation; and John Koskinen, Chairman of the President's Council on Year 2000 Conversion. Copies will be made available to others upon request.

If you have any questions, please contact me or Deborah Davis, Assistant Director, at (202) 512-6240 or by e-mail at *hiter.aimd@gao.gov* or *davisd.aimd@gao.gov*. Other major contributors to this work were Cristina Chaplain, Carl Higginbotham, and John Ortiz.

Randolph C. Hite
Associate Director, Governmentwide
and Defense Information Systems

Briefing to the Special Committee on the Year 2000 Technology Problem

GAO **Accounting and Information Management Division**

Briefing to Senate Special Committee on Year 2000 Technology Problem

FBI Year 2000 Business Continuity Planning

August 19, 1999

1

GAO Overview

- Objectives, Scope, and Methodology
- Results in Brief
- Background
- Detailed Results
- Conclusions and Recommendations

2

GAO Objectives, Scope, and Methodology

The Committee asked us to determine

- the status of and plans for completing the FBI's contingency planning for continuity of business operations, and
- whether the FBI's contingency planning efforts satisfy the key processes in GAO's contingency planning guide.*

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

3

GAO Objectives, Scope, and Methodology (cont'd)

GAO Business Continuity and Contingency Planning Guide

Initiation	• Establish continuity work group and develop high-level planning strategy and related guidance and procedures. (8 key processes)
Business Impact Analysis	• Assess risk and impact of system failures on core business processes and define minimum acceptable levels of output. (5 key processes)
Contingency Planning	• Develop contingency plans and implementation modes, assign resumption teams, and define implementation triggers. (5 key processes)
Testing	• Develop contingency test plans, execute tests, and validate business continuity strategy. (8 key processes)

4

GAO Objectives, Scope, and Methodology (cont'd)

- We reviewed completed and planned continuity of operations activities; discussed each such activity with FBI Year 2000 program office and contractor officials; obtained and reviewed documentation to corroborate officials' statements; and compared plans and progress to GAO-advocated milestones.

- We identified business continuity planning structures and controls (organization, standards, policies, guidance) in place and compared these to the key processes in GAO's business continuity and contingency planning guide.

5

GAO Objectives, Scope, and Methodology (cont'd)

- We discussed business continuity planning activities, structures, and controls with managers in five divisions (Criminal Investigative Division, Criminal Justice Information Services Division, Information Resources Division, Laboratory Division, and National Security Division) and three major field offices (New York, Los Angeles, and Washington).
- We performed our work from March 1999 through August 1999 in accordance with generally accepted government auditing standards.

6

GAO Results In Brief

- Objective 1: FBI has made some progress in its business continuity planning but its division-level efforts are four months behind the GAO-recommended milestone, it has not established milestones for developing field office business continuity plans, and it has not developed milestones for testing both division and field office business continuity plans.

- Objective 2: FBI has satisfied, partially satisfied, or plans to satisfy 16 of the 26 key processes in GAO's contingency planning guidance, but has not satisfied the remaining 10 key processes.

7

GAO Background

- The FBI's mission is to
  - investigate violations of federal criminal law;
  - protect the United States from foreign intelligence and terrorist activities;
  - provide leadership and law enforcement assistance to federal, state, local, and international agencies.

8

GAO Background (cont'd)

- To carry out its mission, the FBI depends on information technology (IT) systems that contain information on fugitives, wanted persons, stolen vehicles, etc. State and local law enforcement agencies also depend on these systems.
- Computer centers in Washington, DC and Clarksburg, WV support
  - 464 field offices & resident agencies, and
  - 35 foreign legal attaches.

