REPORT OF

THE

STATE AUDITOR

Mainframe Disaster Recovery

Performance Audit
January 2007

LEGISLATIVE AUDIT COMMITTEE
2007 MEMBERS

Senator Stephanie Takis
Chair

Representative James Kerr
Vice-Chair

Representative Dorothy Butcher
Senator Jim Isgar
Representative Rosemary Marshall
Representative Victor Mitchell
Senator Nancy Spence
Senator Jack Taylor

Office of the State Auditor Staff

Sally Symanski
State Auditor

Dianne Ray
Deputy State Auditor

Rosa Olveda
Kevin Sear
Colin Whitenack
Legislative Auditors

SALLY SYMANSKI, CPA
State Auditor

STATE OF COLORADO

OFFICE OF THE STATE AUDITOR
303.869.2800
FAX 303.869.3060

Legislative Services Building
200 East 14th Avenue
Denver, Colorado 80203-2211

January 10, 2007

Members of the Legislative Audit Committee:

This report contains the results of a performance audit of state Mainframe Disaster Recovery planning. The audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government. The report presents our findings, conclusions, and recommendations, and the responses of the Governor's Office of Information Technology and the Departments of Personnel and Administration, Human Services, Labor and Employment, and the Department of Revenue.

TABLE OF CONTENTS

PAGE

STATE OF COLORADO
OFFICE OF THE STATE AUDITOR **REPORT SUMMARY**

SALLY SYMANSKI, CPA
State Auditor

Mainframe Disaster Recovery
Performance Audit, January 2007

Authority, Purpose, and Scope

This performance audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the Office of the State Auditor to conduct performance audits of all departments, institutions, and agencies of state government. The audit work, performed from August to October 2006, was conducted in accordance with generally accepted government auditing standards.

The purpose of this audit was to assess the disaster recovery planning for critical information systems that are located on the state mainframe computer. As part of this audit, we reviewed the disaster recovery plans of critical systems that five state departments have on the mainframe. We also observed the annual disaster recovery test of the mainframe, which occurred over three days in August 2006. We acknowledge the assistance extended to us by the Governor's Office of Information Technology; the Department of Personnel and Administration - Division of Information Technologies; and the Departments of Human Services, Labor and Employment, Public Health and Environment; and the Department of Revenue.

Overview

A mainframe computer is capable of storing and processing large amounts of data and running multiple information systems simultaneously. The state mainframe is managed by the Division of Information Technologies (the Division) within the Department of Personnel and Administration. Staff at five departments have identified 11 mainframe systems as critical to their daily functions. Among other things, these functions include tracking and processing income tax; creating records of births and deaths in the State; and processing child support payments, unemployment benefits, and paychecks for all state employees.

The Governor's Office of Information Technology (OIT) and the Commission on Information Management (IMC), which are statutorily authorized to create policies that direct the use of state information systems, adopted a statewide disaster recovery policy in 1990 that requires all state agencies to prepare and test disaster recovery plans for their respective information technology systems. The policy outlines six elements that every plan should address: establishing a disaster recovery team, identifying hardware and software requirements for recovery, developing recovery processes, establishing recovery time frames, maintaining the plan, and testing the plan. Additionally, the Division conducts an annual disaster recovery test of the mainframe computer that includes participation of the agencies with critical systems on the mainframe. The purpose of the test is to determine the ability of those departments to quickly recover critical functionality in the event of a disaster or interruption.

Summary of Audit Comments:

We evaluated the disaster recovery plans for the 11 critical systems on the state mainframe as identified by the departments and observed the annual mainframe disaster recovery test. We noted several weaknesses, including:

- **The Governor's Office of Information Technology is not ensuring that departments have developed disaster recovery plans for systems on the state mainframe computer.** Although the IT systems' disaster recovery policy has been in place for more than 15 years, the OIT does not ensure that agencies are complying with the policy by implementing plans for recovering their systems in the event of a disaster or other interruption.

- **The disaster recovery plans developed by four of the five agencies with critical systems on the mainframe were inadequate.** Many of the plans were missing one or more components required by the OIT/IMC disaster recovery policy. Additionally, one agency had not developed plans for all of its systems.

- **The 2006 annual disaster recovery did not adequately test the recovery capabilities of mainframe systems.** We found that three critical systems were not tested during the 2006 annual test and that four others were not tested adequately.

- **The 2006 annual disaster recovery test was poorly coordinated.** Staff at the Department of Personnel and Administration, Division of Information Technologies are responsible for managing the state mainframe computer, including testing its recovery capability on an annual basis. For staff to fully test the mainframe computer, agencies with systems on the mainframe must be involved. We found, however, that staff at some of the agencies were unaware of the 2006 test because the Division did not formally notify all affected agencies and their respective personnel.

- **The current disaster recovery policy needs updating.** Although all the requirements in the policy are valid according to industry standards, additional requirements would enhance the policy. For example, establishing a distribution policy within the plan will ensure the right people have the plan, and a post-resumption review policy in the plan will assist in establishing the best practices possible when the plan is updated.

Making improvements in these areas would strengthen recovery efforts on the part of the agencies that provide critical functions to the State of Colorado. Our recommendations and the responses of the Governor's Office of Information Technology; the Departments of Human Services, Labor and Employment, Personnel and Administration, Public Health and Environment; and the Department of Revenue can be found in the Recommendation Locator in the following section of this report.

RECOMMENDATION LOCATOR

Rec. No.	Page No.	Recommendation Summary	Agency Addressed	Agency Response	Implementation Date
1	21	Ensure that state departments develop and submit comprehensive annual disaster recovery plans for all critical systems on the state mainframe including: (a) verification that agencies have submitted plans within prescribed time frames and corrective action when agencies do not submit plans, (b) review of plans for comprehensiveness in accordance with the IMC's Contingency Planning/Disaster Recovery Policy, and (c) timely feedback and assistance, when needed.	Governor's Office of Information Technology	Agree	July 2007
2	21	Adopt disaster recovery plans that adhere to the requirements of the IMC's Contingency Planning/Disaster Recovery Policy for their respective critical systems housed on the state mainframe. The plans should be submitted to the Office of Information Technology no later than the June 2007 deadline specified in the 2006 Information and Technology Strategic Plan.	Department of Human Services	Agree	June 2007
			Department of Labor and Employment	Agree	June 2007
			Department of Personnel and Administration	Agree	June 2007
			Department of Revenue	Agree	June 2007

