Colorado Department of Personnel & Administration
Division of Information Technologies
Data Center and Technology Management Unit

Report on Controls Placed in Operation and Tests of Operating Effectiveness

Period from July 1, 2004 through June 30, 2005

State of Colorado
Legislative Audit Committee
2006 Members

Senator Jack Taylor
Chair

Senator Stephanie Takis
Vice-Chair

Representative Fran Coleman
Senator Jim Isgar
Representative David Schultheis
Senator Nancy Spence
Representative Val Vigil
Representative Al White

Office of the Colorado State Auditor

Joanne Hill
State Auditor

Sally Symanski
Deputy State Auditor

Greg Fugate
Kevin Sear
Legislative Auditors

BKD, LLP

Rob MaCoy
Rodney Walsh

Colorado Department of Personnel & Administration
Division of Information Technologies
Data Center and Technology Management Unit
Report on Controls Placed in Operation and Tests of Operating Effectiveness
Period from July 1, 2004 through June 30, 2005

Contents

Section

I. Independent Service Auditors' Report 1

II. Report Summary

Authority, Standards, and Purpose/Scope of Examination 3

Summary of Major Audit Comments 4

Summary of Progress in Implementing Prior Audit Recommendations 5

III. Recommendation Locator 6

IV. Organization and Functions of the Division of Information Technologies Data Center and Technology Management Unit 7

V. Description Provided by the Division of Information Technologies Data Center and Technology Management Unit 16

VI. Information Provided by the Service Auditor

Findings and Recommendations 38

Control Objectives, Control Activities, Tests of Operating Effectiveness and Results of Tests 47

Figure 1 – Define IT Strategic Plan 48

Figure 2 – Define the IT Organization and Relationships 50

Figure 3 – Manage Human Resources 51

Figure 4 – *This Figure Intentionally Left Blank* 54

Figure 5 – Communicate Management Aims and Directions 55

Figure 6 – Assess Risks 56

Figure 7 – Manage Facilities 57

Figure 8 – *This Figure Intentionally Left Blank* 61

Figure 9 – Manage Quality 62

Figure 10 – Acquire or Develop Application Software 63

Figure 11 – Acquire Technology Infrastructure 64
Figure 12 – Develop and Maintain Policies and Procedures 65
Figure 13 – Install and Test Application Software and Technology Infrastructure 66
Figure 14 – Manage Service Levels 77
Figure 15 – Define and Manage Service Levels 78
Figure 16 – Manage Third-Party Services 79
Figure 17 – Enhance System Security 81
Figure 18 – Manage the Configuration 91
Figure 19 – Manage Problems and Incidents 93
Figure 20 – Manage Data 94
Figure 21 – Manage Operations 95
Figure 22 – Human Resource/Payroll System 98

VII. Status of Implementation of Prior Recommendations 105

VIII. User Control Considerations 111

Distribution Page 115

This Page Intentionally Left Blank

Section I
Independent Service Auditors' Report

Independent Service Auditors' Report

To Members of the State of Colorado Legislative Audit Committee:

We have examined the accompanying description of controls provided by the Division of Information Technologies (DoIT) Data Center and Technology Management Unit (DC/TMU) relative to the COFRS (Colorado Financial Reporting System), CPPS (Colorado Personnel Payroll System) and Data Center Housing and Hosting Activities. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of DoIT's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of DoIT's controls; and (3) such controls had been placed in operation as of June 30, 2005. The control objectives were specified by the management of DoIT. Our examination was performed in accordance with the standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the Division of Information Technologies (DoIT) and Technology Management Unit's controls presents fairly, in all material respects, the relevant aspects of DoIT's controls that had been placed in operation as of June 30, 2005. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of DoIT's controls.

The accompanying description states that DoIT controls will provide for reasonable assurance that third-party services are secure, accurate and available, support processing integrity and be defined appropriately in performance contracts. Based on inquires of management personnel and inspection of documents, the associated control activities as outlined in Figure 16 of Section VI were not operating effectively.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls listed in Section VI of this report to obtain evidence about their effectiveness in meeting the related control objectives, described in the Control Objectives Matrices of Section VI, during the period from July 1, 2004 to June 30, 2005. The specific controls and the nature, timing, extent and results of the tests are listed in the Control Objective Matrices of Section VI. This information has been provided to user organizations of DoIT and to their auditors to be taken into consideration, along with the information about the internal control of user organizations, when making assessments of control risk for user organizations. In our opinion, except for the matter referred to in the preceding paragraph, the controls that were tested, as described in the Control Objective Matrices of Section VI, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in the Control Objective Matrices of Section VI were achieved during the period from July 1, 2004 to June 30, 2005. However, the scope of our engagement did not include tests to determine whether control objectives not listed in the Control Objective Matrices of Section VI

were achieved; accordingly, we express no opinion on the achievement of control objectives not included in the Control Objective Matrices of Section VI.

The relative effectiveness and significance of specific controls at DoIT and their effect on assessments of control risk at user organizations are dependent upon their interaction with the controls and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of controls at individual user organizations.

The description of controls at DoIT is as of June 30, 2005, and information about tests of the operating effectiveness of specific controls covers the period from July 1, 2004 to June 30, 2005. Any projection of such information to the future is subject to the risk that, because of changes, the description may no longer portray the system in existence. The potential effectiveness of specified controls at DoIT is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

The information included in Section VI and described severally as "Department of Personnel & Administration's Response" is presented by DoIT to provide additional information to user organizations and is not a part of DoIT's description of controls that may be relevant to user organizations' internal control as it relates to an audit of financial statements. The information in Section VI and described severally as "Department of Personnel & Administration's Response" has not been subject to the procedures applied in the examination of the description of the controls related to DoIT and, accordingly, we express no opinion on it.

This report is intended solely for use by the Members of the State of Colorado State Legislative Audit Committee and management of DoIT, the user organizations, and the independent auditors of the user organizations.

BKD, LLP

September 27, 2005

This Page Intentionally Left Blank

Section II
Report Summary

Authority, Standards and Purpose/Scope of Examination

This examination of the general controls at the Division of Information Technologies (DoIT) Data Center and Technology Management Unit (DC/TMU) was conducted under the authority of Section 2-3-103, CRS, which authorizes the Office of the State Auditor to conduct audits of all departments, institutions and agencies of state government. (Please refer to Section IV for a description of the DoIT and DC/TMU organization.) This examination was conducted in accordance with standards established by the American Institute of Certified Public Accountants (AICPA). The period under review was July 1, 2004 through June 30, 2005.

SAS 70 Overview

The SAS 70 (Statement on Auditing Standards No. 70, *Service Organizations*) is an auditing standard developed by AICPA. The SAS 70 provides guidance that allows a service organization such as DC/TMU to disclose its control activities and processes to its customers (user organization) and its customer's auditors (user auditor). The service organization employs an independent accounting and auditing firm (service auditor) to examine its control objectives and control activities. The service auditor issues a Service Auditor's Report to the service organization at the end of the examination that includes the auditor's opinion.

Objectives of the Examination

This report on examination of controls placed in operation is intended to provide interested parties with information sufficient to understand the basic structure of controls within DC/TMU. This report, when coupled with an understanding of controls in place at user locations, is intended to permit evaluation of the total system of internal control surrounding transactions processed through the reviewed systems.

Our examination was restricted to selected services provided to system users by DC/TMU, including users of the COFRS (Colorado Financial Reporting System) and CPPS (Colorado Personnel Payroll System) applications, and, accordingly, did not extend to controls in effect at user locations. It is each interested party's responsibility to evaluate this information in relation to controls in place at each user location in order to assess the total system of internal control. The user and DC/TMU portions of the system must be evaluated together. If effective user controls are not in place, DC/TMU controls may not compensate for weaknesses.

Auditors using this report as part of their review of a user's system of internal controls may conclude that DC/TMU's description of controls provides a basis for reliance thereon and for restricting the extent of their substantive tests. Alternatively, user auditors may elect not to rely on controls within DC/TMU's system. In that event, they should accomplish their audit objectives by other means.

The objectives of data processing controls are to provide reasonable, but not absolute, assurance about such things as the following:

- Protection of data files, programs and equipment against loss or destruction
- Prevention of unauthorized use of data records, programs and equipment

- Proper handling of input and output data records
- Reliable processing of data records

The concept of reasonable assurance recognizes that the cost of a system of internal control should not exceed the benefits derived and, additionally, that evaluation of internal control necessarily requires estimates and judgments by management.

Summary of Major Audit Comments

A complete listing of our recommendations from this year's examination and management's responses may be found in Section III – Recommendation Locator. Additional details regarding the following recommendations, plus additional recommendations of lesser significance, may be found in Section VI – Information Provided by the Service Auditor.

It should be noted that in many instances, the recommendations are the logical result of an exception noted during the examination. However, a number of recommendations refer to control objectives and activities that did not exhibit an exception during the examination. This is a result of the Division of Information Technologies successfully meeting the objective, but a best practice recommendation is being made to offer improvements to current established controls.

The following summarizes the more significant findings contained in this report:

- Individual departments and agencies are responsible for designing and requesting their own mainframe backups. Although these backups are not a part of this control, we observed a lack of continuity in the various backup tasks identified by the individual departments. This lack of coordination is evident in the narrative in the last disaster recovery plan (DRP). We strongly recommend that backup processes and procedures be brought under the review of an individual or committee within DoIT that meets on a regular basis to review processes. This process could also prove beneficial to non-mainframe housed and hosted data.

- We observed that individual departments are responsible for maintaining and designing their backup testing requirements. We observed a lack of continuity in the process. We believe that a once-a-year test is not adequate. We recommend that tapes and CD backup materials be tested on a sampling basis on drives other than the creating drives at least quarterly.

- Segregation of Duties – Systems Development Life Cycle (SDLC) is a systems approach to problem solving and is made up of several phases, including software design, programming, testing and implementation. These functions are a regular component of the activities performed within DoIT in support of COFRS and CPPS, but testing is often the responsibility of an individual or small group of programming staff. Segregation of these duties among separate staff enhances the reliability and control of the SDLC or change-management functions. We recommend that DoIT review and enhance segregation of duties among programming and testing staff.

- When contracts for third-party services are below a stated dollar threshold, DoIT is not required to submit the contract for DPA review. There is limited review and monitoring of third-party services that fall under the dollar threshold where DPA involvement is not required. With the dollar threshold being increased to $50,000 per engagement, the services can be significant.

It is recommended that an individual be designated to monitor and report per the control objective.

- The Top Secret security administration function is currently distributed among users. DoIT manages Top Secret administrator accounts. We recommend consideration of centralizing Top Secret security administrator responsibilities with DoIT in order to control and monitor usage of assets and assign security. In addition, additional and regular Top Secret training for the Security Operations Center staff, including key top management, is recommended in order to add depth to key security positions and enhance management's ability to manage and monitor operations.