9

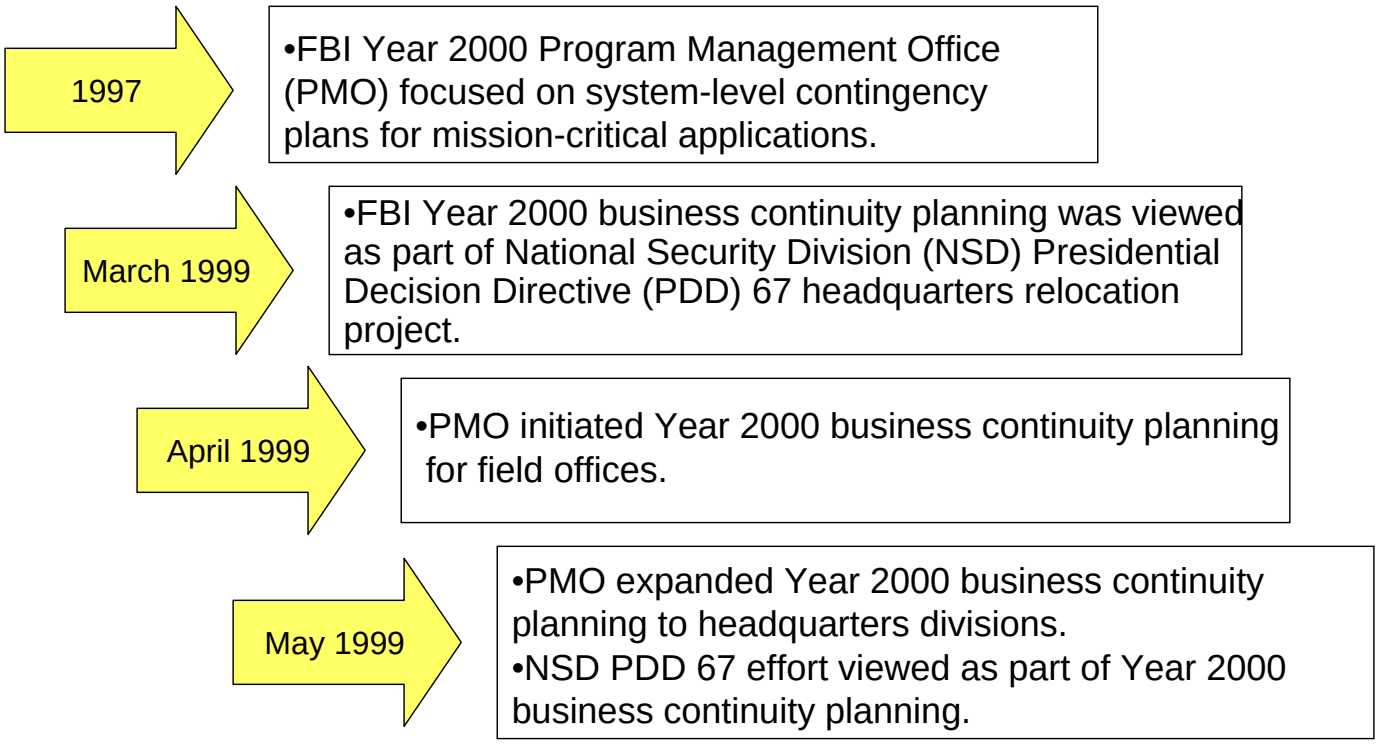
GAO Background (cont'd)

- All FBI locations are linked by classified networks.
- FBI has 43 mission-critical IT systems, and hundreds of mission-critical non-IT assets, including laboratory equipment and telephone and building systems.

10

GAO

FBI Scope and Approach to Business Continuity Planning Has Evolved



11

GAO

Objective 1: Planning Efforts Are Late And Key Milestones Are Missing

- FBI plans to develop division-level business continuity plans by early September 1999, four months past the April 30, 1999, date recommended by GAO.
- FBI has not established a date for developing field office business continuity plans.
- FBI has not developed a plan or established milestones for testing division-level and field-level business continuity plans.

12

GAO Objective 1: Planning Efforts Are Late And Key Milestones Are Missing

- In May 1999, PMO directed the divisions to
  - define core business processes,
  - determine the impact of internal and external failures, and
  - prepare contingency plans and procedures for each process by mid-June 1999
- PMO has revised the mid-June delivery date to mid-August.
- Four of the five divisions we contacted reported that they expect to meet the August deadline and one plans to develop its plan in September/October.

13

GAO Objective 1: Planning Efforts Are Late And Key Milestones Are Missing

- PMO provided guidance to the field offices in late April 1999 that directed them to:
  - identify potential failure scenarios,
  - conduct risk assessments and impact analyses,
  - review existing contingency plans and use them as a base for developing new plans, and
  - develop continuity of operations plans.
- Guidance to the field offices does not include milestones for completing development and testing of business continuity plans.
- PMO plans to provide guidance on the contingency plan content and zero day procedures in October 1999.
- All three field offices we contacted reported that they are currently developing their plans.

