STATE OF NORTH CAROLINA

AUDIT OF THE

MICRO INFORMATION PRODUCTS APPLICATION

AND

INFORMATION SYSTEMS GENERAL CONTROLS

AT

NORTH CAROLINA PARTNERSHIP FOR CHILDREN

RALEIGH, NORTH CAROLINA

MAY 2002

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE

MICRO INFORMATION PRODUCTS APPLICATION

AND

INFORMATION SYSTEMS GENERAL CONTROLS

AT

NORTH CAROLINA PARTNERSHIP FOR CHILDREN

RALEIGH, NORTH CAROLINA

MAY 2002

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
Board of Trustees, North Carolina Partnership for Children, Inc.
Ms. Karen Ponder, Executive Director, North Carolina Partnership for Children, Inc.

Ladies and Gentlemen:

We have completed our information systems (IS) audit at The North Carolina Partnership for Children (NCPC). The audit was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards*.

The primary objective of this audit was to evaluate controls for the Micro Information Product (MIP) application and to determine if those controls which effect the overall information system (IS) function at NCPC are effective. The scope of our audit included a review of application controls for the MIP accounting system and a review of IS general controls at NCPC. Application controls for the MIP accounting system include data completeness, data accuracy, table maintenance, user access, data backup, processing, and contingency planning. The purpose of application controls is to ensure that as data passes through the application, it is complete, accurate, timely and protected from unauthorized access. Information systems general controls include general security management, access controls, program maintenance, physical security, operations procedures, system software, telecommunications, and disaster recovery. Our audit was limited to the activities of NCPC and did not include consideration of procedures performed by the local Smart Start partnerships.

This report contains an executive summary and audit results which details the areas where NCPC has performed satisfactorily relevant to our audit scope and where improvements should be made.

We wish to express our appreciation to the staff at NCPC for the courtesy, cooperation, and assistance provided to us during this audit.

North Carolina General Statutes require the State Auditor to make audit reports available to the public. Copies of audit reports issued by the Office of the State Auditor may be obtained through one of the options listed in the back of this report.

Respectfully submitted,

Ralph Campbell, Jr.
State Auditor

TABLE OF CONTENTS

We conducted an information system (IS) audit at the North Carolina Partnership for Children from May 1, 2001 through June 28, 2001. The primary objective of this audit was to evaluate the Micro Information Products (MIP) accounting system application controls and the IS general controls in place during that period. We conducted a follow-up review through March 21, 2002, to determine the updated status of controls in place as of that date. Based on our objective, we report the following conclusions.

MIP Accounting System Application Controls

Application reviews determine whether the design of the critical application controls support management's financial statement assertions and that the controls are functioning effectively. These reviews are performed when the auditor intends to rely on the application system controls to reduce the amount of substantive testing of details required before rendering an opinion on the financial statements. The critical application controls that are tested in an application review are: data completeness, data accuracy, table maintenance, user access, data backup, processing, and contingency planning. The vendor of the MIP application system denied us access to the proprietary documentation detailing the system's controls. Therefore, our examination of the application controls of the MIP application was limited to user access, data backup, and contingency planning. We found that NCPC does not have a formal disaster recovery plan for the MIP application. See Audit Finding 1, *Disaster Recovery Plan* under the General Control Section.

Information System General Controls

General security involves the establishment of a reasonable security program that addresses the general security of information resources. We did not identify any significant weaknesses in general security controls of information resources.

The **access control** environment consists of access control software and information security policies and procedures. We reviewed the access controls for the NCPC application system and the local area network (LAN). We did not identify any significant weaknesses in access controls over the NCPC application system and LAN servers during our audit.

Program maintenance primarily involves enhancements or changes needed to existing systems. Our audit did not identify any significant weaknesses in this area.

The operations of the computer should be reasonably secure from foreseeable and preventable threats from fire, water, electrical problems, and vandalism. We did not identify any significant weaknesses in **physical security** during our audit.

The **operations procedures** of the computer center include all of the activities associated with running application systems for users. Our audit did not identify any significant weaknesses in this area.

System software is the collection of programs that drive the computer. The selection of systems software should be properly approved and the software should be maintained by the computer center. Our audit did not identify any significant weaknesses in this area.

The computer service center's **telecommunications** activities should be operated in a way that protects the security and completeness of data being transmitted. Our audit did not identify any significant weaknesses in this area.