Summary of Progress in Implementing Prior Audit Recommendations

The Division of Information Technologies Data Center and Technology Management Unit have made significant progress in implementing the recommendations from prior audits and reports covering the period from April 2000 through June 30, 2004. The most common issues cited for recommendations not yet implemented include staffing limitations and/or budget limitations. A complete discussion of the status of implementation is provided in Section VII – Status of Implementation of Prior Audit Recommendations.

Section III
Recommendation Locator

Recommendation Locator

No.	Figure Reference(s)	Recommendation	Agency response	Implementation date
1	17.35, 20.1	Provide centralized review and guidance for all backup procedures for DoIT users.	Agree	7/31/2006
2	20.1	Implement regular internal data recovery testing on a sampling basis in addition to the formal annual data recovery test.	Agree	6/30/2006
3	13.4, 13.11	Review and enhance segregation of duties among programming and testing staff.	Partially Agree	6/30/2006
4	16.1 – 16.6, 17.36, 17.37	Designate an individual to manage third-party services.	Partially Agree	12/31/2006
5	17.3	Centralize the Top Secret Security Administration function to DoIT and provide additional training for DoIT Top Secret Security Administration staff.	Agree	6/30/2006
6	17.21, 17.22	Institute documented incident response criteria and response escalation procedures.	Agree	6/30/2006
7	13.45	Implement improved physical security around warrant stock.	Agree	5/1/2006
8	14.1, 15.2	Implement and track service level agreement for all DoIT clients.	Agree	4/1/2006 and ongoing
9	3.2, 3.3, 5.1, 5.2, 5.3, 6.1, 9.3, 11.2, 13.8,13.26, 13.27	Institute a process to retain source documents for reference and audit for an appropriate period commensurate with the data.	Agree	6/30/2006
10	5.1, 5.2, 5.3, 17.4	Ensure critical information and decisions are communicated and reinforced with affected employees.	Agree	6/30/2006
11	7.4, 7.5, 9.1, 17.31	Review documentation against control objectives and current operations to ensure consistency with current practice.	Agree	6/30/2006 and ongoing
12	9.1	Consolidate Outage Notification and Remedy issue tracking system to track outages and assign responsibility within a single system.	Agree	4/1/2006 and ongoing

Section IV
Organization and Functions of the Division of Information Technologies Data Center and Technology Management Unit

The Division of Information Technologies (DoIT) Data Center and Technology Management Unit both reside under the Colorado Department of Personnel & Administration. The following outlines the mission, funding sources and organization and functions of both the Data Center and the Technology Management Unit.

Data Center

Mission

The Data Center currently functions as a service bureau to provide data processing services to the executive, legislative and judicial branches of state government.

The Data Center's mission is "to efficiently, effectively and economically provide quality information products and services to meet customer program objectives." The Data Center performs various services for state agencies that include converting and processing data, maintaining and backing up data, preparing reports and ensuring that its computer system can be recovered in the event of a disaster. It also maintains a data communication network from its computer system to agency terminals and minicomputers.

The Data Center has established controls to ensure the security and integrity of users' data, programs and output, and the protection of its own equipment and software. The implementation of the Colorado Financial Reporting System (COFRS) in 1990 eliminated the former General Government Computer Center's responsibility for control of the development and maintenance of other portions of the State's central financial system. COFRS, now part of the Technical Business Applications Section of the Department of Personnel & Administration, has assumed these responsibilities.

The Data Center utilizes two primary methods of customer contact for the purpose of improving the Center: (1) the Customer Roundtable (CR) and (2) the direct customer meeting. The Data Center established the CR Forum to improve communications between itself and its users. The direct customer meeting was established to provide specific input regarding the direction and service levels of the Data Center.

Funding Sources

The Data Center is a cash-funded agency with more than 90 billable customers in more than 30 state departments, institutions and agencies. Billable items include computer processing time, computer storage space, printing charges and database support. Funds for these items are appropriated to each department, with the Data Center receiving matching cash spending authority. The money in the cash fund is subject to annual appropriation. During fiscal year 2005, the Data Center received an appropriated spending authority of approximately $12 million to provide computer services to state agencies.

Organization and Functions

The Data Center operates 24 hours per day, seven days a week, including holidays. Approximately 61 of the DoIT 149 full-time equivalents (FTE) are directly involved with the Data Center. These FTEs include the following:

- **Management:** The DoIT Division director spends approximately 50% of his time in the management of the Data Center; the Computing Services manager is engaged full-time in Data Center management.

- **Business and Administrative Services:** These are support services required to operate the Data Center. Services including budget preparation, control and monitoring. Also included are internal accounting, personnel functions, word processing and switchboard/receptionist services at the Data Center.

- **Customer Support Services:** These are the direct customer support services personnel. Responsibilities include change management, security and handling customer service requests for informational reports extracted from system files in a short time period. The Service Center is a functional area within Customer Services providing scheduling, console management, help desk and videoconference support.

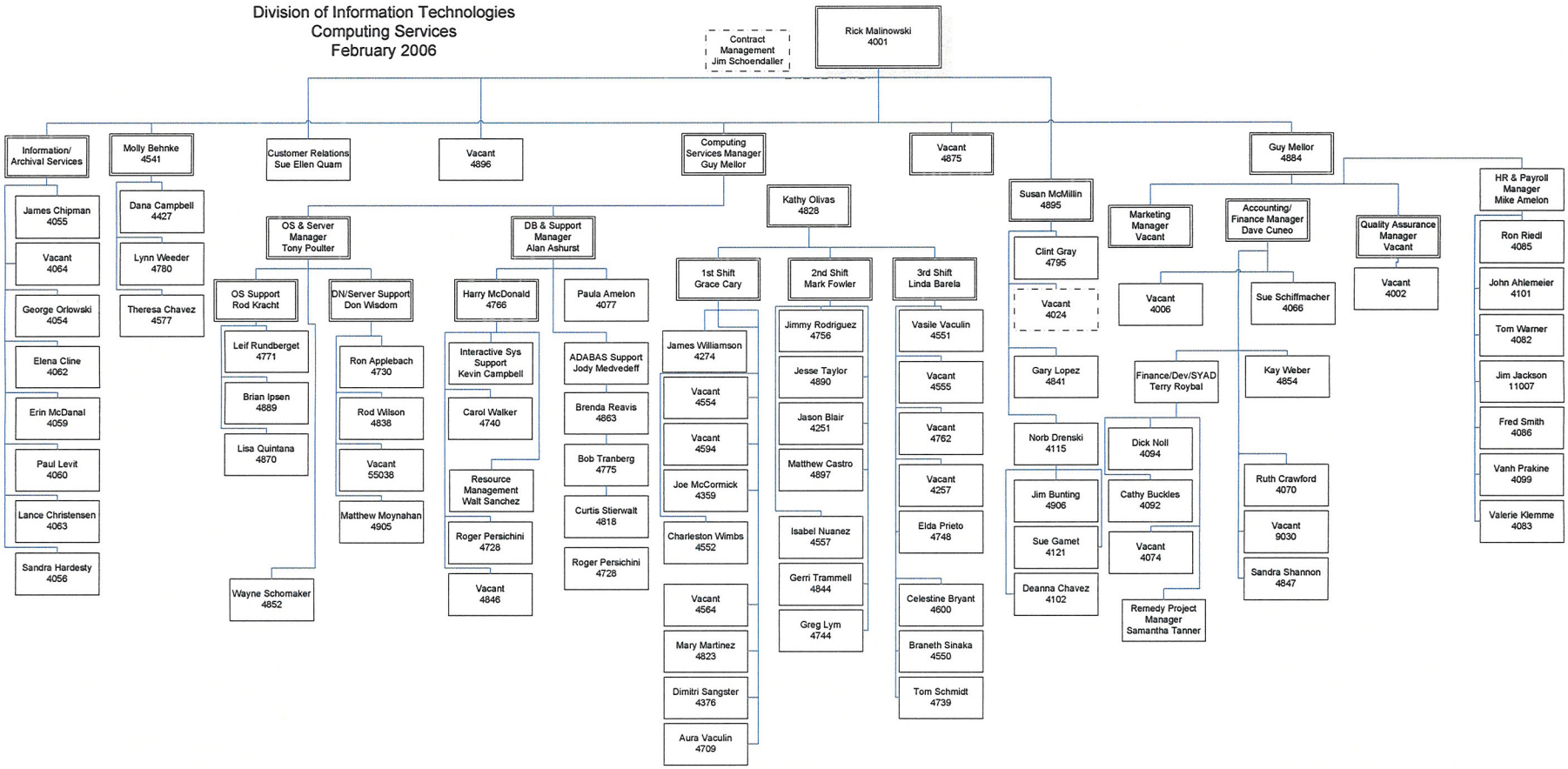
- **Technical Services:** These services include the installation, implementation and maintenance of all computer systems software at the Data Center. Technical Services also provides support for all shared databases and support activities. Technical Services staff perform hardware and software evaluations and provide technical training and documentation for Data Center customers. Desktop, server and local area network equipment directly operated by DoIT is supported within this functional group as well.

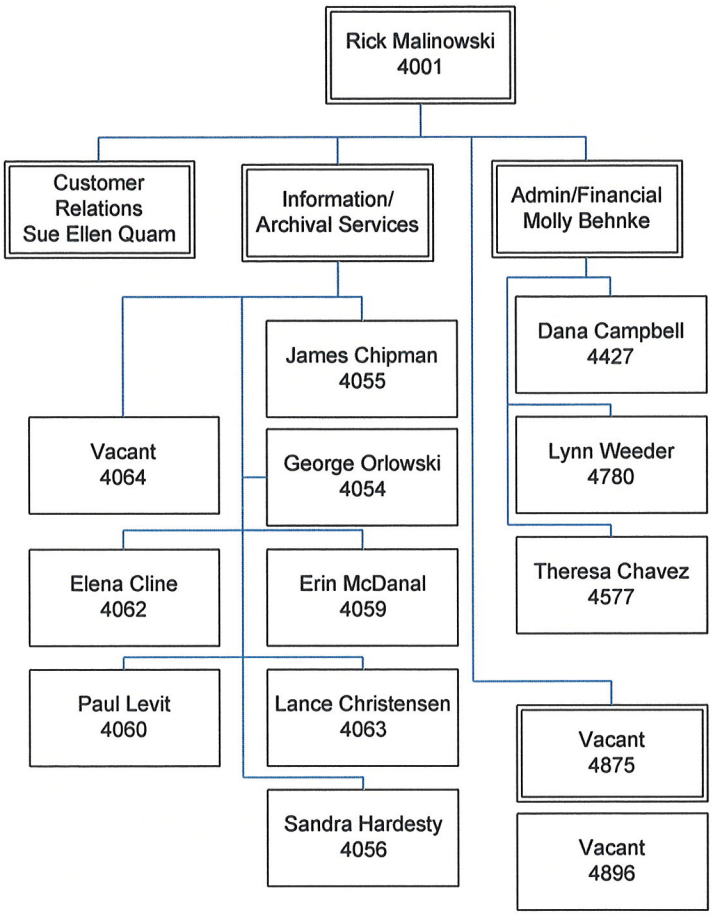
- **Computer Operations:** These services include installing and operating computer and printing equipment, maintaining disk and tape systems and the control and distribution of computer output. The disaster recovery function within this area is responsible for developing, implementing, coordinating and monitoring the Data Center's disaster recovery plan.