14

GAO Objective 1: Planning Efforts Are Late And Key Milestones Are Missing

- FBI reports contingency plans developed for 41 of 43 mission-critical IT systems. The last two plans will not be ready until September or October.
- FBI and DOJ contractors plan to perform independent verification and validation (IV&V) of all system-level plans. Of the 41 plans submitted for IV&V, 40 have been approved, and one is being revised.

15

GAO Objective 2: Many GAO Key Processes Not Satisfied

Phase	Number of Key Processes			
	Satisfied	*Partially Satisfied*	*Plans to Satisfy*	*Not Satisfied*
Initiation	2	3	2	1
Business Impact Analysis	1	2	2	0
Contingency Planning	0	3	1	1
Testing	0	0	0	8
Total	3	8	5	10

16

GAO Criteria For Satisfying Key Processes

- Satisfied - key process developed and implemented; documentation provided
- Partially satisfied - some components, but not all, of key processes developed and implemented; documentation provided
- Plans to satisfy - key process not yet developed or implemented, but guidance directs divisions or field offices to develop
- Not satisfied - key process not developed and not addressed in guidance

17

GAO Detailed Results: Initiation Phase

GAO Key Processes	*Results*
1. Establish business continuity work group	Satisfied
2. Develop high-level business continuity planning strategy	Not satisfied
3. Identify core business processes	Plans to satisfy
4. Define roles and assign responsibilities	Satisfied
5. Develop master schedule and milestones	Partially satisfied
6. Implement a risk management process and establish reporting system	Partially satisfied
7. Assess existing business continuity, contingency, and disaster recovery plans	Partially satisfied
8. Implement quality assurance reviews	Plans to satisfy

18

GAO Detailed Results: Initiation Phase Key Process 1

- A business continuity workgroup should be established that reports to executive management and includes representatives from major business units.
- FBI established a task force consisting of division representatives to share business continuity information among divisions and agree on responsibilities for contingency plans that require action by more than one division. The PMO reports the group's progress monthly to the FBI Deputy Director.
- Satisfied

19

GAO Detailed Results: Initiation Phase Key Process 2

- A high-level business continuity planning strategy should be developed and documented to guide the planning effort. It should include project structure, metrics and reporting requirements, and cost and schedule estimates.
- FBI has not documented a high-level strategy to guide its overall business continuity effort.
- Not Satisfied

20

GAO Detailed Results: Initiation Phase Key Process 3

- Core business processes and the supporting mission-critical systems should be defined for each business area.
- In May 1999, the PMO tasked headquarters divisions to identify their core business processes and supporting mission-critical systems. One of the divisions we contacted reported that it has defined its core processes and supporting mission-critical systems and the other four reported that they are in the process of doing so.
- Plans to satisfy

21

GAO Detailed Results: Initiation Phase Key Process 4

- Roles should be defined and responsibilities assigned for leading the planning effort, performing analyses, and designing business alternatives.
- The PMO assigned responsibilities and roles for performing impact analyses and developing contingency plans to division Assistant Directors and to field office Special Agents- and Assistant Directors-in-Charge.
- Satisfied

22

GAO Detailed Results: Initiation Phase Key Process 5

- A master schedule, including milestones for the delivery of interim and final products, should be established.
- PMO has not developed a master schedule. However, it directed headquarters divisions to develop continuity plans by mid-June 1999 originally, now by mid-August 1999, and has established early September as the milestone for integrating the divisions' plans.
- Partially satisfied

23

GAO Detailed Results: Initiation Phase Key Process 6

- Organizations should implement a risk management and reporting process for the business continuity planning project that includes identifying project risks, developing metrics, establishing reporting requirements, and assessing system renovation risk.

- PMO has not identified project risks, developed project metrics, or established a reporting system for its business continuity planning project; but it has implemented a risk management process for its mission-critical system renovation effort.

- Partially satisfied

24

GAO Detailed Results: Initiation Phase Key Process 7

- Organizations should assess existing business continuity, contingency, and disaster recovery plans for their applicability in addressing the Year 2000 problem.

- PMO directed field offices, but not the divisions, to review existing contingency plans as part of their business continuity planning effort. Two of the five divisions and all three field offices we contacted reported that they have assessed their existing plans.