RECOMMENDATION LOCATOR

Rec. No.	Page No.	Recommendation Summary	Agency Addressed	Agency Response	Implementation Date
3	27	Strengthen the effectiveness of the annual mainframe disaster recovery test by (a) providing adequate formal notification to the chief information officers at all of the agencies with critical systems on the mainframe and notification to the Office of Information Technology, and (b) defining the scope, timing, and purpose of the test in coordination with the participating agencies.	Department of Personnel and Administration, Division of Information Technologies	Agree	July 2007
4	28	Improve disaster recovery testing for critical mainframe systems by (a) identifying and testing their respective critical mainframe systems; (b) Identifying and testing all components of non-mainframe systems that the critical mainframe systems interface with; (c) developing comprehensive test plans that adequately test the disaster recovery plans developed for critical systems and actively coordinating with the Division of Information Technologies; and (d) assigning testing responsibilities to all appropriate personnel, including system administrators as well as end users, and ensuring all necessary activities and transactions are tested.	Department of Human Services	Agree	August 2007
			Department of Labor and Employment	Agree	June 2007
			Department of Personnel and Administration	Agree	July 2007
			Department of Revenue	Agree	a. N/A b. June 2007 c. March 2007 d. March 2007

RECOMMENDATION LOCATOR

Rec. No.	Page No.	Recommendation Summary	Agency Addressed	Agency Response	Implementation Date
5	31	Review agency disaster recovery test plans and results to verify that the test was completed, assess whether the individual agency tests meet the requirements of OIT disaster recovery policies, and perform follow-up as appropriate.	Governor’s Office of Information Technology	Agree	January 2008
6	33	Enhance the statewide Contingency Planning/Disaster Recovery Policy by including requirements for information technology system continuity framework, plan distribution, off-site backup storage; and post-resumption review.	Governor’s Office of Information Technology	Agree	July 2007

Mainframe Critical System Disaster Recovery

Overview

According to Section 24-37.5-101, C.R.S., "communication and information resources in the various agencies of state government are valuable strategic assets belonging to the people of Colorado that must be managed accordingly." In keeping with this overall directive, the Colorado Commission on Information Management annually adopts a statewide Information and Technology Strategic Plan (the Plan). The current Plan states, "natural disasters and the rise of domestic and international terrorism place the State's technology systems at increased risk at a time when business functions are becomingly increasingly dependent on reliable technology support." Additionally, catastrophic events, as well as attacks against technology infrastructure and systems, can have a severe impact on business operations. Further, the Plan states that "we must work together to ensure that the State's critical (mission essential) systems are sufficiently safeguarded in appropriate facilities by robust recovery plans...to maintain business continuity of state government." Thus, information system disaster recovery is essential if government is to continue providing critical services in the event of natural or man-made disruptions or disasters. Basically, information system disaster recovery planning refers to the process of identifying, testing, and evaluating all of the resources and procedures needed to make specific information system-based functions of an organization operational after a disruption in service.

State agencies in Colorado rely on a variety of information systems to conduct their daily activities and provide essential services. These systems can be agency-specific such as timekeeping and project management systems. Often, these systems operate on servers or personal computers. Other systems that are critical to one or more agencies, such as statewide financial, payroll, or benefit payment systems, are frequently operated through a mainframe computer. For example, the Colorado Financial Reporting System (COFRS), the Colorado Personnel Payroll System (CPPS), and the Department of Human Services' Electronic Benefits Transfer System (EBT) all operate on a mainframe computer. A mainframe computer generally differs from a personal computer or standard server in that a mainframe is capable of storing and processing large amounts of data and running multiple information systems simultaneously.

State Information System Oversight

Responsibility for developing and overseeing the implementation of the State's information system and disaster recovery planning has been statutorily assigned to the Governor's Office of Information Technology (OIT), the Chief Information Officer of the OIT, and the Colorado Commission on Information Management (IMC). In addition, as described below, the Division of Information Technologies (Division) within the Department of Personnel and Administration plays a critical role in the State's mainframe information system planning processes, including disaster recovery.

Office of Information Technology

According to Section 24-37.5-101 (1)(g), C.R.S.:

> It is the policy of this state to coordinate and direct the use of communication and information resources technologies by state agencies and to provide as soon as possible the most cost-effective and useful retrieval and exchange of information both within and among the various state agencies and branches of government and to the people of Colorado. To that end, the Office of Information Technology is created.

By statute, the Office of Information Technology, or OIT, (formerly the Office of Innovation and Technology) is organizationally located within the Governor's Office. Also by statute (Section 24-37.5-103, C.R.S.), the OIT is to be headed by the Chief Information Officer, who is to be appointed by the Governor. Among the Chief Information Officer's statutory duties are to:

- Monitor trends and advances in communication and information resources and data processing.

- Direct and approve a comprehensive, statewide, four-year planning process.

- Plan for the acquisition, management, and use of communication and information resources and data processing.

- Require state agencies to prepare and submit communication data processing plans to the OIT as part of the State's planning and budgeting process.

In Fiscal Year 2006 the OIT had a budget of approximately $937,000 and employed 10 FTE.

Commission on Information Management

Within the Office of Information Technology is the Commission on Information Management (IMC). The IMC's statutory purpose is to advise the OIT and state agencies on (1) strategic planning and the policies for the State's communications and information systems and (2) the continuity of communications and planning and control of the State's investment in information systems. To fulfill this purpose, the IMC has a number of statutory duties. Among these are the duties to:

- Review the State's information technology plan and the long-range plans of state agencies developed in accordance with the State Plan.
- Assess the status of current state data processing systems and evaluate other potential systems.
- Assist the OIT in developing an approach for achieving statewide compatibility or accessibility of communications and information systems.

By statute, the Chief Information Officer of the OIT serves as a member and the chair of the 15-member IMC. Six members of the IMC are to be appointed by the Governor from the private sector and four are to be members of the General Assembly appointed by House and Senate leadership. The remaining four IMC members are the Director of the Office of State Planning and Budgeting, the Executive Director of the Department of Personnel, the State Court Administrator, and the Executive Director of one principal department designated by the Governor.

Division of Information Technologies

The Division of Information Technologies (Division) is organizationally located within the Colorado Department of Personnel and Administration. The Division's mission is "to support Colorado State Government business functions with high quality information technology and telecommunications tools." Basically, whereas the OIT and the IMC have responsibility and authority for statewide information system policy, the Division provides state agencies with hardware and software support services for agency information systems relating to the state mainframe computer.