A complete **disaster recovery plan** must be developed, approved by management, and tested for the protection of data and the continuity of the entity's operations. This should enable NCPC to recover from an extended interruption due to the destruction of the computer center or other agency assets. We found that NCPC does not have a formal disaster recovery plan for the computer center and the MIP application. See Audit Finding 1, *Disaster Recovery Plan.*

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Under the North Carolina General Statutes Chapter 147-64.6, the State Auditor is responsible for examining and evaluating the adequacy of operating and administrative procedures and practices, systems of accounting, and other elements of State agencies. Information system (IS) application controls audits are examinations of controls, which affect a specific application system. IS general controls audits are examinations of controls which effect the overall organization and operations of the IS function. This IS audit was designed to ascertain the effectiveness of application controls for the Micro Information Product (MIP) accounting system application and the effectiveness of information system general controls at NCPC.

SCOPE

Application controls are those controls that are specific to a particular application system. The scope of our application control audit was to review data completeness, data accuracy, table maintenance, user access, data backup, processing, and contingency planning for the Micro Information Product (MIP) accounting system application.

IS general controls govern the operation and management of computer processing activities. The scope of our IS general controls audit was to review general security management, access controls, program maintenance, physical security, operations procedures, systems software, telecommunications, and disaster recovery which directly affect NCPC computing operations. Other IS general control topics were reviewed as considered necessary.

The North Carolina Partnership for Children (NCPC) provides statewide oversight of the Smart Start initiative. The MIP accounting system is mandated for use by the local Smart Start partnerships. NCPC is responsible for the support and maintenance of the MIP application system at NCPC and the local partnerships. Our audit was limited to the activities of NCPC and did not include consideration of procedures performed by the local Smart Start partnerships.

METHODOLOGY

This IS audit was performed in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and *Information Systems Audit Standards* issued by the Information Systems Audit and Control Association. Our methodology included:

- Reviews of policies and procedures.
- Review of application system documentation.

- Interviews with key administrators and other personnel.
- Examinations of system configurations.
- Tours of the computer facility.
- On-line testing of system controls.
- Reviews of appropriate technical literature.
- Reviews of computer generated reports.

BACKGROUND INFORMATION

During the 1993 Session, the North Carolina General Assembly approved legislation and funding for a statewide early childhood initiative program referred to as Smart Start. At that time, the Department of Human Resources (now the Department of Health and Human Services) was responsible for providing program and administrative oversight for the Smart Start program and for assuring the distribution and accountability of state funds appropriated for the program.

The new legislation required that the North Carolina Partnership for Children (NCPC) and twelve local demonstration projects (local partnerships) be established under separate nonprofit organizations. The purpose of these organizations was to bring together leaders from business, government, education, churches, nonprofit organizations, communities, and families to develop a strategy to improve services to children and families. The initial role of NCPC was to select and provide leadership to the local partnerships, and to solicit financial support for the Smart Start initiative. Currently, NCPC provides technical assistance to eighty-one local Smart Start partnerships in the areas of program development, administration, organizational development, communication, fiscal management, technology, contracts management and fundraising for eighty-one local partnerships.

The General Statutes, required NCPC to develop and implement a comprehensive fiscal accountability plan to ensure the integrity and accountability of State funds appropriated to it and the local partnerships. The aforementioned provision requires all local partnerships to participate in the standard fiscal accountability plan adopted by NCPC in order to receive State funds. Pursuant to this provision NCPC selected the Micro Information Products (MIP) accounting system to be used by NCPC and all local partnerships. MIP is a fund accounting system developed for Non-Profit entities. All local partnerships are required to participate in NCPC's regional accounting and contracting plan; Multi-Partnership Accounting and Contracting (MAC) plan. This plan divides the eighty-one partnerships into regions, each with a lead partnership. Each local partnership is affiliated with one of the lead partnerships. The lead partnership enters data in the MIP application system for itself and its affiliated partnerships.   NCPC   installed   a   new   version   of   the   MIP   software   on September 17, 2001. This version of the MIP Non-Profit series, NPS Pro, provides more security for the application and data files than was possible in the previous versions of the MIP application.

[This Page Left Blank Intentionally]

The following audit results reflect the areas where The North Carolina Partnership for Children has performed satisfactorily and where recommendations have been made for improvement.