- Partially satisfied

25

GAO Detailed Results: Initiation Phase Key Process 8

- Quality assurance reviews should be conducted to verify that the continuity of operations plans satisfy information requirements.
- The PMO plans for its contractor to review some division-level plans and is considering expanding their review to field office plans.
- Plans to satisfy

26

GAO Detailed Results: Business Impact Analysis Phase

GAO Key Processes	*Results*
1. Define and document information requirements, methods, and techniques	Partially satisfied
2. Define and document Year 2000 failure scenarios	Satisfied
3. Perform risk analysis of each core business process	Plans to Satisfy
4. Assess and document infrastructure risks	Partially satisfied
5. Define the minimum acceptable level of outputs and services for each core business process	Plans to satisfy

27

GAO Detailed Results: Business Impact Analysis Phase Key Process 1

- Organizations need to define detailed information requirements, techniques, and methods for constructing a business continuity plan.
- PMO has provided some information requirements to the divisions and field offices, including personnel, special equipment, system access, status of facilities' assets/systems, electricity, and telecommunications. However, the PMO has not provided the field offices or headquarters divisions any information on methods or techniques for developing contingency plans.
- Partially satisfied

28

GAO Detailed Results: Business Impact Analysis Phase Key Process 2

- Organizations need to define and document Year 2000 failure scenarios, including the loss of all mission-critical information systems, the possibility that problems may be encountered earlier than expected, and the potential disruption of infrastructure services.

- PMO defined failure scenarios for headquarters divisions and has also directed field offices to identify potential disruptions to internal systems and the public infrastructure, including electric power and transportation. Two of the three field offices we contacted reported they have either defined or are currently defining the potential disruptions.

- Satisfied

29

GAO Detailed Results: Business Impact Analysis Phase Key Process 3

- Organizations should monitor Year 2000 progress and determine the risk and impact of internal and external system failures on each core business process.
- The PMO directed both headquarters divisions and field offices to assess the impact of internal and external system failures on core functions and to use these analyses in their business continuity planning, but directed only the field offices to perform a risk assessment of internal and external system failures. Four of the five divisions and one of the three field offices we contacted reported that they have begun their impact analyses and the others plan to conduct them.
- Plans to satisfy

30

GAO Detailed Results: Business Impact Analysis Phase Key Process 4

- Organizations should monitor the Year 2000 readiness of the public infrastructure, assess the risk of service outages, and determine if emergency services may be available to mitigate outages.
- PMO provided Year 2000 compliance information for public infrastructure services, including electric power and telecommunications, to field offices to use in conducting their business impact analyses.
- Three of the five divisions we contacted are conducting their own assessments.
- Partially satisfied

31

GAO Detailed Results: Business Impact Analysis Phase Key Process 5

- To facilitate the selection of adequate contingencies, organizations need to define the minimum acceptable level of outputs and services for each core business process.
- According to the FBI senior year 2000 executive, the FBI has long-established and well-understood rules governing emergency operations and priorities. The executive plans for these rules to govern how the FBI deals with Year 2000 contingencies.
- Plans to satisfy

32

GAO Detailed Results: Contingency Planning Phase

GAO Key Processes	*Results*
1. Assess the cost and benefits of identified alternatives and select the best contingency strategy for each core business process	Not satisfied
2. Identify and document contingency plans and implementation modes	Plans to satisfy
3. Define and document triggers for activating plans	Partially satisfied
4. Establish a business resumption team for each core business process	Partially satisfied
5. Develop and document “zero day” strategy and procedures	Partially satisfied

33

GAO Detailed Results: Contingency Planning Phase Key Process 1

- Organizations need to assess the cost and benefits of identified alternatives and select the best contingency strategy for each core business process.
- FBI has not assessed the costs and benefits of alternative strategies and has not instructed the headquarters divisions or field offices to do so. One of the five divisions reported that it has developed a cost estimate for its preferred alternative but was not able to obtain funding for the alternative. All three field offices reported that they have not developed cost estimates.
- Not satisfied

34

GAO Detailed Results: Contingency Planning Phase Key Process 2

- Organizations need to identify and document contingency plans.
- PMO has instructed both the headquarters divisions and field offices to prepare contingency plans, and the five divisions and three field offices that we talked to reported that they are currently preparing their plans.
- Plans to satisfy

35

GAO Detailed Results: Contingency Planning Phase Key Process 3

- Organizations need to define and document triggers for activating contingency plans for each core business process.
- The PMO instructed the headquarters divisions to use the defined failure scenarios as triggers but has not instructed the field offices to use or develop triggers. Four of the five divisions and one of the three field offices we contacted reported they are developing triggers for their plans.
- Partially satisfied