The Data Center, within the Division of Information Technologies, provides various services for more than 30 state departments, institutions, and agencies. Services provided by the Data Center include converting and processing data, maintaining and backing up data, preparing reports, and managing the state mainframe computer. The state mainframe computer, which is housed in a controlled and secure environment at the Data Center facility in Lakewood, Colorado, provides information system processing for a number of state agencies. At the time of our audit, Division staff reported that six state departments had at least 23 systems on the state mainframe.

In return for the services it provides, the Data Center receives user fees (cash and cash-exempt funds) from these departments. In Fiscal Year 2006 the Data Center had an appropriated spending authority of approximately $9.7 million to provide computer services to state agencies. During this period, approximately 40 of the 175 FTE within the Division were directly involved with the Data Center. The remaining staff at the Division are responsible for a variety of activities including administering COFRS and CPPS, managing the State's telecommunication infrastructure, and conducting other administrative and support activities.

Agency Use of the State Mainframe

The Colorado Financial Reporting System (COFRS), which is the official record of the State's financial information, is housed on the state mainframe at the Data Center. Consequently, personnel in all state agencies regularly use the mainframe to record the financial transactions of their respective agencies. In addition, some agencies use the state mainframe to house other, agency-specific information systems. Among these information systems are those that agencies have identified as ***critical systems.*** According to the Office of Information Technology, a critical system is one that delivers those functions which, if not performed, would have a grave impact upon the lives of the public and on private property in Colorado. Additionally, the Division of Information Technologies has defined a critical system as one that an agency could not operate without for more than 32 days.

Our audit focused on disaster recovery for the state mainframe and for the critical systems located on it. As shown in the following table and described below, at the time of our audit, there were 11 information systems on the state mainframe that had been identified as critical by the five state departments that rely upon them. It is important to note that many of the information systems operating on the state mainframe have not been identified as critical by the agencies that use them. Furthermore, some agencies have information systems that they may classify as critical that are not located on the state mainframe. Rather, agencies may operate these systems via a server or personal computer. For example, the Colorado Benefits Management System (CBMS), which processes eligibility information for various public and medical assistance programs, is not located on the state mainframe but on a server. Thus, it was not among the systems included in the scope of this audit.

Colorado Division of Information Technologies
Critical Systems Located on the State Mainframe
August 2006

Department	Systems
Human Services	1. Automated Child Support Enforcement System (ACSES) 2. Low-Income Energy Assistance Program (LEAP) 3. Electronic Benefits Transfer (EBT) 4. State Identification Module (SIDMOD)
Labor and Employment	5. Colorado Unemployment Benefits System (CUBS) 6. Workers' Compensation Special Funds
Personnel and Administration	7. Colorado Financial Reporting System (COFRS) 8. Colorado Personnel Payroll System (CPPS)
Public Health and Environment	9. Colorado Vital Information System (COVIS)
Revenue	10. Drivers License System (DLS) 11. Taxation System

Source: Office of the State Auditor review of Department of Human Services, Labor and Employment, Personnel and Administration, Public Health and Environment, and Revenue data.
Note: Systems were identified and self-reported as critical by the state departments associated with them.

Each of the systems identified in the table is described briefly below.

Department of Human Services

The Department of Human Services (DHS) has identified four information systems on the state mainframe as critical to its operations. These four systems are the:

- **Automated Child Support Enforcement System (ACSES)**. The mission of the Child Support Enforcement Program is to "assure that all children receive financial and medical support from each parent." The ACSES performs case management, case enforcement, and financial management of child support collections. In Fiscal Year 2006, DHS staff used ACSES to process about 1.7 million transactions totaling $363 million in child support benefits.

- **Low-Income Energy Assistance Program (LEAP)**. A federally funded program, LEAP is designed to help income-eligible individuals pay their winter home heating bills. Program administrators use a mainframe system, also called LEAP, to determine eligibility and make payments to individuals and vendors. In Fiscal Year 2006, LEAP was used to approved almost $60 million in energy assistance benefits to more than 100,000 households.

- **Electronic Benefits Transfer System (EBT).** The EBT is used to make state benefit payments to eligible recipients or providers of benefit services for programs such as TANF, Child Support, LEAP, and Foster Care. In Fiscal Year 2006, EBT disbursed more than $867 million in benefit and service payments.

- **State Identification Module (SIDMOD).** The SIDMOD is used to create and verify unique identification codes for each recipient of state benefit programs. The identification codes are essential for the issuance of program benefits to recipients, including Child Support, LEAP, Food Stamps, and Temporary Assistance to Needy Families (TANF). Department staff estimate that SIDMOD generates more than 300 new identification codes on a daily basis.

Department of Labor and Employment

The Colorado Department of Labor and Employment (CDLE) administers both the Workers' Compensation program and the Colorado Unemployment Insurance (UI) program. Each of these programs has an information system on the state mainframe that CDLE identified as critical:

- **The Workers' Compensation System** is a mainframe system that facilitates claim intake and then authorizes payments to assist injured workers in Colorado receiving state benefits. The CDLE has identified two subsets of the overall Workers' Compensation System as being critical systems. In Fiscal Year 2006 these two subsets (referred to as Special Funds) distributed almost $13.8 million in benefits to approximately 1,700 recipients.

- **Colorado Unemployment Benefits System (CUBS)** is a mainframe system operated and supported by CDLE and used to distribute benefits. In Fiscal Year 2006 the Department disbursed $301.6 million in UI benefits to eligible individuals.

Department of Personnel and Administration

In addition to its support responsibilities for the State's mainframe described above, the Department of Personnel and Administration (DPA) has responsibility for operating two critical statewide information systems located on the mainframe:

- **Colorado Financial Reporting System (COFRS)**. COFRS is the financial information system for the official accounting records for Colorado State Government. According to DPA, there are approximately 3,000 users of COFRS statewide, and in Fiscal Year 2006, COFRS recorded $24.7 billion in expenditures.

- **Colorado Personnel Payroll System (CPPS)**. CPPS is the payroll system for the State of Colorado's classified personnel system employees. In addition to classified employees, CPPS processes the payrolls for the Judicial Branch and for the Community College System. In addition, all employee benefit information (e.g., health insurance, dental insurance, and long-term disability insurance) is entered through the CPPS online system and stored on the database. According to DPA, CPPS currently processes the payroll and maintains benefit information for approximately 38,000 employees.