Colorado Department of Personnel & Administration
Division of Information Technologies
Data Center and Technology Management Unit

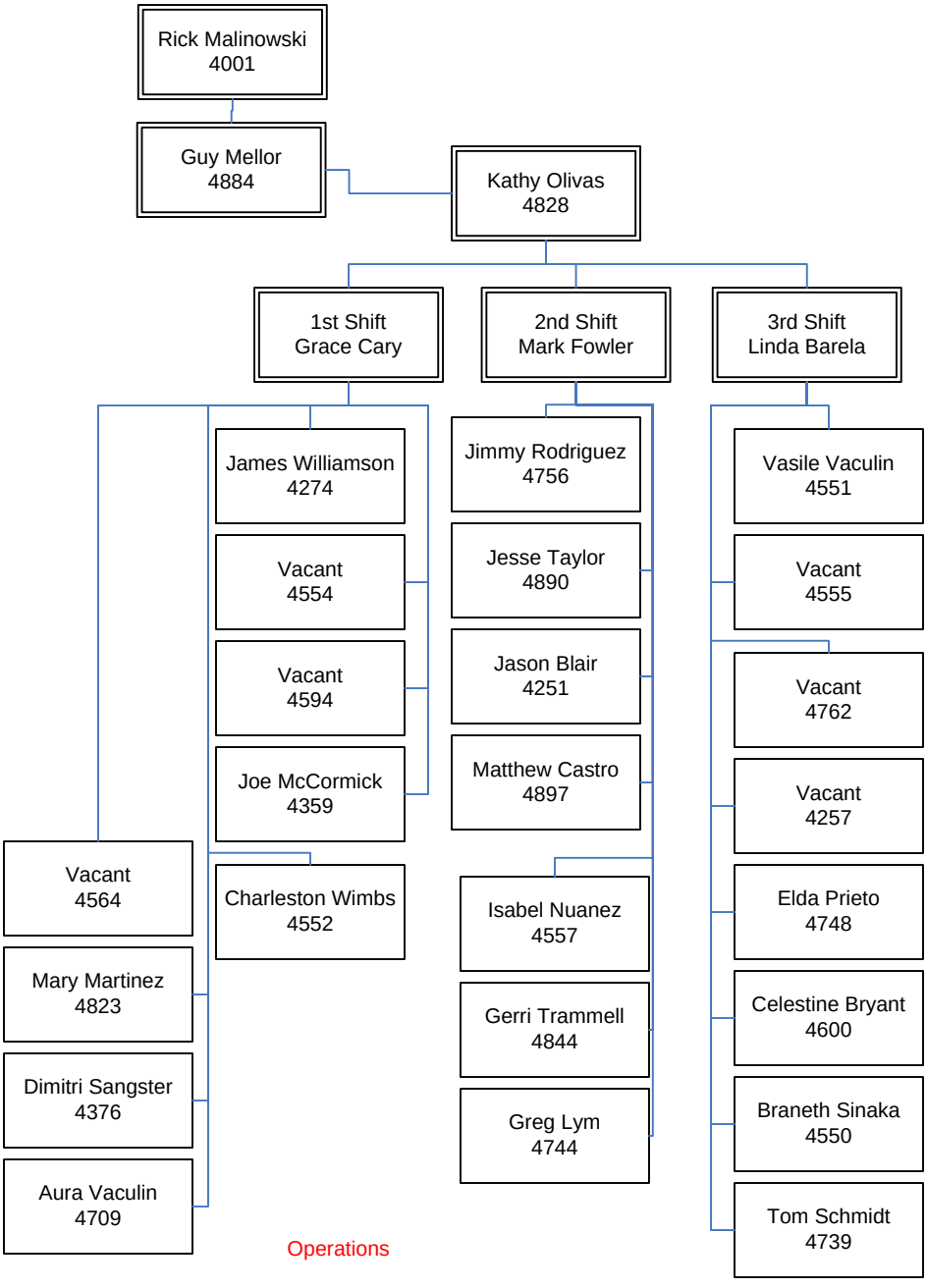
Report on Controls Placed in Operation and Tests of Operating Effectiveness
Period from July 1, 2004 through June 30, 2005

Division of Information Technologies
Functional Organization Chart



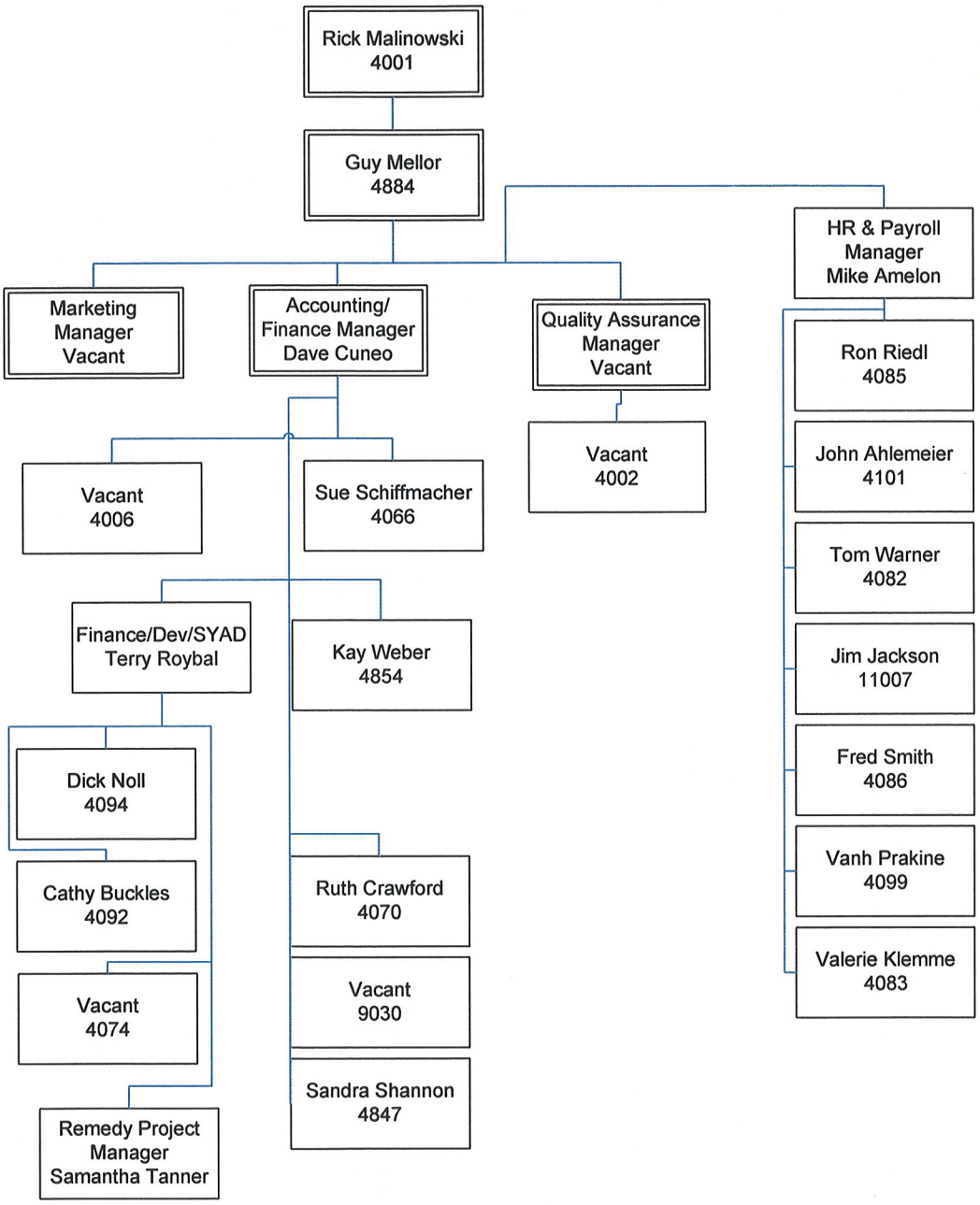


Archives/Admin

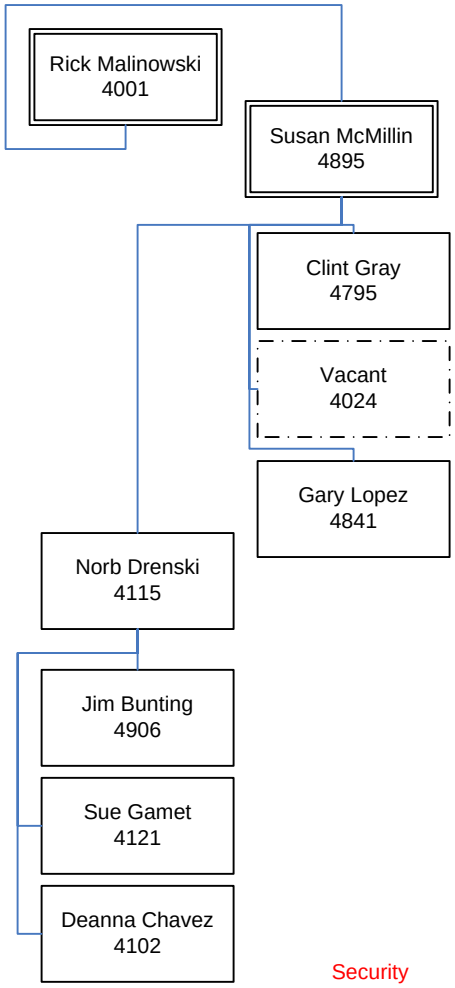

Rick Malinowski
4001
Guy Mellor
4884
Kathy Olivas
4828
1st Shift
Grace Cary
2nd Shift
Mark Fowler
3rd Shift
Linda Barela
James Williamson
4274
Vacant
4554
Vacant
4594
Joe McCormick
4359
Charleston Wimbs
4552
Vacant
4564
Mary Martinez
4823
Dimitri Sangster
4376
Aura Vaculin
4709
Jimmy Rodriguez
4756
Jesse Taylor
4890
Jason Blair
4251
Matthew Castro
4897
Isabel Nuanez
4557
Gerri Trammell
4844
Greg Lym
4744
Vasile Vaculin
4551
Vacant
4555
Vacant
4762
Vacant
4257
Elda Prieto
4748
Celestine Bryant
4600
Braneth Sinaka
4550
Tom Schmidt
4739
Operations