36

GAO Detailed Results: Contingency Planning Phase Key Process 4

- Organizations need to designate responsible individuals to ensure that the plans are executed if necessary.
- PMO has instructed the divisions to identify and notify such individuals of their responsibilities. The PMO did not instruct the field offices to identify these individuals. All five divisions and one of the three field offices we contacted reported they have begun identifying the responsible individuals.
- Partially satisfied

37

GAO Detailed Results: Contingency Planning Phase Key Process 5

- Organizations should develop a risk reduction strategy and procedures for the period between December 30 1999, and January 3, 2000.
- FBI has not yet developed strategies, but the PMO has directed field offices and headquarters divisions to develop procedures for the weekend of December 31, 1999 to January 2, 2000. Three of the five divisions and one of the three field offices we contacted reported they have begun preparing such procedures for the weekend.
- Partially satisfied

38

GAO Detailed Results: Testing Phase

GAO Key Processes	*Results*
1. Validate business continuity strategy	Not satisfied
2. Develop and document contingency test plans	Not satisfied
3. Establish test teams and acquire contingency resources	Not satisfied
4. Prepare for and execute tests	Not satisfied
5. Validate the capability of contingency plans	Not satisfied
6. Rehearse business resumption teams	Not satisfied
7. Update the business continuity plan based upon lessons learned and re-test if necessary	Not satisfied
8. Update disaster recovery plans and procedures	Not satisfied

39

GAO Conclusion

- FBI reports good progress in making its mission-critical systems Year 2000 compliant and in developing system-level contingency plans. However, because the Justice Department has not required and emphasized the importance of business continuity plans, the FBI is late in undertaking its business continuity planning effort, and is now faced with a compressed timeframe for testing and finalizing its plans. Unless the FBI moves swiftly to implement management controls and processes it lacks, it is unlikely to have effective business continuity plans in place by the turn of the century and it runs the serious risk of not being able to sustain the minimal levels of service needed to meet its mission if confronted with Year 2000 system failures.

40

GAO Recommendations

- The Attorney General should direct the Justice Department's Year 2000 Office to:
  - clarify the Department's expectations for Year 2000 business continuity planning for all Justice component agencies and to ensure this clarification emphasizes the need for these plans and discusses OMB's adoption of our guidance as a federal standard.

41

GAO Recommendations (cont'd)

- The Attorney General should direct the FBI Director to take the following actions:
  - establish and implement a plan for the timely development and testing of effective headquarters and field Year 2000 business continuity plans, including incremental milestones for completing all relevant key processes in GAO's guides associated with business impact analysis, plan development, and plan testing, and

42

GAO Recommendations (cont'd)

- establish and implement effective controls and structures for managing Year 2000 business continuity planning, including each of the relevant key processes in GAO's Year 2000 contingency planning guide discussed in this briefing as not being satisfied.

43

Objectives, Scope, and Methodology

Our objectives were to determine (1) the status of and plans for completing the FBI's contingency planning for continuity of operations and (2) whether the FBI's contingency planning efforts satisfy the key processes described in our business continuity and contingency planning guide.[1]

To accomplish our first objective, we reviewed the FBI's progress towards developing and testing business continuity plans and compared it to our recommended milestones.[2] Also, we reviewed supporting documentation to evaluate the status and progress of the FBI's efforts against milestones. Specifically, we reviewed the FBI's business continuity guidance provided to headquarters divisions and field offices, business continuity task force meeting minutes, IT and non-IT status reports, and system-level contingency planning documents. In addition, we reviewed Justice's Year 2000-related guidance, including its roles, responsibilities and guidance document, dated January 23, 1999; and its guidelines for testing contingency plans, dated March 1999.

We accomplished our second objective by identifying the FBI's Year 2000 program management controls and comparing these to controls (i.e., key processes) described in our business continuity and contingency planning guide. In addition, we reviewed supporting documentation to verify that the management controls were functioning as intended and, using specified criteria,[3] determined whether each of the key processes was satisfied. To do this verification, we reviewed documents describing the FBI's business continuity planning activities, business continuity task force meeting minutes, contractors' statements of work, organization charts, and business continuity planning guidance provided to the headquarters divisions and field offices by the Year 2000 Program Office.