Department of Public Health and Environment

The Vital Records Section within the Colorado Department of Public Health and Environment (CDPHE) is the State’s central and official repository of vital event documentation. Vital events are births, deaths, spontaneous fetal deaths (miscarriages), induced terminations of pregnancy (abortions), marriages, and marriage dissolutions (divorces or annulments). The Vital Records Section uses the Colorado Vital Information System (COVIS) to store and retrieve vital records data. Identified as a critical system, COVIS resides on the state mainframe and contains approximately 3.5 million birth and 1.4 million death records from 1906 to the present.

Department of Revenue

Two separate sections within the Department of Revenue have critical information systems located on the state mainframe. The two sections and their information systems are described below:

- **The Tax Business Group** is charged with the collection, administration, audit, and enforcement of all taxes, fees, bonds, and licenses covered under Colorado tax laws. The Tax Business Group has an information system on the state mainframe that combines the processing of income tax, business and license tax, and delinquency cases using three applications. The three applications are the:

- Income Tax application, which processes income taxes for individuals, estates, trusts, and businesses. In Fiscal Year 2006 the income tax system processed about 2.3 million accounts.

- Revenue Accounting System/Taxpayer Registration System (RAS/TRS) provides automated recording, posting, and reporting for business taxes, licenses, and fees collected for the State, counties, cities, and special jurisdictions. In Fiscal Year 2006 the RAS system recorded about $7.9 billion in collections.

- Automated Accounts Receivable Audit Processing System (AARAP) is also known as the tax delinquency system. AARAP assesses penalties and interest on delinquent accounts, establishes repayment agreements and timetables with taxpayers, and calculates interest owed. In Fiscal Year 2006 the AARAP system recorded more than $148 million in collections.

- **The Driver License Section** is responsible for issuing driver licenses, instruction permits, commercial driver licenses, and identification cards to qualifying residents of Colorado. On an annual basis, staff at the Driver License Section have contact with more than 1.3 million customers. The Department has identified its Driver’s License System (DLS) as a critical system on the state mainframe. The DLS is used to issue licenses and contains all pertinent driver information and driver history.

Audit Scope

As part of the Office of the State Auditor's (OSA) audit of the State's Comprehensive Annual Financial Report, the OSA must review the internal controls over the operation of the State's financial reporting system–COFRS–and the Data Center. For Fiscal Year 2005 the OSA conducted a review of the Controls Placed in Operation and Tests of Operating Effectiveness for the Department of Personnel and Administration's Division of Information Technologies' Data Center and Technology Management Unit. The review was conducted in compliance with the Statement on Auditing Standards No. 70, *Service Organizations* (SAS 70), which is an auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The purpose of an SAS 70 review is to report on the safety and integrity of data used in processing agencies' transactions. Although the Fiscal Year 2005 SAS 70 review was limited to internal controls for the state mainframe and the Data Center, it did note related areas of potential concern. Among these concerns was the adequacy of the disaster recovery processes adopted by state agencies with systems on the state mainframe.

The purpose of this audit was to follow up on the concerns identified in the SAS 70 review related to disaster recovery. Consequently, the scope of our current audit was to review the disaster preparedness and recovery processes and plans for the five state departments that have identified critical systems on the mainframe. Because these critical systems require a fully operational mainframe computer to process and store data, we also reviewed the disaster preparedness and recovery processes adopted by the Division of Information Technologies for the State's mainframe computer. As part of the audit, we reviewed statewide and individual agency disaster recovery plans. We also observed the annual mainframe computer disaster recovery test conducted in August 2006, reviewed related test documents, interviewed staff about the test procedures, and evaluated current best practices and industry standards related to information system disaster recovery.

Disaster Recovery Planning

Chapter 1

Overview

In 1990 the Colorado Commission on Information Management (IMC) issued a statewide Contingency Planning/Disaster Recovery Policy (the Policy). The Policy, which is still in effect today, requires "all state branches, agencies, departments, and institutions to prepare and test disaster recovery plans that will be maintained and used in the event of a disaster." Inherent in this policy is the necessity for disaster recovery plans to address all information systems, particularly those identified as critical to agency operations. According to the Policy, agency disaster recovery plans are to follow specific guidelines. The guidelines focus on the following six areas:

- **Designation of a disaster recovery team** including a coordinator and key user personnel.

- **Recovery requirements for each system application** that address physical space, hardware, software, communications, and other resources for recovery.

- **Recovery time frames** outlining both recovery requirements and user procedures.

- **Recovery procedures** detailing the ways in which the applications will be restored, the locations to be used during recovery, and the procedures for returning to the permanent site.

- **Plan testing** on an annual basis, including testing of the recovery requirements, time frames, and the detailed procedures.

- **Plan maintenance** to ensure the plan is updated or modified to reflect changes in recovery requirements, time frames, personnel, or other factors.

In addition to this long-standing statewide policy, the IMC's 2006 Information and Technology Strategic Plan requires that by June 30, 2007, each agency is to complete plans for providing robust disaster recovery functionality to all of their critical systems by June 30, 2008.

In this chapter we discuss issues related to disaster recovery planning for agency information systems. Specifically, we focus on the disaster recovery plans and procedures associated with the 11 critical systems on the state mainframe. As described in the previous chapter, these 11 systems have been identified as mission-critical by the Departments of Human Services, Labor and Employment, Personnel and Administration, Public Health and Environment, and Revenue. Inadequate disaster recovery planning for any one of the 11 systems could significantly and adversely affect the delivery of essential services in the event of a disruption or disaster. Systemwide planning weaknesses could severely cripple state government functioning in many areas including state employee payroll, workers' compensation benefits, driver's license identification and issuance, and income-based assistance programs if multiple systems could not be restored in a timely manner.

In evaluating the disaster recovery plans for the 11 critical information systems on the state mainframe, we found weaknesses in each of the plans, with the exception of one. Moreover, we found the need for statewide improvements in oversight and coordination. In this chapter we present our findings concerning individual agency plans, disaster recovery plan testing, and statewide disaster recovery planning policy.