Colorado Department of Personnel & Administration
Division of Information Technologies
Data Center and Technology Management Unit

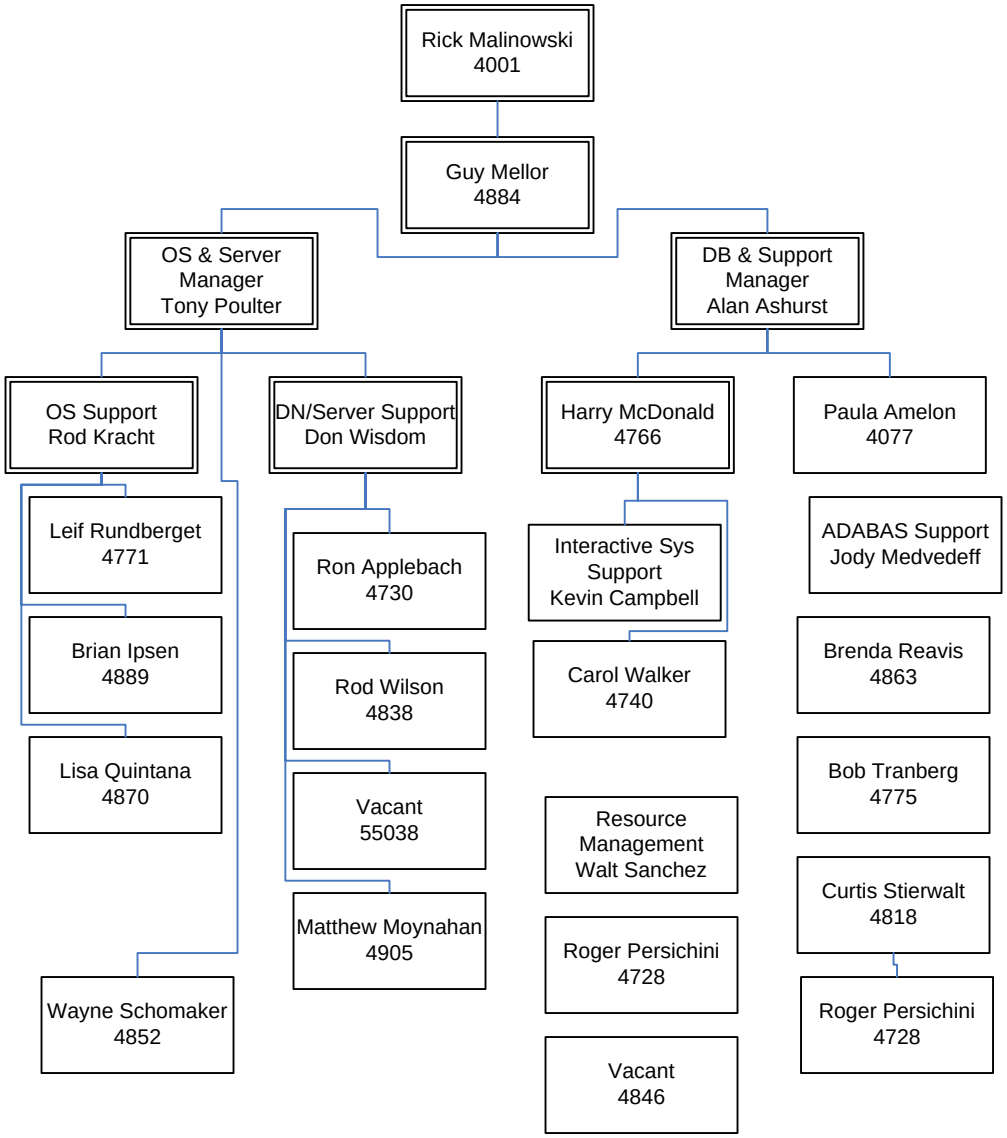
Report on Controls Placed in Operation and Tests of Operating Effectiveness
Period from July 1, 2004 through June 30, 2005



Application Services


Rick Malinowski
4001
Susan McMillin
4895
Clint Gray
4795
Vacant
4024
Gary Lopez
4841
Norb Drenski
4115
Jim Bunting
4906
Sue Gamet
4121
Deanna Chavez
4102
Security

Colorado Department of Personnel & Administration
Division of Information Technologies
Data Center and Technology Management Unit
Report on Controls Placed in Operation and Tests of Operating Effectiveness
Period from July 1, 2004 through June 30, 2005



Technology Management Unit

Organization and Functions

The Technology Management Unit is responsible for acquiring, implementing, operating and maintaining statewide information systems for the State of Colorado. Ten computer software systems meet the definition of "statewide information system" and consequently fall under the responsibility of the Technology Management Unit.

- The **Colorado Financial Reporting System (COFRS)** is the accounting system of final record used by the state of Colorado. All state agencies except Higher Education institutions use COFRS directly to perform their day-to-day accounting functions. Higher Education institutions utilize their own accounting systems, but pass along summarized accounting information to COFRS through interface programs.

- **View Direct/INFOPAC,** licensed from Mobius Management Systems, provides report archiving and management for COFRS reports.

- **The Employee Data Base (EMPL)** tracks the history of all employees, positions and classifications of the state. It implements personnel rules and yearly cost-of-living increases. The system is used by all State agencies, certain Higher Education institutions and the judicial branch of government.

- The **Applicant Data System (ADS)** tracks applicants, employment tests and test schedules and monitors the applicant selection process for all branches of State government except the Legislature. The system allows personnel administrators to monitor the status of applicants throughout the application and testing process and posts job announcements on the Internet. For certain classifications of jobs, ADS develops automated applicant lists.

- The **Colorado Personnel Payroll System (CPPS),** purchased from Integral Systems, Inc., pays approximately 30,000 employees of the State, plus additional Higher Education employees.

- **Financial Data Warehouse (FDW)** provides users with the ability to create their own customized reports and/or views of the data. All data are loaded into the warehouse on a daily basis and are extracted directly from the ledgers.

- **Utility Data Warehouse (UDW)** is a system that is currently under development, parts of which are being utilized by various agencies. This system contains utility bills, payments and other data relevant to energy usage and analysis by state energy managers.

For all applications listed above, activities include the following: (1) application specification, design, programming and modifications; (2) system administration, monitoring and tuning, development of batch JCL and job scheduling; (3) application assurance verification, provision of consultation, help desk, training and documentation services to agencies; (4) development and administration of backup, archiving and disaster recovery programs; and (5) unit and system testing and management of agency extract and interface processes.

Section V
Description Provided by the Division of Information Technologies Data Center and Technology Management Unit

Data Center Overview

As part of the State of Colorado Executive Branch, The Department of Personnel & Administration, Division of Information Technologies operates the State Data Center located in Lakewood, Colorado. The Data Center houses the State's mainframe for traditional legacy systems. It also houses a growing number of servers for State agencies. Customers continue to rely heavily on the Data Center to deliver traditional database processing, online access, tape and disk storage and printing services. The Data Center is housed in a secure facility with 24/7 on-site staffing for operations and Service Center personnel plus environmental controls, fire suppression system, uninterruptible power supply (UPS), generator backup and adequate space for additional equipment.

Data Center customers continue to move to new technologies and the Division of Information Technologies is partnering with them to deliver state-of-the-art IT solutions. In particular, the Data Center is helping customers expand their distributed systems by developing more capability in the area of "virtual servers" and "web enablement" technologies. The total number of servers housed at the Data Center grew from a total of 128 in fiscal year 2001–2002 to 176 in fiscal year 2002–2003, a 38% increase. A server consolidation effort was undertaken in fiscal year 2003–2004 to reduce the number of physical servers through the use of virtual servers that can host multiple applications on one "box." As of fiscal year 2003–2004, the total number of servers hosted at the Data Center has now been reduced to 152.

Data Center Physical Facilities

The Data Center has 9,075 square feet of raised floor space containing the computer room, server farm, office space, Service Center and print and distribution areas.

Power from Xcel Energy is obtained through one power grid, which the Data Center manages with five power distribution units (PDU) and one extension unit. Fail-over power is available through a standby generator located adjacent to the Facility. This generator currently operates at 70% of capacity allowing room for Data Center expansion.

The Data Center is supported by a UPS system to ensure continuous availability of electrical power between the initial interruption of power and the standby generator coming on line. The UPS system operates at 60% of capacity, leaving adequate room for Data Center expansion.

The raised floor environment is adequately controlled with five high-capacity air conditioning units and three humidifiers. In the fall of 2003, the Data Center's halon fire suppression system was replaced to accommodate the ozone-friendly FM-200 extinguishing agent.

Mainframe

The Division of Information Technologies managed, operated and maintained an Amdahl Millennium 785 mainframe processor until April 2003. This Amdahl mainframe utilized eight engines and provided 497 million instructions per second (MIPS), 1 GB each of central and extended memory, 48 Enterprise Systems Connection (ESCON) channels and 32 parallel (132-wire copper) channels. The system included 1.7 terabytes (TB) of disk space.

In April 2003, the Amdahl was replaced with an IBM z800 Enterprise Server with Integrated Facility for Linux (IFL). The z800, rated at 500 MIPS, runs the z/OS 1.4 operating system in one parti-

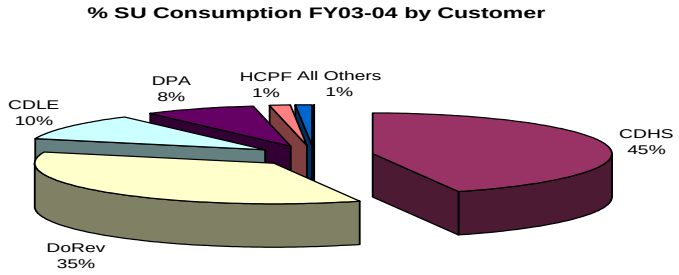
tion and VM/Linux in the other partition. The z800 not only has four times the previous mainframe memory but also has 30% additional power for implementing virtual servers.

The IBM z800 provides the processing capacity sufficient for our current and near-future anticipated workload. The new mainframe expands processing memory capacity from 2 GB to 8 GB. In addition, the IFL component provides the facility the means by which multiple distributed system servers can be aggregated into the architecture without acquisition of additional physical servers. Together, the IBM z800 and the IFL allow personnel to work in compliance with the Colorado Statewide IT Plan fiscal year 2003–2006 by implementing an Enterprise Server (mainframe) architecture that continues to provide support for aggregated legacy mainframe processing while supporting aggregated distributed system processing.