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

[2] *Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions* (GAO/T-AIMD-99-50, January 20, 1999).

[3] "Satisfied" means that the key process was developed and implemented, and documentation was provided. "Partially satisfied" means that some, but not all, components of the key process were developed and implemented, and documentation was provided. "Plans to satisfy" means that the key process was not yet developed or implemented but guidance directs the divisions to develop it. "Not satisfied" means that the key process was not developed and not addressed in guidance to the divisions.

To supplement our analysis of documentation, we interviewed key Year 2000 program officials, such as the Year 2000 Program Manager, support contractor representatives, and headquarters' division and field office representatives[4] responsible for developing business continuity plans. We selected these offices because the divisions were responsible for developing continuity plans for the FBI's core business processes and the field offices were three of the largest field units. The Year 2000 Program Office agreed with our selections.

We performed our work at FBI headquarters in Washington, D.C. We performed our work from March through August 1999 in accordance with generally accepted government auditing standards.

[4]Criminal Investigative Division, Criminal Justice Information Services Division, Information Resources Division, Laboratory Division, National Security Division and the Los Angeles, New York, and Washington, D.C., field offices.

Comments From the Department of Justice

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

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535

September 21, 1999

Randolph C. Hite
Associate Director
Governmentwide and Defense Information Systems
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Hite:

This letter serves as the Department of Justice's (DOJ) response to GAO's draft report entitled "Year 2000 Computing Challenge: FBI Needs to Complete Business Continuity Plans." DOJ has asked the FBI to send the response. The FBI and DOJ both appreciate the opportunity to review the draft report.

In the draft, GAO recommends that the Attorney General direct DOJ's Year 2000 Program Office to clarify the Department's expectations for Year 2000 business continuity planning for all Justice component agencies, emphasizing the need for these plans and discussing OMB's adoption of GAO's guidance as a federal standard.

See comment 1.

On January 23, 1998, the Assistant Attorney General for Administration (AAG/A) issued to Department Heads Year 2000 (Y2K) Guidance which provided a succinct overview of the Department's Y2K Program. The document contains a description of the roles and responsibilities of the Y2K Program Manager and departmental components, OMB reporting guidelines, contingency plan guidelines, and test plan guidelines. Soon thereafter, beginning in February 1998, the Department's Y2K Program Office provided information on Business Continuity and Contingency Plans (BCCPs) to components, including the FBI. Passages in GAO's draft, including the conclusion, which suggest that the Department did not place adequate emphasis on the BCCPs should be changed to note that the Department did, in fact, provide guidance to components in a timely and effective manner.

See comment 2.

In a March 31, 1999, memorandum (copy being sent under separate cover) to component heads, the AAG/A issued Y2K-related guidance to test contingency plans. The exercises are to involve stakeholders and are expected to relate to each organization's core business processes. Each component reported the method of

contingency plan testing and the test schedule for each mission critical system. Testing was to begin by July 1, 1999, with reporting of the test results by October 1, 1999.

See comment 3.

As reported in quarterly submissions to the OMB, the Department has concentrated on system-level contingency plans as opposed to continuity of business plans. Nonetheless, the Department developed a department level BCCP in conjunction with departmental components as requested in a May 13, 1999, memorandum from Jacob Lew, Director, OMB. This BCCP was provided to OMB on June 15, 1999.

See comment 4.

Of the eight DOJ components (Bureau of Prisons (BOP) Drug Enforcement Administration (DEA); Executive Office for United States Attorneys (EOUSA); Executive Office for United States Trustees (EOUST); Federal Bureau of Investigation (FBI); Immigration and Naturalization Service (INS); Justice Management Division (JMD)/Computer Services Staff (CSS); United States Marshals Service(USMS)) requiring plans, three have plans currently in place. They are BOP, DEA, and JMD/CSS.

See comment 5.

The BOP has always had contingency plans in place throughout its institutions to ensure that its overall mission is not interrupted by possible internal and external threats. These plans have been reviewed, factoring internal and external Y2K issues into the framework, to ensure the BOP mission makes a smooth Y2K transition. The BOP plans were favorably reviewed by the GAO. The DEA has developed plans for completing contingency planning for continuity of business operations and has established effective management controls. DEA is working to resolve remaining issues as identified by GAO.

See comment 6.