Critical System Disaster Recovery Plans

As stated above, the IMC Policy requires every state agency, department, and institution to develop and test disaster recovery plans for their respective information systems. We analyzed the disaster recovery plans for the 11 critical systems on the state mainframe by comparing them with the requirements set forth in the IMC Policy. We identified problems in two areas. First, as shown in the following table, we found that disaster recovery plans do not exist for all of the critical information systems. Specifically, the Department of Human Services (DHS) has not developed disaster recovery plans for three of the four state mainframe systems it has identified as being critical to its operations. As the table shows, DHS has not developed a disaster recovery plan for the system used to determine and record eligibility and make payments for the Low-Income Energy Assistance Program (LEAP). Of possibly even greater significance, the Department has not developed plans for either the EBT (Electronic Benefits Transfer) or SIDMOD (State Identification Module) systems. As described in the previous chapter, these two systems are part of the basic infrastructure essential to many of the Department's programs and services such as Child Support, LEAP, Foster Care, Food Stamps, and Temporary Assistance for Needy Families (TANF). Without these two systems, eligibility determination and benefit distribution would be seriously hindered. In the absence of either system, manual processes would be necessary, thereby reducing the efficiency and effectiveness with which many Departmental services could be delivered and adversely affecting county departments of social services, many recipients, and service providers.

The second problem we identified relates to the eight plans that the departments have developed. We found that with one exception, none of the plans contained all of the components identified in the Policy as being essential for recovering critical systems following a disaster. The only plan that addressed all six components was the Colorado Department of Public Health and Environment's (CDPHE) disaster recovery plan for its vital records information system, COVIS. As the table shows, all of the remaining seven plans contained provisions related to disaster recovery procedures and plan testing. However, most of these plans did not address plan maintenance or recovery requirements such as physical space and hardware/software. Our results are summarized in the following table.

Colorado Division of Information Technologies
Critical Information Systems on the State Mainframe
Disaster Recovery Plan Elements
As of August 2006

Department	Critical System	Tea m	Recovery Requirements	Time Frames	Procedures	Test	Maintenance
Human Services	Automated Child Support Enforcement (ACSES)	✓		✓	✓	✓	✓
	Low-Income Energy Assistance Program (LEAP)						
	Electronic Benefits Transfer (EBT)						
	State Identification Module (SIDMOD)						
Labor and Employment	Colorado Unemployment Benefits System (CUBS)				✓	✓	
	Workers’ Compensation	✓	✓		✓	✓	
Personnel and Administration	Colorado Financial Reporting System (COFRS)	✓	✓	✓	✓	✓	
	Colorado Personnel Payroll System (CPPS)	✓	✓	✓	✓	✓	
Public Health and Environment	Colorado Vital Information System (COVIS)	✓	✓	✓	✓	✓	✓
Revenue	Drivers License System (DLS)	✓			✓	✓	✓
	Taxation System	✓			✓	✓	✓

Source: Office of the State Auditor analysis of Departments of Human Services, Labor and Employment, Personnel and Administration, Public Health and Environment, and Revenue disaster recovery plans.
✓ = Plan contained the specific element.

Strengthen Oversight

In keeping with statutes, the Office of Information Technology (OIT) and the Commission on Information Management have adopted statewide policies for information system continuity, including requirements for state agencies to develop disaster recovery plans. However, neither the OIT nor the IMC has implemented adequate methods for ensuring compliance with the requirements. In November 2005 the OIT issued a rule requiring the chief information officer of each agency to annually certify to the IMC that their respective agency is in compliance with contingency planning and disaster recovery planning requirements. However, at the time of our audit, we found no evidence that certification had been provided by any agency or that it had been requested by the OIT. Further, although certification is one means of providing some assurance about plan development, we do not believe it is sufficient. As we have indicated, the agency plans that do exist are often incomplete.

According to Section 24-37.5-106 (1.5), C.R.S., the Chief Information Officer, who heads the OIT and serves as Chairman of the IMC, has the authority to enforce all of the "policies, procedures, standards, specifications, guidelines, or criteria" that are developed pursuant to statute. In addition, by statute, the IMC is charged with assisting and advising the Chief Information Officer in connection with any of his or her duties and responsibilities. Therefore, the OIT and the IMC should work together to strengthen oversight for agency compliance with the State's Contingency Planning/Disaster Recovery Policy. This should include requiring all agencies to submit copies of their annual plans. Staff at the OIT should review the plans for completeness, particularly as they relate to critical information systems on the state mainframe. As we describe in the next section, this should include documentation that annual testing of the plans has occurred and that modifications have been made as a result of the tests, when needed. The OIT should provide feedback and assistance to agencies in developing plans and addressing deficiencies and develop procedures in the event corrective actions are needed. Because the 2006 Information and Technology Strategic Plan requires each agency to complete plans for providing robust disaster recovery by June 30, 2007, the OIT and the IMC should implement a compliance review process to correspond with the Strategic Plan timelines. Finally, the Departments of Human Services, Labor and Employment, Personnel and Administration, and Revenue should take immediate steps to address the plan deficiencies we identified for their critical systems on the mainframe. Comprehensive plans for critical systems on the mainframe should be developed in keeping with the Disaster Recovery Policy and with the timelines outlined in the Strategic Plan.

Recommendation No. 1:

The Governor’s Office of Information Technology should ensure state departments develop and submit comprehensive annual disaster recovery plans for all critical systems on the state mainframe within the time frames specified in the Strategic Plan. This process should include:

a. Verification that agencies have submitted plans within prescribed time frames and corrective action if agencies do not submit plans.

b. Review of plans for comprehensiveness in accordance with the Information Management Commission's Contingency Planning/Disaster Recovery Policy.

c. Timely feedback and assistance, when needed.

Governor's Office of Information Technology Response:

a. Agree. Implementation date: July 2007.

The OIT will develop mechanisms to track plan submissions and follow up with agencies that do not submit plans as prescribed.

b. Agree. Implementation date: September 2007.

The OIT will review all agency disaster recovery plans to ensure compliance with state information technology policies and rules, including the Contingency Planning/Disaster Recovery Policy.

c. Agree. Implementation date: September 2007.

The OIT will develop a formalized process in which feedback will be given to state agencies regarding their disaster recovery plans. This process will also include a mechanism for state agencies to request assistance in developing or refining their plans.

Recommendation No. 2:

The Departments of Human Services, Labor and Employment, Personnel and Administration, and Revenue should take immediate steps to adopt disaster recovery plans that adhere to the requirements of the Information Management Commission's

Contingency Planning/Disaster Recovery Policy for their respective critical systems housed on the state mainframe. The plans should be submitted to the Office of Information Technology no later than the June 2007 deadline specified in the 2006 Information and Technology Strategic Plan.

