FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: October 21, 1999

REPLY TO
 ATTN OF: Inspector General

SUBJECT: Business Continuity and Contingency Planning

TO: Chairman

On August 16, 1999, the Office of Inspector General (OIG) issued the "Audit of the FCC Year 2000 Program." In my cover transmittal to that report, I advised you that the OIG would continue to monitor and support the internal efforts being undertaken by the Commission to address the potential Year 2000 problem. This Special Report focuses upon our findings to date in the critical area of Business Continuity and Contingency Planning (BCCP). In the attached report we note that the Commission does not have documented assurance that in the event of a disruption to the Commission's infrastructure many mission critical functions could perform in an unimpeded manner.

Overall, the Commission's BCCP program was initiated in a late manner and has experienced significant delays since inception. The Chief Information Officer (CIO) attributed this condition to delays in obtaining requisite funding and competing priorities such as thc move of the Commission to the Portals facility. This consolidation .of Commission personnel and related workstations and servers placed a heavy burden on network personnel.

The majority of plans for operational continuity in the case of a disruption for identified mission critical systems have not been tested for the Year 2000 event. The OIG recommends that the Commission work aggressively in the limited time frame available to focus upon the most critical systems by subjecting them to simulation testing.

We are continuing to perform additional work in this and other areas relating to internal preparations for the year 2000 event. I will continue to provide you with pertinent information generated by this office.

Sincerely,

H. Walker Feaster, III
Inspector General

Attachment

cc: Commissioner Powell
    Chief of Staff
    Managing Director

Special Review Report of the Commission's Draft Business Continuity and Contingency Plan (BCCP)

EXECUTIVE SUMMARY

This special review report reflects the results of work performed by the Office of Inspector General (OIG), as of October 19, 1999, related to our analysis of the status of the Federal Communications Commission (FCC) Business Continuity and Contingency Plan (BCCP). A BCCP is a formal plan outlining the specific steps to be instituted in the event of a System failure. Office of Management and Budget (OMB) Circular A-130 issued February 1996 directs each Federal agency to "establish and periodically test the capability to perform the agency function supported by the application in the event of failure." The need for the FCC to have a BCCP for all mission critical systems is amplified in light of potential disruptions, which may be experienced in connection with the Year 2000 (Y2K) event. OIG auditors have identified that the FCC does not have a sufficiently detailed and tested BCCP in place to prepare for an outage of one or more mission critical systems (excluding Auctions systems). With approximately eighty (80) days remaining until the Year 2000, the Commission does not have sufficient time to fully address this situation. Thus, the OIG recommends that the Commission focus its attention upon performing detailed BCCP tests only for those highest in its ranking order.

BACKGROUND

On August 16, 1999, the OIG issued the "Audit of the FCC Year 2000 Program." This report identified a number of deficiencies in the FCC's preparations for the Year 2000 event. One area of concern was the lack of a BCCP for twenty-nine (29) of thirty (30) mission critical systems. Only the spectrum auction system was identified as having a BCCP. All other mission critical systems, such as the Universal Licensing System (ULS), did not have a documented and tested BCCP. A complete listing of these Systems is provided as Appendix 1 to this report. Thus, in the event of tire, electrical failure, or other disruption, the Commission lacks assurance that operations in these functional areas could proceed. The aforementioned condition exists in contrast to the requirements contained in OMB Circular A-130.

The FCC did establish, on April 6, 1999, a Business Continuity Task Force (BCTF) composed of representatives from the Office of the Managing Director (OMD), the Information Technology Center (ITC), and the Commission's Bureaus and Offices. This task force was charged with advising and tracking the progress of the development of a BCCP. On June 23,1999, the task force issued the "Year 2000 Business Continuity and Contingency Plan (BCCP)." This plan contained information on the following:
- Business Continuity Strategy
- Roles and Responsibilities
- Identification of Core Business Areas
- Contingency Plan Testing

This document met the core requirements contained in OMB Memorandum, <u>Business</u>

Continuity and Contingency Planning for the Year 2000, May 13, 1999. What this document did not address was the BCCPs for Bureau/Office mission critical systems. Thus, if a mission critical system such as ULS were to fail on January 1,2000, there is no documented process in place to continue program operations.