MIP ACCOUNTING SYSTEM APPLICATION CONTROLS

DATA COMPLETENESS

Data completeness controls are designed to ensure that all transactions are entered into the system once and only once, that all errors are corrected without any being lost, duplicated or added, that all transactions are processed, that databases are updated completely, and that all output reports are complete. We could not examine data completeness controls because the vendor denied us access to proprietary MIP application documentation.

DATA ACCURACY

Data accuracy controls ensure that the details of transactions are entered and processed correctly, and that printed output is not distributed to the user until it is checked for reasonableness. We could not examine data accuracy controls because the vendor denied us access to proprietary MIP application documentation.

TABLE MAINTENANCE

Systems use tables to make computations and to verify valid codes during data entry. Table maintenance controls ensure that tables used in processing include correct and timely values. We could not examine table maintenance controls because the vendor denied us access to proprietary MIP application documentation.

USER ACCESS

User access controls ensure that only authorized persons are able to inquire about, record, change, or delete data, that electronic signatures used to approve transactions are valid, that only authorized users receive printed reports, and that blank negotiable instruments are protected. We examined user access controls as part of the access controls review for the IS general controls. We did not identify find any significant weaknesses for access controls.

DATA BACKUP

Data backup procedures ensure that the system can be restored if a disaster destroys the primary data files. We examined controls for data backup as part of the disaster recovery review for the IS general controls. We did not identify any significant weaknesses for data backup.

PROCESSING

Processing includes all of the activities associated with running productions jobs. We could not examine processing controls because the vendor denied us access to proprietary MIP application documentation.

CONTINGENCY PLANNING

Agency operations will be disrupted if the agency cannot run the application because of a disaster at the computer center. We examined contingency planning controls as part of disaster recovery review for the IS general controls. NCPC does not have a formal disaster recovery plan for the MIP accounting system. See Audit Finding 1, *Disaster Recovery Plan,* for the IS general controls.

INFORMATION SYSTEMS GENERAL CONTROLS

GENERAL SECURITY

General security management involves the maintenance of a sound security management structure. A sound security management structure should include a method of classifying and establishing ownership of resources, proper segregation of duties, a security organization and resources, policies regarding access to the computer systems and a security education program. We did not identify any significant weaknesses in general security during our audit.

ACCESS CONTROLS

The access control environment consists of access control software and information security policies and procedures. An individual or group with responsibility for security administration should develop information security policies, perform account administration functions and establish procedures to monitor and report any security violations. We did not identify any significant weaknesses in access controls during our audit.

PROGRAM MAINTENANCE

Program maintenance consists of making changes to existing application systems. Programmers should follow program change procedures to ensure that changes are authorized, made according to specifications, properly tested, and thoroughly documented. Application programmers should be restricted to a test environment to ensure that all changes to production resources are tested and approved before moving the changes into production. Changes to application system production programs should be logged and monitored by management. Our audit did not identify any significant weaknesses in program maintenance.

PHYSICAL SECURITY

Controls over physical security are designed to protect a computer center from service interruptions resulting from fire, water, electrical problems, vandalism, and other causes. The Agency's physical security controls ensure that the computer service center is reasonably secure from foreseeable and preventable threats to its physical continuity. We did not identify and significant weaknesses in physical security during our audit.

OPERATIONS PROCEDURES

The operations of the computer center include all of the activities associated with running application systems for users. Procedures should be in place to control the scheduling and running of production jobs, restarting production jobs when problems occur, storing, handling and mounting of tapes, and maintaining computer equipment. Our audit did not identify any significant weaknesses in operations procedures.

SYSTEMS SOFTWARE

Systems software is the collection of programs that the computer center uses to run the computer and support the application systems. This software includes the operating system, utility programs, compilers, database management systems and other programs. The systems programmers have responsibility for the installation and testing of upgrades to the system software when received. Our audit did not identify any significant weaknesses in systems software.

TELECOMMUNICATIONS

Telecommunications is the electronic transmission of any kind of information by radio, wire, fiber optics, microwave, laser, or any other electromagnetic system. It can be evaluated along several lines including the type of system, the geographical organization and the service environment.   The computer service center's telecommunications activities should be operated in a way that protects the security and completeness of data being transmitted. Our audit did not identify any significant weaknesses in telecommunications.

DISASTER RECOVERY

Disasters such as fire and flood can destroy a computer service center and leave its users without computer processing support. Without computer processing, many of the Agency services would grind to a halt. To reduce this risk, computer service centers develop disaster recovery plans. Disaster recovery procedures should be tested periodically to ensure the recoverability of the data center.