Mainframe CPU availability continued to improve from 98.8% in fiscal year 2001–2002 to 99.86% in fiscal year 2002–2003 and 99.99% in fiscal year 2003–2004.

CPU Consumption

CPU, CICS and ADABAS service unit (SU) consumption on a statewide basis for the last fiscal year is depicted in the following figure:



The leaders of total service unit usage on a statewide basis have not changed for several years and that is expected to continue. The Department of Human Services continues to be the leader in total service unit consumption with 40% and 45% for the last two fiscal years, respectively. The Department of Revenue has remained the second-largest user over the past two fiscal years with consumption of 35%. Department of Labor and Employment has remained the third-largest user with 12% and 10%, respectively. The Department of Personnel & Administration remains the fourth-largest user with 9% and 8% since fiscal year 2003.

Server Hosting

Server hosting is a service that has grown and will continue to grow as state agencies choose to let the Division of Information Technologies perform the care and maintenance of their servers in the Data Center server farm. The Division of Information Technologies is analyzing and implementing server consolidation options through such platforms as Linux under z/VM and VMware for Intel platforms in an effort to reduce costs by sharing hardware equipment among state agencies. The Data Center provides a range of server support levels ranging from floor space (power and network

connections only) to full service hosting (complete operating system and application package installation). To support its growing server hosting services, the Data Center has invested in SAN (Storage Area Network) technologies, enterprise-class backup solutions such as dedicated backup infrastructure and automated tape libraries and effective physical support features such as KVM switches, multiple-zoned power feeds, protective racks and cabinets.

The number of servers hosted at the Data Center by agency is illustrated in the table below:

Agency	Fiscal Year 2001–2002	Fiscal Year 2002–2003	Fiscal Year 2003–2004
Department of Human Services	36	80	59
Department of Revenue	24	12	23
Department of Personnel & Administration	47	56	52
Department of Health	4	3	3
Historical Society	3	2	2
Judicial branch	2	2	2
General Assembly	2	2	2
Department of Natural Resources	1	0	4
Department of Public Safety	9	0	0
Department of Corrections	9	3	2
Department of Labor and Employment	0	1	1
Colorado Legislative Council	1	4	2
Total	128	176	152

Storage Overview

Disk

At the beginning of fiscal year 2004–2005, a Hitachi HDS 7700E supplied 1.5 TB of disk storage to the mainframe running z/OS and 500 GB of storage to a Fujitsu Primepower 600 running Solaris 8. Temporary supplemental storage (40 volumes) was supplied to the mainframe by an EMC 8830 owned by CDHS. In the fall of 2004, DoIT acquired a 4-TB EMC Symmetrix DMX1000 to subsume the functionality of the 7700E. Eight hundred GB of the new disk is being set aside for distributed systems and the remainder for mainframe. All data will be migrated from the 7700E and the 8830 to the new DMX subsystem.

Disk online storage usage increased by 6% in fiscal year 2003. The largest users of this service in order are Colorado Department of Human Services, Colorado Department of Revenue, Colorado Department of Labor and Employment and Department of Personnel & Administration, which recorded an increase (decrease) of 4%, (3%), 28% and 4%, respectively. The four major users in this category make up 91% of the total consumption. With the expansion of distributed systems, it is projected that demand for disk space will continue to grow. Additional distributed systems disk storage is supplied by a 500-GB RAID disk unit in a stand-alone cabinet. Numerous servers have dedicated RAID and non-RAID disk drives within their server cabinets.

Tape

Tape storage for the mainframe is provided by the following:

- Two – 3420 (round reel) tape drives (read only)
- Ten – 3480 18-track cartridge drives and an inventory of 21,000 tapes
- Ten – 3590 (Magstar) drives serviced by an automated tape library (ATL) containing 2,750 tapes
- 64 – Virtual tape subsystem (VTS) logical drives with 630 Magstar back store tapes

Tape storage (backup) for distributed systems is provided by a Quantum M1500 DLT ATL consisting of two interconnected units. Distributed systems backup for some DPA servers is managed using the Veritas suite. Numerous other servers have on-board tape devices used for backup.

Storage History

Disk

When the HDS 7700E was acquired in October 2000, it was envisioned that it would be expanded to satisfy virtually all the mainframe and distributed systems disk needs. It was further envisioned that it might provide a kind of storage utility platform that could be parceled out to agencies with distributed systems storage requirements. With the collapsing price structure in the disk storage market, this business model proved to be prohibitively expensive.

When the EMC DMX1000 acquisition was made, it was decided to continue to use enterprise storage to support the Fujitsu Solaris server, since that server has been considered to be our "enterprise" distributed systems solution. Recent indications were that future large scale distributed systems disk requirements would be met by storage solutions other than the DMX. Such solutions can be anywhere from 80% to 95% less expensive in cost per megabyte. In December 2004, a purchase order request was initiated for six terabytes of distributed systems disk using a Dell (EMC) solution that averages $13,500 per terabyte as compared to $60,000 per terabyte on the recent enterprise storage platform (EMC DMX 1000).

Tape

The 3420 tape drives are antiquated and a plan to retire them will be developed this year. The 3480 cartridge technology was originally introduced in conjunction with an STK automated silo. When, after several years, electro-mechanical and media problems became intolerable, that technology was replaced and downgraded to manual-mount mode 3480 drives.

The IBM VTS and Magstar ATL subsystems were introduced to replace the 3480 silos as the mainline tape technology.

The Quantum ATL solution for the distributed systems servers represents relatively recent digital linear tape (DLT) technology and has performed well. Consideration is being given to replacing the installed system with even newer technology.

Storage Management Software and Processes

Disk

Mainframe disk management and billing is handled in large part by in-house routines written to enforce policies that evolved in the absence of cohesive vendor-supplied management methods. CA-ASM2 supplies much of the source data for these housekeeping and billing functions. Full pack backups are performed by CA-ASM2 and DF/DSS. Incremental backups are performed by CA-ASM2. Archiving and retrieval are performed by CA-ASM2/IXR. Space billing is handled through CA-NeuMICS via a user-written interface.

A project is underway to use IBM's SMS and HSM to replace virtually all the housekeeping and backup functions currently performed by CA-ASM2/IXR. This is intended to obviate the need for most of the in-house written procedures. As a result of this implementation, some customer-facing data management policies will change, but many will remain the same.

Server disk management is performed by a combination of manual methods and features built into applications such as MS Exchange with its automatic purge features. Backup is performed by a combination of application utilities, server-level system utilities and cross-system utilities such as Veritas, which is being implemented as DPA's departmental/enterprise server backup solution.

Tape

Mainframe tape management, including vault management, is handled by CA-1. In-house written routines invoke CA-1's expiration and scratch features to enforce locally defined policies. No plans exist to replace or significantly change our mainframe tape management software or procedures. Server tape management is handled by a combination of manual methods for some servers and by catalog/repository for Veritas-managed servers.

Technology Management Unit (TMU)

Within DoIT, the Technology Management Unit is responsible for acquiring, implementing, operating and maintaining statewide administrative information systems for the State of Colorado. All departments and agencies within State government use these data processing systems.

Current TMU Responsibilities

The **Applicant Data System (ADS)** is the applicant tracking system for the State of Colorado. This system tracks job applicants, employment tests and test schedules and monitors the applicant selection process for the State. Developed by State employees in 1992, the system allows personnel administrators to monitor the status of applicants throughout the application and testing process. The ADS system is used for tracking all state jobs, including the judicial branch and Higher Education positions.

In 1998, a separate job announcement system for posting job announcements on the Internet was developed and implemented. In 2003, the system was enhanced to allow applicants to complete job applications over the Internet.

The ADS system is developed utilizing the ADABAS database management system with Natural coding language. The Job Announcement system was developed with Lotus Notes. The job application is a Java-based system utilizing TN3270 emulation to interact directly with the ADABAS system.

The **Colorado Financial Reporting System (COFRS)** is the accounting system of final record used by the State of Colorado. All state agencies except Higher Education institutions use COFRS directly to perform their day-to-day accounting functions. Higher-education institutions have implemented their own accounting systems but interface summarized accounting information to COFRS.

The state licensed two software applications, (1) CORE and (2) the Government Financial System (GFS) from American Management Systems (AMS) in 1989. The State has extensively customized the software and neither the CORE nor the GFS software is maintained by the vendor. The GFS software is maintained by TMU and has been significantly modified and enhanced to meet the specific needs of the State. These modifications preclude upgrading to new versions of GFS.

The original purchase of COFRS was supported by the State Auditor's Office who needed one auditable system to replace the many different departmental systems in place. COFRS was also supported by the State Controller's Office as a single source of data for the statewide financial reports.

The application (GFS) software of COFRS is implemented on the mainframe in COBOL. It uses a VSAM (Virtual Sequential Access Method) file structure. The CORE software (database and file handling routines) of COFRS is implemented in a mixture of Assembly language and COBOL.

The **Colorado Personnel Payroll System (CPPS)** is the payroll system for the State of Colorado. This system was purchased from Integral Systems, Inc. in 1984 and has been modified to meet the rules and procedures for the State, including a benefits sub-system for reporting insurance premiums. The CPPS system is currently supported by TMU for system modifications and vendor supplied software updates.

The CPPS system is developed in the COBOL language using VSAM file structures. Ad Hoc reporting is accomplished using the FOCUS programming language.

The **Employee Data Base (EMPL)** system is the State of Colorado Human Resource system of record. The EMPL system is responsible for maintaining current and historical information on all employees, positions and job classifications. The EMPL system was developed by State employees in 1981 for use by all State agencies, certain Higher Education institutions and the judicial branch of government. Since initial implementation, the software has been heavily modified as State personnel policies have been updated.

The EMPL system was developed using the ADABAS database management system with Natural and COBOL coding languages.

Infopac/Document Direct: Infopac is a document management system used by COFRS, EMPL, CPPS and DPA billing systems. This product was purchased from Mobius Management, Inc. in

late 1995 and implemented in early 1996. Infopac replaced an American Management System report distribution product. It added the feature of on-line viewing of reports using a 3270 emulator. In the summer of 2000, Document Direct for the Internet was purchased to allow users the ability to view reports using a browser and also to print at their local desktop.

FDW (Financial Data Warehouse) is a research and reporting tool for selected COFRS tables and all COFRS accounting, budget and grant transactions. This system was developed in 1999 and went live in January 2000. The system allows users to see summary information by year-to-date, accounting period or daily amounts and then, if needed, the users can drill down into the detail transactions that make up the balance.