The Commission's BCCP identified the core Commission business areas and supporting critical infrastructure, with the associated threats to their continued functioning. The BCCP then developed a business impact analysis for each threat and ranked them as to severity. To address and mitigate the risks from these threats, the BBCP required the Bureaus and Offices to develop and test local contingency plans, which included the mission critical systems.[1] The deadline for completing the development of local plans was August 15, 1999.

Thirteen of the fourteen Bureaus and Offices required to develop a BCCP met the initial August 15, 1999, deadline. But, according to the Chief Information Officer (CIO), most of the plans submitted by the original deadline required additional work. One Bureau, the International Bureau (IB), completed its BCCP after one revision. The remaining thirteen BCCPs needed at least three drafts. This process required the Year 2000 Program Manager to schedule meetings to review the plans in detail, agree on plan changes, and establish new target dates for completion. The revision process was time consuming and required a modification of the completion dates for local plans. The new target date for completion of the final drafts was October 1, 1999, over one month later.

Only the IB completed its BCCP by the October 1, 1999, milestone. The Managing Director then set new target dates for reviews of the final drafts of the remaining local plans. Some reviews were scheduled as late as October 14, 1999. These delays put the development of local BCCP plans two months behind its original August 1, 1999, milestone date, with less than three months left.

After plan development, the next step is to test the plans. There are two types of BCCP tests: desktop and simulation testing. A desktop test requires the Bureau/Office manager responsible for contingency testing to develop a solution to a Year 2000 outage "on paper." The participants in a desktop test do not mimic an actual disaster.

The other test scenario, simulation testing, requires that the testers declare a mock disaster. For example, the Bureau/Office declares a Year 2000 "emergency" and conducts actual business as if the computer applications were not available. Simulation tests require a high level of planning and coordination. The agency wide BCCP does not specifically state which test scenario will be used. Simulation tests require much more coordination and planning than do desktop tests.

The Commission must test its BCCPs to determine if they will provide an acceptable level of service for core Commission business areas. The ITC had established a deadline of October 15, 1999 for completion of testing of the Commission's BCCP, including the

---

[1] The FCC Year 2000 BCCP document tasked Bureaus and Offices with developing local BCCPs, including mission critical systems. This document shifted the emphasis of BCCP development from OMB mission critical systems focus to the more encompassing Bureau/Office view.

Bureau and Office plans for supporting core business areas. With plan reviews scheduled for October 14, 1999, the Commission did not meet this milestone.

FINDING

The FCC does not have a sufficiently detailed and tested BCCP in place to prepare for an outage of one or more mission critical systems (with the exception of Auctions). As of October 6, 1999, the Commission has not completed thirteen of its fourteen local BCCPs for its Bureaus and Offices. No documented plan has been tested. With less than three months until January I, 2000, the Commission does not have sufficient time to fully address this problem.

The agency level BCCP established August 15, 1999, as the original target date for the completion oflocal plans. According to the CIO, most of the plans submitted by that original deadline required additional work. Therefore, the Year 2000 Program Manager had to schedule meetings to review the plans in detail, agree on plan changes, and establish new target dates for completion. The CIO took these steps to insure that Bureaus and Offices will have thorough and realistic contingency plans. As of October 6, 1999, only them had completed its local plan. The Managing Director then set revised target dates for reviews of the final drafts of the remaining local plans. Some were scheduled as late as October 14, 1999. The original testing milestone was October 15, 1999. Because of these delays, the Commission did not meet this milestone. The BCCP program is also two months behind its original milestone dates, with less than three months left until January 1, 2000. Accordingly, should an outage occur to one or more mission critical systems due to the Y2K phenomenon or some other adverse event, the Chairman cannot be provided assurance that the Commission has the capability to continue business operations in effected mission critical program areas.