AUDIT FINDING 1: DISASTER RECOVERY PLAN

NCPC does not have a comprehensive business continuity plan that would direct the critical operating areas in the event of serious disruptions to computing capabilities. NCPC does have some policies and procedures in place for disaster recovery for the computer center and the MIP application but these have not been incorporated in a formal disaster recovery plan that has been approved by management and tested. NCPC has begun the development of a formal disaster recovery plan for the computer operations and the MIP application; however, it is not fully developed or functional at this time.

The lack of a business continuity plan could lead to delays or inadequate reactions to a major disruption of NCPC operations.

Recommendation: NCPC should continue to develop the disaster recovery plan for its computer operations and MIP application. This disaster recovery plan should be part of a comprehensive business continuity plan for the entire organization and the related MAC sites.

Auditee's Response: NCPC agrees and will complete the disaster recovery plan by December 31, 2002.

DISTRIBUTION OF AUDIT REPORT

In accordance with G.S. § 147-64.5 and G.S. § 147-64.6(c)(14), copies of this report have been distributed to the public officials listed below. Additional copies are provided to other legislators, state officials, the press, and the general public upon request.

EXECUTIVE BRANCH

The Honorable Michael F. Easley	Governor of North Carolina
The Honorable Beverly M. Perdue	Lieutenant Governor of North Carolina
The Honorable Richard H. Moore	State Treasurer
The Honorable Roy A. Cooper, III	Attorney General
Mr. David T. McCoy	State Budget Officer
Mr. Robert L. Powell	State Controller
Ms. Karen Ponder	Executive Director
	North Carolina Partnership for Children, Inc.

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

Senator Marc Basnight, Co-Chairman	Representative James B. Black, Co-Chairman
Senator Charlie Albertson	Representative Martha B. Alexander
Senator Frank W. Ballance, Jr.	Representative Flossie Boyd-McIntyre
Senator Charles Carter	Representative E. Nelson Cole
Senator Daniel G. Clodfelter	Representative James W. Crawford, Jr.
Senator Walter H. Dalton	Representative William T. Culpepper, III
Senator James Forrester	Representative W. Pete Cunningham
Senator Linda Garrou	Representative Beverly M. Earle
Senator Wilbur P. Gulley	Representative Ruth M. Easterling
Senator Kay R. Hogan	Representative Stanley H. Fox
Senator David W. Hoyle	Representative R. Phillip Haire
Senator Luther H. Jordan, Jr.	Representative Dewey L. Hill
Senator Ellie Kinnaird	Representative Mary L. Jarrell
Senator Howard N. Lee	Representative Maggie Jeffus
Senator Jeanne H. Lucas	Representative Larry T. Justus
Senator R. L. Martin	Representative Edd Nye
Senator William N. martin	Representative Warren C. Oldham
Senator Stephen M. Metcalf	Representative William C. Owens, Jr.
Senator Fountain Odom	Representative E. David Redwine
Senator Aaron W. Plyler	Representative R. Eugene Rogers
Senator Eric Miller Reeves	Representative Drew P. Saunders
Senator Dan Robinson	Representative Wilma M. Sherrill
Senator Larry Shaw	Representative Ronald L. Smith
Senator Robert G. Shaw	Representative Gregg Thompson
Senator R. C. Soles, Jr.	Representative Joe P. Tolson
Senator Ed N. Warren	Representative Russell E. Tucker
Senator David F. Weinstein	Representative Thomas E. Wright
Senator Allen H. Wellons	Representative Douglas Y. Yongue

DISTRIBUTION OF AUDIT REPORT (CONCLUDED)

Other Legislative Officials

Representative Philip A. Baddour, Jr.	Majority Leader of the N. C. House of Representatives
Senator Anthony E. Rand	Majority Leader of the N. C. Senate
Senator Patrick J. Ballantine	Minority Leader of the N. C. Senate
Representative N. Leo Daughtry	Minority Leader of the N. C. House of Representatives
Representative Joe Hackney	N. C. House Speaker Pro-Tem
Mr. James D. Johnson	Director, Fiscal Research Division

Other Officials

Chairman and Members of the Information Resource Management Commission

ORDERING INFORMATION

Copies of this report may be obtained by contacting the:

Office of the State Auditor
State of North Carolina
2 South Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Internet: http://www.ncauditor.net

Telephone: 919/807-7500

Facsimile: 919/807-7647