FDW uses the Information Builders, Inc. (IBI) WebFocus reporting tool. The database is Microsoft SQL Server 2000 and the web pages were built using active server pages. The database is loaded daily with COFRS transactions and tables.

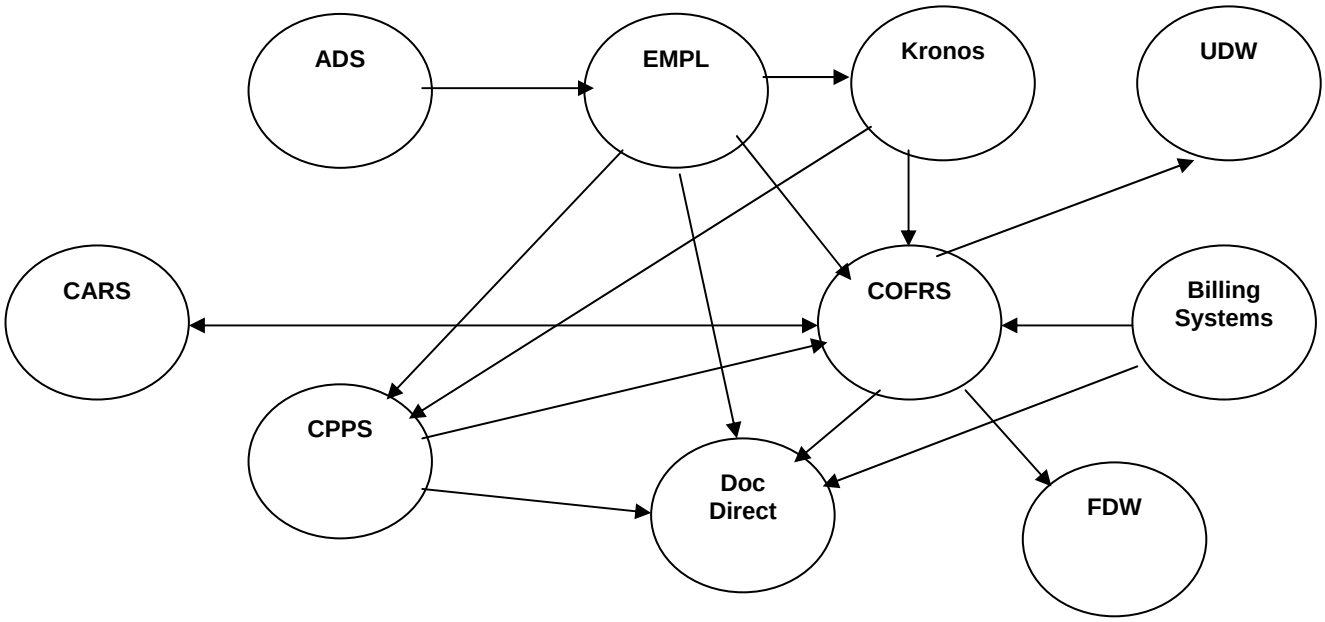
KRONOS – is a vendor-provided timekeeping/leave tracking system. The KRONOS system was implemented in July 2001 as a result of a New Century Colorado (NCC) recommendation that the State of Colorado implement a statewide system to centralize labor force timekeeping and seek consistent standards and compliance in performance, accuracy and accountability.

The Department of Human Services implemented a version of KRONOS in 1996–1997; the Department of Labor and Employment implemented an upgrade in 1998–1999. The Department of Public Health and Environment in July 2001 and the Department of Natural Resources implemented a statewide version of KRONOS and upgraded to the current version in April 2003. The Department of Labor and Employment joined the statewide system in April 2004; the Department of Personnel & Administration implemented it in July 2004. Several other departments and agencies are just starting the process of implementation.

UDW (Utility Data Warehouse) – was a secondary project that was incorporated into the COFRS Electronic Data Interchange (EDI) project. Originally, the COFRS EDI was an effort to receive electronic invoices, automate the generation of a COFRS payment voucher and send an EFT payment with an addendum record that would include the vendor's invoice number, account number, amount and description back to the vendor. Public Service Company, now Xcel Energy, was our partner for the EDI project and when it was learned that the Department of Human Services was receiving some electronic files on energy consumption, a UDW was constructed that would benefit the whole State.

Relationships between Supported Systems

These systems are interrelated through interfaces and extracts, shown below.



Systems Moved to DPA Support Team now known as ITU (Information Technology Unit)

On July 1, 2004, TMU responsibilities were redefined to include only statewide information systems. The responsibility for the support of DPA-only systems was directed to the DPA Executive Director's office. Of the traditional systems supported by TMU, CARS, BIDS and billing services were moved to DPA EDO.

- The **BIDS System** was developed by TMU staff for the Division of Purchasing in 1996 and 1997. It provides a means for agency purchasing staff to advertise bidding opportunities on the Internet and facilitates the distribution of bid information to interested vendors.

- The **Billing Systems** collect information about work performed for other State agencies by various DPA divisions, automatically invoices this work and interfaces (submits) the invoices to COFRS. This system also provides detailed information from the invoices to departments and agencies.

- **Colorado Automotive Reporting System** (**CARS)** integrates all aspects of management and billing of the State's vehicle fleet. Built in 1997 and 1998 by Central Services contractors and TMU staff using a relational-object database, CARS identifies vehicles nearing the end of their useful life that require replacement, analyzes vendor bids for new vehicles, creates purchase orders, expedites vehicle enrollment into the fleet, assigns vehicles to agencies and performs billing. It also collects and analyzes incidence and cost information about accidents, repairs and vehicle maintenance.

Controls and Processes Now in Place

ADS – The Applicant Data System (ADS) is an in-house developed system utilizing an ADABAS DBMS and Natural coding language. TMU staff works in conjunction with the Division of Human Resources (DHR) for technical as well as functional support for the system. All requests for modification to the system are funneled from agency personnel through a DHR representative to ensure system integrity. DHR personnel are responsible for the review and prioritization of all requests and the testing and approval of requests when complete. All requests are passed to TMU management, in writing, utilizing the TMU work intake form.

COFRS software is highly customized to meet customer requirements and is no longer on a vendor software upgrade path. TMU staff analyzes modification requests received from customers. TMU management determines the appropriateness of requests and prioritizes them. A paper-based software configuration management process is used with a signoff sheet. A software release letter is sent to customers via e-mail and documentation is available on the Intranet.

CPPS – The Colorado Personnel Payroll System (CPPS) is a packaged system purchased from Integral Systems, Inc. TMU staff works in conjunction with the Central Payroll Office to provide technical as well as functional support for the system. All requests for modification to the system are funneled from agency personnel through the State payroll manager to ensure system integrity. The State payroll manager is responsible for the review and prioritization of all requests and the testing and approval of requests when complete. All requests are passed to TMU management, in writing, utilizing the TMU work intake form.

EMPL – The State Employee Database System (EMPL) is an in-house developed system utilizing an ADABAS DBMS and Natural coding language. TMU staff works in conjunction with the Division of Human Resources (DHR) to provide technical as well as functional support for the system. All requests for modification to the system are funneled from agency personnel through a DHR representative to ensure system integrity. DHR personnel are responsible for the review and prioritization of all requests and the testing and approval of requests when complete. All requests are passed to TMU management, in writing, utilizing the TMU work intake form.

FDW (Financial Data Warehouse) – The FDW has daily and weekly load procedures that are launched by the database. Temporary table records are counted and summed, then compared to log files to verify the import was performed correctly. Extract dates are loaded into history files to prevent files from being loaded twice. After the permanent tables and ledgers are loaded, the system assurance reports are run and then the nightly maintenance jobs are processed.

In the first half of 2004, TMU, in conjunction with the Department of Corrections, implemented a disaster recovery site for FDW in Colorado Springs.

Infopac/Document Direct products are maintained by Mobius Management, Inc. The State does not have access to the source code. Infopac has been upgraded to stay current with CICS upgrades on the mainframe and Z OS. Document Direct version 1.3 is no longer supported and plans are underway to move to the current version 2.3.

To add reports and users into the database requires a manual process, meaning that for every report required by a user for either online viewing or print requires an entry into the database.

KRONOS – KRONOS is a vendor-maintained product that DoIT is upgrading with the vendor. The KRONOS system is linked into three statewide systems using imports and extracts. On a nightly basis, daily additions (new employees) and changes to our Employee Database (EMPL) are imported into KRONOS. On a bi-weekly and monthly basis, employee hours and related accounting distributions are extracted from KRONOS and imported into the State's payroll system (CPPS). These hours and accounting distributions are also sent to the State's financial system (COFRS) for redistribution.

UDW – This database is updated in the COFRS nightly cycle with detail information received from Xcel Energy. There are internal controls in place to not load duplicate records and to validate that the load process has updated correctly. These controls also verify that the detail transactions equal the total invoices.

Current Customers and their Requirements

ADS – The ADS system is the applicant tracking system for all Colorado state classified jobs and is composed of three separate systems; the mainframe based applicant data system, the job announcement system and the on-line job application system. The primary customers of the ADS system are the individual department and agency personnel analysts and all applicants for State classified jobs. **COFRS** has approximately 3,500 customers using the application. These include accountants, purchasing agents, inventory clerks, budget analysts, project accountants and grant accountants. The COFRS application attempts to satisfy both the individual business requirements of State departments with very different business needs and the centralized control functions of both the State controller and the State auditor.

COFRS provides a mainframe, character-based user interface. Most users today have come to rely on the graphical interfaces provided by personal computers and web browsers. Customers would like easier access to the COFRS data and the ability to do downloads into spreadsheets and word processing documents. The financial data warehouse (FDW) has met many of these requirements for accounting transaction data but the need is there for future enhancements.

CPPS – The CPPS system is used to process payroll for all Colorado State employees with the exception of those employees employed at the State four-year colleges.

EMPL – The EMPL system is the system of records for all employees of the State of Colorado. It is used by all personnel analysts to record employee information along with each employee's demographic and job information. The EMPL system is also the primary historical system for all employees, positions and class information.

FDW (Financial Data Warehouse) – FDW is used by approximately 800 accountants, budget staff and program managers. This system is used daily by many employees but the heaviest usage is at month-end and fiscal year-end. The State Controller's Office has one staff member who develops specialized reports to meet selected user needs.

Infopac/Document Direct: Currently, COFRS is the largest system on this application with the greatest number of users and reports. CPPS reports were added several years ago followed by EMPL reports. In July 2004, DPA billing reports were added.

KRONOS – The Department of Public Health and Environment, the Department of Natural Resources, the Department of Labor and Employment and Depart of Personnel & Administration are the main users. The Department of Law is conducting a small pilot and the Department of Public Safety has conducted two pilots.