Department of Human Services Response:

Agree. Implementation date: June 2007.

DHS will take the necessary steps to modify the existing ACSES disaster recovery plan and to adopt disaster recovery plans for LEAP and SIDMOD that all adhere to the IMC's Contingency Planning/Disaster Recovery Policy. These plans will be submitted to the Office of Information Technology no later than June 30, 2007. The EBT system is currently scheduled to be moved off the mainframe environment by June 30, 2007, and as such, a separate disaster recovery plan for EBT will be completed reflecting its new non-mainframe environment.

Department of Labor and Employment Response:

Agree. Implementation date: June 2007.

The Colorado Department of Labor and Employment Information Technology Management Office will develop Disaster Recovery (DR) plans for the Unemployment Insurance (CUBS) and Workers' Compensation Special Funds systems that fully comply with the DR policy set forth by the Office of Information Technology (OIT). That plan will then be submitted to OIT by June 1, 2007.

Department of Personnel and Administration Response:

Agree. Implementation date: June 2007.

The COFRS and CPPS teams, which comprise the Technology Management Unit (TMU) of the Division of Information Technologies, will complete their plans and submit them as requested. These teams will add plan maintenance to their existing plans as this was the only element identified as missing in their plans.

Department of Revenue Response:

Agree. Implementation date: June 2007.

The Department has completed the statewide Continuity of Operations Plan (COOP) according to state guidelines. As a part of COOP, the Department identified critical and essential functions and their supporting systems. In addition, contractors working for the Department of Local affairs completed a test review of the COOP and executed a successful "table top" exercise of the plan. As a next step, the Department is developing disaster recovery plans which will address the critical systems as identified within COOP. The Department will adopt disaster recovery plans that adhere to the IMC Contingency Planning/Disaster Recovery policy for the respective critical systems housed on the State mainframe and will submit them to OIT by June 2007.

Mainframe Disaster Recovery Test

One of the Information Management Commission's rules for information technology disaster recovery planning is that all state agencies prepare and **test** the contingency and disaster recovery plans that will be used in the event of interrupted operation. Further, the rule states that the chief information officer of each agency "shall annually certify to the IMC as to their agency's compliance with this rule." This rule applies to all state agency systems, whether the systems are on the state mainframe or not. Periodic testing of disaster recovery plans is vital to providing a high level of assurance that planned recovery activities will indeed restore critical processes to functionality within a specified time.

For those agencies with systems on the mainframe, the annual disaster recovery test must be scheduled with and coordinated by Division of Information Technologies' staff. Disaster recovery testing of the mainframe simulates a service disruption and requires relocating Division staff from their usual work location to an alternate facility. The alternate facility, known as a "hot site," is a fully operational computing environment equipped with the necessary servers, storage, and networks needed to recover the mainframe computer in the event of an actual disaster. It is important to note that during the disaster recovery test, the State's mainframe does not become inoperable. That is, normal business activity continues. Rather, during the mainframe test, a second backup mainframe at the hot site location is brought online, and selected testing on critical systems occurs.

The Division contracts with an outside provider for the hot site. The current contract provides the State with hot site availability 24 hours a day, 365 days a year at a monthly cost of about $7,400. This monthly charge applies regardless of whether hot site use is needed. In addition, there is a charge of approximately $10,900 for the first two days of an actual recovery and a charge of about $4,000 for each additional day. One 72-hour test per year is included in the contract.

The most recent mainframe disaster recovery test occurred during a three-day period in August 2006. We evaluated the August 2006 test to determine whether the mainframe and the 11 identified critical systems on the mainframe, which are the focus of this report, were adequately tested. As part of our evaluation, we reviewed test planning documents, observed portions of the test, interviewed staff who conducted the test, and assessed post-test documentation. Overall, we found that a lack of adequate planning and coordination resulted in several weaknesses in the mainframe test. These weaknesses diminish the test's effectiveness in providing assurances of the ability to restore critical systems in the event of a disaster, as described in the following sections.

Mainframe Testing

The 11 critical systems on the mainframe computer contain a variety of confidential data related to child support, personal income, taxes, driver’s licenses and other personal and/or confidential information. During normal operations, the Division uses security software that prevents users from gaining unauthorized access. However, during the mainframe computer test, the Division configured the security software in such a way that all users participating in the test could have accessed any mainframe data, regardless of their access rights. The risk for unauthorized access was minimal because access was limited to a few users. Also, access was monitored by Division staff. Nonetheless, the risk was present, and the State has a responsibility to maintain the confidentiality of these data at all times. In addition, by reconfiguring the security software to conduct the test, the Division did not allow the security software to be tested adequately. Division staff cannot ensure that the standard mainframe security software would function correctly in the event of a disaster or whether the software would adversely affect the mainframe or other systems running on the mainframe. Therefore, the test should be run using the standard security software.

Untested Systems

During the 2006 test, the Department of Human Services (DHS) did not test three of its four critical systems that are located on the state mainframe. These are the same three systems for which the DHS has not developed disaster recovery plans–the Low-

Income Energy Assistance Program (LEAP), the State Identification Module (SIDMOD), and the Electronic Benefits Transfer (EBT) utility. Mainframe disaster recovery testing for these systems is necessary to ensure that benefits and services are delivered in an uninterrupted manner. For example, SIDMOD assigns more than 300 unique identifiers per business day and verifies as many as 3,000 daily requests for all DHS eligibility systems. Likewise, EBT transfers benefits from various eligibility systems to a third-party vendor of electronic funds for delivery to benefit recipients. Other DHS systems, both on the mainframe computer and on other servers, rely on EBT and SIDMOD to distribute benefits for child support, child welfare, and direct-care services for the mentally ill, the developmentally disabled, and juvenile offenders. For example, the Colorado Benefits Management System (CBMS), which is on a server, relies on SIDMOD to create identification numbers for new accounts and on EBT to route payments and other benefits to recipients. Annually, the CBMS is responsible for eligibility determination related to approximately $2.1 billion in medical and public assistance benefits to recipients.

For the DHS and all state departments to ensure critical systems are available in the event of a disaster, all critical mainframe systems need to be included in the annual test, and testing should include interfaces with other departmental systems. The test should be planned and designed so that it encompasses the interface and the components of the critical non-mainframe systems that are affected by the mainframe systems.