The JMD/CSS has developed a Business Continuity and Contingency Plan (BCCP) which describes the CSS core business processes and ensures the continuity of these activities by identifying, assessing, managing, and mitigating Y2K risks. It identifies mitigation strategies, alternate resources and processes needed to operate the business in the event of a Y2K induced failure, and to facilitate the return to normal service as quickly as possible in a cost-effective manner. This plan was prepared using the August 1998 GAO BCCP document which provided the conceptual framework and guidance. It should be understood that this plan is not intended to replace the existing CSS disaster recovery plan for resuming business operations due to traditional disasters such as fires, floods, and other natural disasters. This plan draws upon the same structure, business resumption teams, processes, and procedures already in place in the CSS disaster recovery plan. It specifically focuses on

specifically addressing the Y2K induced failures. Most Y2K problems, particularly those related to commercial off-the-shelf (COTS) hardware and software, can not be resolved by merely executing the normal disaster recovery plan since the same hardware and software will be operating at the backup site. Realizing that the BCCP is a "living" document, revisions will be necessary to reflect any changes in strategies, resources, processes, hardware/software implementations, or customer requirements.

See comment 7.

INS, USMS, EOUSA and the EOUST were recently requested by the AAG/A (copies of these letters are being sent under separate cover) to immediately develop and test a BCCP using GAO guidelines. Deborah A. Davis, Assistant Director, Accounting and Information Management Division, GAO, provided outstanding assistance to the Department by conducting a briefing on the GAO guidelines, discussing component-specific issues and providing invaluable insight into developing a BCCP. INS, USMS, EOUSA and EOUST have initiated their BCCP with preliminary activities and development of high level milestones.

See comment 8.

The Department has noted that the FBI has successfully implemented many aspects of its BCCP, including the April 15, 1999, Y2K Guide Book for Field Offices. More specifically, however, in response to the recommendation that the FBI establish and implement a plan for the timely development and testing of effective headquarters and field office Year 2000 business continuity plans, including incremental milestones for completing all relevant key processes in GAO's guide associated with business impact analysis, plan development, and plan testing, the FBI disseminated communications (copies of which are being provided under separate cover) to headquarters and all FBI field offices on September 13 and 14, 1999. These communications provide detailed information and guidelines to aid field offices and headquarters in fulfilling Y2K readiness requirements.

See comment 9.

Pursuant to GAO's second recommendation to the FBI, the Bureau has taken action to establish controls and structures for managing Year 2000 business continuity planning, including each of the relevant key processes in GAO's Year 2000 contingency planning guide which was identified in the draft report as not being satisfied. The taskings set forth in the two aforementioned communications will be tracked by the Y2K Program Management Office (PMO) at the FBI in order to ensure timely and effective completion. In addition, a checklist (also being provided under separate cover) will be used to monitor interim progress on a weekly basis to ensure that timely corrective actions are taken.

If you have any questions regarding this response, please contact me on (202) 324-4510.

Sincerely,

A. Robert Walsh
Legislative Counsel
Office of Public and
Congressional Affairs

The following is our detailed response to the Department of Justice's comments, dated September 21, 1999, on a draft of this report.

GAO Response

1. We do not agree with Justice's statement that its guidance and information adequately emphasizes the importance of business continuity planning, and therefore have not modified our position in the report that the department has not required and emphasized the importance of business continuity plans. As we stated in our report, Justice's Year 2000 guidance, dated January 23, 1999, only requires that its bureaus develop system-level contingency plans and does not address business continuity planning. In addition, Justice's Year 2000 Program Manager told us that Justice's Year 2000 guidance does not instruct its bureaus to prepare business continuity plans, and in fact Justice, in its comments on our draft report, states that the Department has concentrated on system-level contingency plans as opposed to business continuity plans.

Regarding the comment that beginning in February 1998, the department's Year 2000 Program Office provided information on business continuity and contingency plans to its components, including the FBI, Justice did not provide evidence with its comments to support this statement. We subsequently asked for support and were advised that the Year 2000 Program Manager provided our Year 2000 business continuity and contingency planning guide to Justice's designated senior officials for Year 2000 and members of Justice's Year 2000 working group. Justice's Year 2000 Program Manager also provided the Year 2000 working members with a copy of SSA's business continuity and contingency plan, as well as meeting minutes from the April and May Chief Information Officer (CIO) Council Committee working group on the Year 2000, where SSA's business continuity plan was discussed. However, Justice provided no evidence that it established expectations for its bureaus with respect to business continuity planning, and Justice's Year 2000 Program Manager told us that communications with the bureaus never included a requirement to develop and test business continuity plans.