UDW – Originally, there were five departments that supported the development of UDW: the Departments of Corrections, Transportation, Natural Resources, Human Services and Personnel & Administration. Currently, only Department of Human Services extracts information from the database.

Service Levels Currently Offered

ADS – TMU currently provides systems analysis and programming expertise for the ADS system. This includes after-hours monitoring for database and batch system processing.

COFRS – TMU currently provides systems analysis and programming expertise. This includes monitoring and operations support 24 hours a day, seven days a week, problem and data integrity analysis and remediation, modification request analysis and programming, user training and helpline support. The COFRS system is available for use from 7:00 A.M.–6:30 P.M. Monday through Thursday, 7:00 A.M.–7:30 P.M. Friday and 9:00 A.M.–5:00 P.M. on Saturday and Sunday except when special processing (such as monthly close) is scheduled.

CPPS – TMU currently provides systems analysis and programming expertise for the CPPS system. This includes after-hours monitoring for database and batch system processing.

EMPL – TMU currently provides systems analysis and programming expertise for the EMPL system. This includes after-hours monitoring for database and batch system processing.

FDW (Financial Data Warehouse) – This system is available 20 or more hours a day, seven days a week. The only time it is scheduled to be down is during the daily and weekly loads that happen about 4:00AM. This application has to be manually stopped and restarted from time to time because the agents cause the system to freeze. When this happens, users are not able to use the system until it is restarted. The ability to move to the disaster recovery site was very important then and this happened during fiscal year 2004 year-end closing.

Infopac/Document Direct: These systems are scheduled to be available from 1:00AM to 11:00PM daily.

KRONOS – This system is available 20 or more hours a day, seven days a week. Due to an increasing number of users continuing to come on board and the fact that there is particularly heavy usage during the first week of each month, response times and other capacity issues need to be addressed for the long term.

UDW – There is a lack of resources to support this application; however, the load programs continue to run without the need for support.

Stakeholders

ADS – The stakeholders for the ADS system are the personnel directors and personnel analysts at each of the initial departments and the Division of Human Resources, Department of Personnel & Administration.

COFRS – The major stakeholders are the State Controller's Office, state auditors, state budget officers and department controllers and accountants.

CPPS – The stakeholders for the CPPS system are the controllers and payroll officers at each of the individual departments and State payroll manager, Division of Finance and Procurement, Department of Personnel & Administration.

EMPL – The stakeholders for the EMPL system are the personnel directors and personnel analysts at each of the individual departments and Division of Human Resources, Department of Personnel & Administration.

FDW (Financial Data Warehouse) – The major stakeholders are the State Controller's Office, state budget officers and department controllers and accountants.

Infopac/Document Direct – The major stakeholders are the State Controller's Office, state auditors, state budget officers and Department of Personnel & Administration.

KRONOS – The major stakeholders are the State Controller's Office, Department of Personnel & Administration, Department of Natural Resources, CDPHE and Department of Labor & Employment.

UDW – Energy managers from the Departments of Corrections and Human Services and the Governor's Office of Energy Management.

Security Measures Now in Place

ADS – The ADS system is a mainframe system utilizing CA-Top Secret, Natural Security and ADS application level security.

COFRS – COFRS is a mainframe application and access to its files is maintained by the mainframe CA-Top Secret software. Within the COFRS application, each department controller or his designee is the COFRS security administrator for that department. TMU staff provide COFRS security administrator training to the department security administrators. In the absence of trained departmental personnel controllers, the State Controller's Office acts as the departments' COFRS security administrator. COFRS security administrators grant appropriate access to department employees to tables and transactions within the COFRS application.

CPPS – The CPPS system is a mainframe system utilizing CA-Top Secret and CPPS application level security.

EMPL – The EMPL system is a mainframe system utilizing CA-Top Secret, Natural Security and EMPL application level security.

FDW (Financial Data Warehouse) – User ID and password security was developed within this system. Security is configurable at the statewide, department and agency levels. Department controllers must approve all user access.

Infopac/Document Direct – The system comes with User ID and password functionality. Department controllers must approve all user access.

KRONOS – The system comes with User ID and password functionality. Department controllers must approve all user access.

UDW – User ID and password security was developed within this system.

Description of Controls

Data Center

The Division of Information Technologies Data Center (Data Center), formerly the Colorado Information Technology Services Data Center, was originally established as a division in the Department of Administration on July 1, 1978, as a service organization to deliver data processing services to various governmental entities. Today, the Data Center is the result of the consolidation of several data centers over the last 26 years.

The most recent significant organizational changes were made to further unify the division; to better reflect the working relationships within the division; and to reduce perceived span of control and conflict of interest weaknesses in the change management and security administration practices. Specifically, the Pueblo Data Entry Center was moved to the Division of Central Services and aligned with the Integrated Document Factory to create the Document Solutions Group, which provides micrographic, data entry, digital imaging and indexing for database retrieval. Data Network technical services staff and the Data Center technical and operational staffs were combined into a Technical Design and Infrastructure section to recognize the close relationship between processing and networking of information. An enhanced customer center was organized under a single manager in order to provide help-desk service, scheduling, security and problem/change management for all Data Center and network services.

Services performed for State agencies include computer processing, maintaining system software, processing of computer output, statewide telecommunications network, secure housing for customer-owned server and network equipment and ensuring the hardware and operating system can be recovered in case of a physical disaster to the Data Center.

Although the basic mission and objectives of the Data Center have not changed, the overall philosophy pertaining to the use of computer systems has evolved since the Division's creation in 1978. There has been a noticeable change in the type of services requested by Data Center customers. Traditional batch processing has predominately shifted to real-time processing. In real-time processing, users have instant access to the computer through remote terminals connected to the Data Center's computer via telecommunications lines. This change to real-time processing places a greater demand on the Data Center's systems.

Real-time processing helps provide more timely and accurate data and also reduces costs associated with creating and maintaining computer-stored data. Errors are usually detected at the source where

those most knowledgeable about the data can make corrections promptly. Thus, the State saves the time and costs associated with making corrections. Also, in some cases, real-time processing reduces the personnel costs associated with the update and maintenance of data on the computer system. Providing real-time processing to DoIT customers resulted when the Data Center installed and made available high-level programming software packages that are more adaptable and easier for non-IT personnel to use.

The change to real-time processing has also brought about a change in the types of customers using the computer system. Managers, statisticians, research analysts, accountants, clerks and others have ready access to the computer system to enter, update, change and query information.

Additionally, customers are requesting that the Data Center expand its services beyond the realm of mainframe processing. They suggest the Data Center coordinate and facilitate the acquisition and support of computing power regardless of whether the requirements are for mainframe or mid-range processors. Customers would like to access resources from the Data Center on an as-needed basis to provide application programming support, training and new technology expertise. Customers also are utilizing the secure and highly available physical infrastructure of the Data Center for their departmentally-managed mid-range server platforms.

The Data Center has expanded its services well beyond the realm of mainframe processing by coordinating and facilitating the acquisition and support of server-class computing resources. Data Center customers can now receive client-server infrastructure support, web-based application development assistance and new technology consulting. Customers are able to utilize the secure and highly available physical infrastructure of the Data Center and manage their mid-range server platforms themselves or turn over varying levels of control and responsibility for their servers to the Data Center.

Organization and Management

State personnel rules and procedures are followed in all areas concerning the hiring, promotion, leave administration, annual performance management and termination of Data Center and Technology Management Unit employees. Additionally, Department and Division orientation sessions are made available to all new employees. Employees are informed of their respective responsibilities and duties through distribution of the organization chart and job descriptions when changes are made. General project, organization, service levels and service delivery information is shared with employees through regularly scheduled staff meetings.

The management team meets weekly to ensure the consistency of direction and objectives and to address system performance issues. Consistency and control is further addressed through the publication, maintenance and use of standard operating procedures. General performance and service level indicators are captured and reported to customers and Data Center management through automated continuous data capture and reporting.

Controls are further exercised through the defined division of responsibilities: computer operators are prohibited from accessing programs and data, application programmers do not have access to the production environment and security administration is performed by an organizational work unit that reports neither to the technical support nor the operations manager. Further, computer operators, data control staff and schedulers do not perform each other's duties unless it is required due to staff vacancies and is achieved through temporary assignment. Application-specific controls are

maintained by the customer agency and are not part of the Data Center's control environment. Automated enforcement of these controls is regularly reviewed and updated and exception logs reflecting potential attempts to bypass these controls are regularly reviewed.

System Software Support

A formal change management system is used to control and document changes to system software. The methodology includes management assessment of the potential impact to client processing and authorization to proceed only by appropriate personnel. Once authorized to proceed, system software modifications are thoroughly tested and approved before introduction into the production environment. Testing is accomplished through an independent test environment and test plans are used to functionally evaluate all system change modifications. A test environment (disk space partitioned and independent of the operating platform) is provided for testing. There is a formal installation process for production software, an implementation schedule is published to the customers and affected clients are notified via e-mail, telephone, or broadcast message prior to placing a change request into production. Back-out procedures are written so that the system can be returned to its pre-implementation condition if necessary.

Documentation for installed system software products is available and current. During system software testing, conversion and implementation, documentation is generated, updated and archived appropriately. The installation process for system software includes a review/update of all associated documentation.

Access to system software is restricted to authorized system programmers at the Data Center and is controlled through the use of Top Secret security software. System programs that allow the bypassing of normal systems or application controls (e.g., Super Zap) are also protected by Top Secret security and are used only when necessary. Such usage is reflected in security logs for review and event documentation.

Acquisition of new software requires business justification and manager approval. The Data Center will request funding for software products only when multi-customer interest is evident. System software is obtained through competitive bid, RFP or formal sole source processes, assuring acquisition from a reputable software development company and proven product reliability. The inventory of system software is complete, audited periodically against software installed throughout the organization and is kept current.

Application Development and Modification

Modifications to software fall in two categories: problem fixes and functional changes. Separate procedures have been developed and documented to guide the process of performing these modifications. Problem fixes are prioritized at three levels and addressed according to priority. Problem reports relating to data integrity or system assurance receive the highest priority. Normally, problem fixes are given higher priority than change requests.

The Technology Management Unit maintains the client support staff as the starting point for processing problem reports and change requests. Client support staff receives problem reports from the system administration staff and also from users via the COFRS help line. Change requests may be submitted by staff at user agencies also and are generated internally within TMU. Some changes

are mandated by legislative action, while others are required by upgrades in Data Center system software. Client support staff verifies the existence of a problem or need for the change request, writes functional specifications for the proposed modification and conducts internal and external meetings to elicit comments on the proposed changes. Client support staff maintains contact with COFRS users through personal contact, the Controller's Forum, the Colorado Financial Management Association and liaison with State Controller's Office staff.