OMB Circular A-130, Appendix 111, issued in February 1996, directs each agency to "establish and periodically test the capability to perform the agency function supported by the application in the event of failure" by developing contingency plans. The General Accounting Office *(GAO)* has recommended that agencies complete Year 2000 BCCPs by April 30, 1999[2] and complete testing by September 30, 1999.[3] FCC Commissioner Michael Powell, in a November 15, 1998 speech before the Year 2000 Contingency Planning for Government Conference, stated that Year 2000 contingency plans are "one of the first things you develop." Further, Mr. Powell stated "the time is now for working on contingency plans.[4] "

Management attributed the late start of the BCCP program to two factors: delays in obtaining funding and competing priorities. The Year 2000 remediation project was not adequately funded until December, 1998, according to the Year 2000 Program Manager.

---

[2] Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999), p. 14.
[3] Ibid., page 12.
[4] Michael K. Powell, "Year 2000 Problem and the Communications Industry" (Speech delivered at the Year 2000 Contingency Planning Conference, November 16, 1998), p. 4.

Competing priorities, such as the Commission's move to the Portals facility, also slowed the Year 2000 project. This consolidation of Commission Personnel and related workstations and servers placed a heavy burden on ITC personnel. The Commission, therefore, had little time available to contend with project delays, such as occurred during the. development of local plans.

The OIG finding was discussed with the CIO and the Year 2000 Program Manager. The Year 2000 Program Manager stated that though the local BCCP project is behind schedule, there is still adequate time for the completion of local BCCPs and to permit testing to the extent needed. The FCC's methodology has been to require thorough and realistic plans before acceptance rather than to accept initial plans and then to perfect them over time. If the FCC had settled for a lesser quality initial product, the FCC could have met the schedule and, possibly, could have avoided some criticism. However, the approach was to require achieving high quality before acceptance.

In addition, the FCC thinks that the testing of plans is important. However, all Bureaus and Offices have within the last six months been required to carry out manual operations for sufficient lengths of time that both management and frontline staff are knowledgeable and prepared for the possible loss of partial or full automated support.

RECOMMENDATION

The Commission should continue to aggressively work to institute and test BCCP's for all mission critical systems. If timing is insufficient to fully simulation test all systems, only those systems of the highest criticality and risk should be simulation tested. All systems should, at a minimum, be subject to an independent desktop test. A desktop test is not optimal, as it does not replicate the conditions related to an actual system outage. Nonetheless, it provides some measure of familiarity to program operators and users of contingency measures, which may require implementation.

Appendix 1 - Mission Critical Systems

As part of our review of the Commission Y2K program, we requested that the CIO provide a listing of mission-critical information systems. In response to this request, the CIO provided the following list.

Bureau/Office	Mission Critical Information System
Cable Services Bureau	Cable Antenna Licensing & Cable Operator Registration Systems (COPS/CARS)
Compliance and Information Bureau	Integrated Voice Response System (IVR)
International Bureau	International Bureau Filing System (IBFS)
International Bureau	Co-Channel Serial Licensing System (USA/Canada) (Coser)
Mass Media Bureau	AM Licensing
Mass Media Bureau	FM Licensing
Mass Media Bureau	TV Licensing
Mass Media Bureau	Multipoint Distribution Systems (MDS)
Mass Media Bureau	EEO[5]
Mass Media Bureau	Children's TV
Office of Engineering and Technology	Equipment Authorization System
Office of Engineering and Technology	Experimental Licensing System
Common Carrier Bureau	Informal Complaints
Common Carrier Bureau	Tariffs
Common Carrier Bureau	Automated Reporting Management Information System (ARMIS)
Office of Managing Director	Collections
Office of Public Affairs	Electronic Comments Filing System (ECFS – RIPS)
Wireless Telecommunications Bureau	Aviation
Wireless Telecommunications Bureau	Marine
Wireless Telecommunications Bureau	Restricted & Commercial
Wireless Telecommunications Bureau	Amateur
Wireless Telecommunications Bureau	Auctions
Wireless Telecommunications Bureau	Cellular
Wireless Telecommunications Bureau	Paging
Wireless Telecommunications Bureau	Personal Communications System

---

[5] On May 14, 1999 EEO was taken off the list of mission critical systems.

Wireless Telecommunications Bureau	Coast & Ground
Wireless Telecommunications Bureau	Land Mobile
Wireless Telecommunications Bureau	Microwave
Wireless Telecommunications Bureau	Interactive Video Data Service (IVDS)
Wireless Telecommunications Bureau	Universal Licensing System (ULS)