Inadequately Tested Systems

To fully test the critical mainframe systems, there are two basic stages of the test. First, technical staff from each agency must connect a computer from their respective agency site to the mainframe computer at the hot site. These staff should then perform the necessary procedures to load data and ensure that the technical components of the system being tested are functioning properly. Second, nontechnical staff who routinely use the system must test it to ensure that daily business operations are functioning. We found that for many of the systems, testing was limited to technical staff, as described below:

- **Colorado Personnel Payroll System (CPPS)**. As stated previously, CPPS processes payroll for state employees. We found that DPA staff who conducted the disaster recovery test on CPPS did not perform routine user transactions such as changing employee addresses or other personnel information. They also did not test the disaster recovery system to determine whether it could successfully print paychecks. The DPA staff reported that there was insufficient time to comprehensively test all transactions and that technical software problems during the test prevented printing checks from the disaster recovery mainframe computer.

- **Drivers License System (DLS).** According to Department of Revenue staff, one of the reasons the DLS is critical is that law enforcement agencies across the State rely on it for driver identification and history information. Staff report that they access the DLS in response to approximately 18,000 law enforcement inquiries per month (about 600 per day). However, these staff were not included in the mainframe disaster recovery test.

- **Department of Labor and Employment (CDLE) Systems**. The CDLE staff use the Colorado Unemployment Benefits System (CUBS) to enter unemployment benefit claims, and then the system automatically runs a transaction to approve benefit payments. Staff who tested CUBS during the disaster recovery test did not include these routine users of the system. We also found that CDLE staff who use the Workers' Compensation System to process claims and benefit payments were not included in the test. Thus, the test did not include a determination of whether claims transactions or benefit approvals functioned properly.

Coordinate Testing

The weaknesses we identified in the August 2006 mainframe disaster recovery test resulted from a lack of thorough planning on the part of the agencies, coordination on the part of the Division, and oversight from the Office of Information Technology. Specifically, we found that:

- Agencies participating in the test did not have test plans, or the plans lacked necessary components such as the identification of critical systems, users, and transactions to be tested.

- Division staff did not formally notify all agencies with critical systems on the mainframe about the test or the test details. Some agency staff reported to us that they were unprepared for the test because they had not received adequate notification from the Division. Agencies are ultimately responsible for ensuring that their systems are tested annually. However, the Division must initiate and coordinate the test because of the involvement of the mainframe. Therefore, the Division should formally and systematically notify and/or coordinate the test with all agencies with critical systems on the mainframe, including providing adequate advance notice. In addition, the Division should provide advance notice of the test to the Office of Information Technology. In this way, OIT staff will be aware that agencies participating in the test should be sending verification of their test results.

- Although the OIT's disaster recovery policy requires that agencies test their systems annually, the OIT does not verify that testing occurs. The OIT should require agencies to submit supporting documentation of the annual testing and its results, in conjunction with annual disaster recovery plans. These documents should then be reviewed by OIT staff to ensure agencies have adequately complied with statewide disaster recovery policies and guidelines.

Recommendation No. 3:

The Department of Personnel and Administration's Division of Information Technologies should strengthen the effectiveness of the annual mainframe disaster recovery test to ensure that it adequately prepares state agencies to recover their critical mainframe systems by:

a. Providing adequate formal notification of the test to the chief information officers at the agencies with critical systems on the mainframe. Notification should also be provided to the Office of Information Technology.

b. Defining the scope, timing, and purpose of the test in coordination with the participating agencies.

Department of Personnel and Administration Response:

Agree. Implementation date: July 2007.

a. The Division’s Disaster Recovery Coordinator will contact the chief information officers of participating agencies to notify the agency of the scheduled date and time for the disaster recovery test and to solicit contact information for planning meetings. The Division’s Disaster Recovery Coordinator will also notify OIT. Follow-up planning meetings will be scheduled with participating agencies to ensure an understanding of recovery requirements.

b. The Division will define the time frame and availability for the test. The Division does not define customer scope, but we will coordinate with agencies to enable their testing needs.

Recommendation No. 4:

The Departments of Human Services, Labor and Employment, Personnel and Administration, and Revenue should improve their disaster recovery testing for critical mainframe systems by:

a. Identifying and testing their respective critical mainframe systems.

b. Identifying and testing all components of non-mainframe systems that the critical mainframe systems interface with.

c. Developing comprehensive test plans that adequately test the disaster recovery plans developed for critical systems and actively coordinating with the Division of Information Technologies.

d. Assigning testing responsibilities to all appropriate personnel, including system administrators as well as end users, and ensuring all necessary activities and transactions are tested.

Department of Human Services Response:

Agree. Implementation date: August 2007.

The Colorado Department of Human Services will apply the four recommended tasks identified to better improve our disaster recovery testing of critical mainframe systems.

a. CDHS has identified its critical mainframe systems and will test them all during the next scheduled mainframe disaster recovery test currently scheduled for August 2007.

b. CDHS will identify and test those non-mainframe systems that interface with our critical mainframe systems during the next scheduled mainframe disaster recovery test currently scheduled for August 2007.

c. CDHS will develop comprehensive test plans that will adequately test the disaster recovery plans for our critical systems during the next scheduled mainframe disaster recovery test currently scheduled for August 2007. CDHS will coordinate these plans with the Division of Information Technologies to help ensure compliance and success.

d. As a part of our test plans, CDHS will ensure that all appropriate personnel, including systems administrators and end users of the system, adequately test appropriate activities and transactions of the system to validate a successful recovery. This will be accomplished during the next mainframe disaster recovery test, scheduled for August 2007.

Department of Labor and Employment Response:

Agree. Implementation date: June 2007.

a. The Colorado Department of Labor and Employment Information Technology Management Office will incorporate within the CDLE Disaster Recovery (DR) plan, tests of the mainframe programs that support the Unemployment Insurance CUBS and Workers' Compensation Special Funds systems.

b. The CDLE Information Technology Management Office will incorporate within the CDLE Disaster Recovery (DR) plan, tests of any non-mainframe systems, servers, or entities, with which the mainframe programs supporting the Unemployment Insurance CUBS and Workers' Compensation Special Funds systems interface. The CDLE, with the assistance of the Division of Information Technologies personnel, as needed, will coordinate the testing of such systems, servers, or entities.

c. The CDLE Information Technology Management Office will incorporate within the CDLE Disaster Recovery (DR) plan, tests of the mainframe programs that support the Unemployment Insurance CUBS and Workers' Compensation Special Funds systems. The CDLE will work closely with the Division of Information Technologies personnel to ensure that the test plan follows and complements the one set forth by the Division.

d. The CDLE Information Technology Management Office (ITMO) will incorporate and identify within the CDLE Disaster Recovery (DR) plan, those individuals, and/or positions, from the business and from ITMO application development and support functions needed to perform the outlined tests of the mainframe programs that support the Unemployment Insurance CUBS and Workers' Compensation Special Funds systems. The CDLE will work closely with the Division of Information Technologies personnel to ensure the involvement of any individuals deemed necessary, to accomplish all testing outlined.