2. Justice issued Year 2000-related guidance to its bureaus on testing contingency plans, but the guidance only addresses the testing of system-level contingency plans, not business continuity plans. In fact, in his March 31, 1999, memorandum, the Assistant Attorney General for Administration makes this point clear when he states that contingency plans have been completed for most of the Department's mission-critical systems and that the next step is the testing of these plans.

3. We have not reviewed the Justice referenced department-level business continuity and contingency plan because this plan was not relevant to the scope of our review. As a result, we cannot comment on this plan beyond noting that many of the essential elements of such a plan, e.g., core business processes, risk and impact analyses, and contingency strategies, had not been completed by all the bureaus at the time Justice submitted the plan to OMB (June 15, 1999). For example, as of August 1999, the FBI had not yet (1) identified its core business processes, (2) completed risk and impact analyses at its headquarters and field offices, and (3) developed contingency strategies. Only since receiving our draft report for comment has Justice requested that four of its bureaus, including the Immigration and Naturalization Service and the U.S. Marshals Service, develop and test business continuity and contingency plans, and thus far these four have only initiated preliminary development activities.

4. We cannot comment on the number of Justice bureaus that do or do not have business continuity plans because we have not reviewed each of the bureaus' continuity planning efforts. However, the fact that Justice acknowledges in its comments that only three of its eight components have developed business continuity plans further demonstrates our point that Justice has not established clear expectations for Year 2000 business continuity planning.

5. We do not agree that we have favorably reviewed the Bureau of Prisons' (BOP) business continuity plans. As of January 1999, when we completed our review of BOP's Year 2000 program management, BOP had not yet completed business continuity plans, and had not yet completed its review and testing of emergency preparedness plans. As we stated in our report, *Year 2000 Computing Crisis: Status of Bureau of Prisons' Year 2000 Effort* (GAO/AIMD-99-23, January 27, 1999), BOP's Year 2000 Program Manager had at that time directed all offices, including BOP contract facilities and institutions, to (1) review and analyze emergency preparedness plans for consideration of the threat of external infrastructure and internal system failures, (2) revise those plans as necessary by March 1, 1999, and (3) test the revised plans prior to April 5, 1999. As a result, we concluded that BOP had established plans for completing important business continuity planning efforts but that BOP still needed to effectively implement its plans to minimize its Year 2000 risks.

6. We have not reviewed Justice Management Division/Computer Services Staff's (JMD/CSS) business continuity plan because it was not relevant to the scope of our review. Therefore, we cannot comment on JMD/CSS' plan.

7. Requiring selected bureaus to develop and test continuity of business plans is the first step in responding to our recommendation. We are committed to providing Justice further assistance, if requested, in explaining our Year 2000 business continuity planning guide. To fully respond to our recommendation, Justice must clarify its expectations for all of its bureaus and explicitly require all of them to effectively develop and test continuity of business plans. In addition, Justice's Year 2000 Program Office must monitor each bureau's business continuity planning efforts and ensure that they are completed in accordance with expectations.

8. Establishing and implementing a plan for timely development and testing of effective headquarters and field office Year 2000 business continuity plans is a first step in responding to our recommendation. The FBI must ensure that its plan is effectively implemented, which among other things, will require it to define reporting requirements and measures of interim progress, and effectively act to address any deviations from expectations.

9. Establishing and implementing effective controls and structures for managing Year 2000 business continuity planning are first steps in responding to our recommendation. In particular, the FBI (1) developed a master schedule for developing and testing contingency plans, (2) tasked its headquarters and field offices to define and describe the minimum acceptable level of business operations, complete contingency plans by the end of October 1999, and develop and execute test plans by November 1999, and (3) provided guidance to its headquarters and field offices for developing contingency plans. However, it did not provide any evidence that it has (1) established a risk management process, (2) initiated quality assurance reviews, and (3) planned for updating business continuity plans based upon test results and retesting the plan, if necessary. Moreover, given that the FBI has many important tasks to complete with very little time, it is important that FBI's leadership monitor its implementation of these controls and structures to ensure that any deviations are identified and corrective action taken immediately.

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.

Orders 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 touchtone 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 an 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

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

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. GI00