Department of Personnel and Administration Response:

Agree. Implementation date: July 2007.

a. COFRS and CPPS have already been identified as critical systems, and testing is performed during each DR test, as identified in the table on page 19 of the audit report.

b. The Department of Personnel and Administration's Information Technology Unit will identify any DPA non-mainframe critical components that interface with critical mainframe systems (COFRS and CPPS) and plan testing for those same components.

c. DPA (COFRS and CPPS) test plans have been created and audit elements have been identified as existing with the exception of plan maintenance (see 19 of the audit report). The Division will improve internal coordination of testing with CPPS and COFRS staff.

d. COFRS and CPPS teams will assign testing to appropriate administrators and end-users to test necessary activities and transactions. The table on page 19 of the audit report indicates that the plans for these systems contain testing elements.

Department of Revenue Response:

Agree. Implementation dates:
a: Not applicable to Department of Revenue
b: June 2007
c: March 2007
d: March 2007

a. This part of the recommendation is not applicable to Department of Revenue, because it previously identified its critical systems and those systems were tested in the annual mainframe disaster recovery test.

b. The Department has identified all critical non-mainframe components that interface with the mainframe systems and will strengthen its test plan for these components to address the auditor’s recommendation.

c. The Department will meet with the Division of Information Technologies and coordinate the Disaster Recovery Testing process utilizing the

Continuity of Operations Plan (COOP) to identify the critical and essential systems. In addition, the Department is in the process of switching to the state standard Docuvault for off-site data backup warehousing in order to improve coordination with the Division of Information Technologies.

d. The Department has assigned and documented testing responsibilities for mainframe functions as identified in the statewide Continuity of Operations Plan. As a part of developing its Disaster Recovery plan, the Department will work with users, vendors, and the Department of Revenue IT to confirm that testing responsibilities as defined in the plan will ensure all necessary activities and transactions are tested.

Recommendation No. 5:

The Governor's Office of Information Technology should review agency disaster recovery test plans and results to verify that the test was completed, assess whether the individual agency tests meet the requirements of OIT disaster recovery policies, and perform follow-up as appropriate.

Governor's Office of Information Technology Response:

Agree. Implementation Date: January 2008.

The OIT will develop procedures for:

a. Reviewing agencies' disaster recovery test plans.

b. Verifying tests were completed.

c. Determining if the tests meet the requirements of the Disaster Recovery Policy.

d. Performing any follow-up.

Disaster Recovery Policy

In conducting this audit, we used the Information Management Commission's Contingency Planning/Disaster Recovery Policy as the basis for much of our analysis. That is, we compared the guidelines set forth in the Policy with the disaster recovery plans developed by the agencies that have critical systems on the state mainframe. Although the scope of this audit was limited to the state mainframe computer and the critical systems residing on it, the Policy and the OIT's and IMC's responsibilities for statewide oversight of disaster recovery extend to all agency information systems whether on the mainframe or not.

Overall, the Policy serves as a strong foundation for information system disaster recovery planning in Colorado State Government. However, it is in need of updating. The Policy was adopted more than 15 years ago and has not been significantly modified since that time. During the same period, there have been significant advances in information technology and disaster recovery controls.

We reviewed current best practices on information system disaster recovery planning and compared the best practices with Colorado's statewide disaster recovery policy. We identified four components that are currently not included in the State's Policy. The addition of these components would enhance the existing policy, thereby providing greater assurance of the ability to perform information system recovery following a disaster or interruption, as described below:

- **Information technology continuity framework.** Each agency should develop an overall framework for business continuity management including the procedures for documenting, testing, and executing the plans. The framework should also address items such as identifying and updating the list of all mainframe and non-mainframe critical systems on a periodic basis, and monitoring and reporting on the availability of critical resources, alternative processing, and the frequency with which systems will be backed up.

- **Plan Distribution**. Disaster recovery plans should be distributed properly and securely to designated personnel. This should include agency management. In our current audit, we found that in some departments, management was unaware of existing disaster recovery plans or their whereabouts.

- **Backup storage**. The existing statewide policy does not address the need for off-site storage of all backup critical media, documentation, plans, and other information system resources necessary for IT recovery and business continuity. Without access to the disaster recovery plans, the ability of agencies to recover their critical systems would be severely diminished. Agency management should ensure that off-site arrangements are periodically assessed for content, environmental protection, and security.

- **Post-resumption review.** Best practices indicate that a review of the disaster recovery efforts should occur following successful resumption of the information systems' functions after a disaster recovery test. Agencies should debrief or evaluate the adequacy of the recovery efforts and update the plan accordingly.

According to Section 24-37.5-106, C.R.S., the Chief Information Officer of the Office of Information Technology is responsible for monitoring information system trends and advances and creating and overseeing statewide information system policies in coordination with the Information Management Commission. In keeping with this mandate, the Chief Information Officer and the IMC should work together to strengthen the State's Contingency Planning/Disaster Recovery Policy by updating it to include the components identified above. The OIT should then ensure that all agencies include the required components in their annual disaster recovery plans.

Recommendation No. 6:

The Chief Information Officer of the Governor's Office of Information Technology, in coordination with the Information Management Commission, should enhance the statewide Contingency Planning/Disaster Recovery Policy by including requirements for information technology system continuity framework, plan distribution, off-site backup storage, and post-resumption review.

Governor's Office of Information and Technology Response:

Agree. Implementation date: July 2007.

The state Chief Information Security Officer (CISO) has developed a new policy that specifically addresses the four Disaster Recovery requirements outlined in this recommendation. The OIT will adopt this new policy and enforce its requirements.

The electronic version of this report is available on the Web site of the
Office of the State Auditor
www.state.co.us/auditor

A bound report may be obtained by calling the
Office of the State Auditor
303.869.2800

Please refer to the Report Control Number below when requesting this report.

Report Control Number 1824