Within the Technology Management Unit, a group of experienced staff review and approve most change requests. Changes with heavy user impact are also cleared through an appropriate user group. In most cases, TMU staff sign off on change requests is required before programming commences. Problem reports are reviewed by client support staff. If the problem report has several possible fixes or major system implications, these are reviewed and approved by TMU staff prior to being turned over for implementation.

Beyond a functional specification, TMU usually requires some technical design document restating the nature of the modification to be made, the programs affected and how the change will be tested. This design document must be reviewed and signed off by a manager or his designate prior to actual programming. TMU performs unit testing of each program modification and the results of this testing are reviewed. Most fixes are supplemented by further testing by TMU staff. Testing includes any data conversions or data recovery required to implement the new or changed software.

Customer communication regarding application changes takes the form of release letters, documentation and training. Changes affecting users are communicated to COFRS users in advance via release letters e-mailed to clients. If the problem report was submitted by a user, he or she is contacted directly by COFRS help line staff. For more significant changes, documentation and training are offered prior to the implementation date.

Final review of functionality, unit tests and acceptance tests are performed by client support staff prior to turning the modified software over to the COFRS system administration group for actual implementation.

Documentation for each problem fix or change request is collected in one or more project folders. The documentation includes the functional design, results of the review, design documentation, documentation of the unit and acceptance tests and changes in user documentation. This documentation is stored on-site for three years and is subsequently archived. Access to the documentation is made through an on-line problem/change tracking system. Additionally, SYAD maintains special internal documentation for the scheduling software schedules and parameter tables used to administer COFRS.

Computer Operations

Computer Associates scheduling software (CA7) is utilized to schedule the processing of batch jobs. Top Secret is used to restrict access to CA7 to appropriately authorized personnel only. Access to scheduling files is restricted to Data Center scheduling personnel; agencies have access to the scheduling software to schedule jobs for their agency only. Computer operators are restricted from discretionary use of the computer system as personnel from the Service Center (schedulers) control the scheduling and submission of computer application jobs. Actions required from an operator during application processing are therefore minimized.

All operator activities are recorded on the console log and system processing is recorded on the System's Management Facility (SMF). Exceptions to normal operations are reported by schedulers and are published for management review on a daily activity history report. Continual problems are identified and discussed in weekly management meetings.

The automated scheduling system ensures that batch jobs are run on a predetermined schedule and are tracked automatically. Where jobs are irregularly scheduled, schedulers check off jobs as they are completed. Batch jobs that do not run correctly are automatically entered into the system log and are entered into the problem management system (INFOSYS). INFOSYS helps to ensure that problems are recorded and tracked to appropriate resolution.

All data, programs and documentation necessary to restore system and data files are stored off-site. Specifics of the data retention program include critical disk packs being duplicated weekly, system data sets and catalogs being duplicated to tape daily, source program libraries being duplicated daily, and databases for which Data Center staff function as the database administrator (DBA) being backed up to tape each weekday and once during the weekend. The off-site data are physically secured and are accessible to authorized personnel only.

Capacity and performance of Data Center computer resources are actively tracked and recorded through the ongoing, real time usage of the SMF. Tracking options are selected to appropriately track system data to monitor the effective and efficient utilization of the computing system on behalf of the customer's application workload. SMF data is captured and retained in order to support historical analysis and reporting, as well as to generate future utilization projections. Capacity and performance metrics are reviewed regularly by management. Certain information is put in graphical and other more readable format and is made available to requesting customer agencies.

Physical Security

All visitors must enter the building through the front entrance and pass through two secured staging areas that are controlled by building reception. All other building entrances are controlled by cipher lock and are used by employees only. Visitors must check in with reception to pass through the staging areas and complete the roster with their name, time in and whom they are seeing. Visitors must be escorted at all times unless granted specific permission for unsupervised admission. Visitors are assigned badges and must wear them while in the building. Badges must be turned in before leaving the building and visitor time-out is recorded on the roster. All employees must also wear badges while in the building.

The Data Center computing facility is composed of three areas: the print/distribution Room, the computer room and the telecommunications room. A unique-combination cipher lock secures each area. Visitors can enter the computing facility only through print/distribution room. Visitors must complete a sign-in/out roster and obtain permission from the shift supervisor, who confirms the visitor's reason for being in the computing facility.

Cipher lock combinations are changed when an employee terminates. Additional changes are made at management's discretion. A distribution list is used to inform employees of new combinations. Employees must sign the distribution list indicating they received the new combinations. Employees receive new cipher combinations for only those areas to which they are authorized.

Data files, negotiable warrants and authorizing signature images are physically secured as governed by documented procedures. These procedures address the acceptance and transfer of materials (data products or common deliveries) in and out of the Data Center, the software-managed migration of storage between the Data Center and off-site storage and the proper handling and tracking of all negotiable documents and the loading and unloading of authorizing signatures.

The Data Center has an uninterruptible power supply (UPS) system to support the Data Center's raised floor equipment. The Data Center has a generator alternate power source that is connected and operational on the Data Center's power grid. The generator and UPS systems are load tested monthly. The technical support and administration area is provided with power outlets (for desktop computers) that are connected to the UPS/generator backup power supply.

Smoke detectors are located above and below the Data Center's raised flooring and directly linked to the fire suppression system. Below-floor water detection devices are located throughout the raised floor area. State Capital Complex Facilities is the custodian for the Data Center building at 690 Kipling Street, Lakewood, Colorado. The custodian provides central maintenance of the building, including the fire alarms, UPS and generator systems and all cooling facilities. The fire alarms are monitored by the state patrol, who will call the fire department if an alarm is activated. During business hours, certain Data Center personnel also have the responsibility to call the fire department as a secondary notification.

Logical Security

Mainframe

The system security and use standard operating procedure (SOP) provides clear guidance regarding the responsibilities of Top Secret security administrators and the issuance of access permissions. The SOP requires that users be granted access to only those resources necessary and appropriate to user's job duties. All Data Center and Technology Management Unit employees receiving logical access to the mainframe are required to sign a compliance statement, referencing and acknowledging the computer usage and data security policy. Computer security information is also included in the SOP, which each employee is given to retain for personal reference. Security administrators are required to sign an additional statement of compliance referencing and acknowledging their responsibilities relative to Top Secret security administration. Agency security administrators are responsible for granting and revoking agency user's rights to the COFRS application.

The Service Center provides new personnel with access to mainframe software and datasets. New personnel receive a unique access identification (ACID), temporary common password and minimum permission rights as directed by their supervisor based on their particular job level and responsibilities. Employees must change the initial password on their first logon attempt or their account will be suspended. Future permission changes/enhancements require an e-mail from the user's supervisor to the Service Center explaining the reason for the permission change. A checklist for departing employees is utilized by the administrative staff to ensure deletion of user access for departing employees. A checklist for new, promoted and transferred employees is utilized by the administrative staff to ensure assignment of proper user profiles for the various systems.

Top Secret security software is used to control access to all mainframe software and data sets. Permissions are defined by user and controlled through login and password. Top Secret is configured to enforce adequate password controls including minimum length, alpha and numeric character re-

quirements, defined password expiration, minimum re-use of password generation and account suspension/lock-out after minimum failed login attempts. Passwords are not displayed as they are input and are encrypted as they are stored.

Top Secret will disable an account if it is not used within six months and will automatically disconnect a login session if no activity occurs within a defined period. The Service Center can unlock and reset an account only after verifying a user's identity from INSTADATA (additional private information a user provides to the security administrator on account start-up as a means to verify his or her identity). Security violations are logged, reviewed and action is taken to investigate violations. Security profile changes are also logged and periodically reviewed and any unusual items are investigated.

Network

Distributed computing logical control is similarly approached for the network. Windows NT is administered by Data Center staff and agency administrators. Each person is given a user ID and temporary password. Additional access requires justification obtained via an e-mail from a user's supervisor. Personnel owning files can grant sharing and access permissions to other users as they deem necessary; however, directory sharing is not activated on a new user's account. The temporary password must be changed upon account activation (log in).

Network security controls are configured to enforce certain password criteria including minimum length and account suspension after a defined number of failed login attempts. In addition, Windows NT generates logs of certain events and Data Center staff review these logs on a monthly basis including logon/logoff failures, file and object access failures, security policy changes and restart, shutdown and system success/failures.

Summary

The description presented above is designed to provide the reader a brief description of the activities performed by DoIT. DoIT's management believes the activities are appropriate for the services provided.

DoIT's specific control objectives and related control activities are included in Section VI of this report "Information Provided by Service Auditor," and captioned as "Provided by DoIT." Although the specific control objectives and control activities are included in Section VI, they are nonetheless an integral part of DoIT's description of controls.

Glossary of Acronyms

Acronym	Definition
ADS	Applicant Data System
ATL	Automated Tape Library
ATM	Asynchronous Transfer Mode
BCV	Business Continuity Volume
BI/ETL	Business Intelligence/Extract, Transform and Load
BGP	Border Gateway Protocol
BPOP	Boulder Giga POP
CBI	Colorado Bureau of Investigation
CBMS	Colorado Benefits Management System
CDHS	Colorado Department of Human Services
CDLE	Colorado Department of Labor and Employment
CDOR	Colorado Department of Revenue
CDPHE	Colorado Department of Public Health and Environment
CDPS	Colorado Department of Public Safety
CICSP	Customer Information Control System Production
CIN	Colorado Information Network
CIVICS	Cooperative Interactive Video in Colorado State Government
COFRS	Colorado Financial Reporting System
CPOPs	County Points of Presence
CPPS	Colorado Personnel Payroll System
DBA	Database Administrator
DDN	Digital Data Network
DLT	Digital Linear Tape
DoIT	Division of Information Technologies
DNR	Department of Natural Resources
DPA	Department of Personnel & Administration
DOR	Department of Revenue
DPA	Department of Personnel & Administration
DR	Disaster Recovery
DS-1	Digital Signal 1
DSL	Digital Subscriber Line
DST	Daylight Savings Time
DU	Denver University
EFT	Electronic Funds Transfer
EMPL	State Employee Database System
ERP	Enterprise Resource Program
ESCON	Enterprise Systems Connection
FDW	Financial Data Warehouse
FICON	Fiber Connectivity
FLC	Fort Lewis College
FMLA	Family Medical Leave Act
FR	Frame Relay
FRGP	Front Range Giga POP
FTC	FRGP Technical Committee

Glossary of Acronyms

Acronym	Definition
FTP	File Transfer Protocol
GFS	Government Financial System
GMT	Greenwich Mean Time
GUI	Graphical User Interface
HBA	Host Bus Adaptor
HRDW	Human Resources Data Warehouse
IBM	International Business Machines
ICG	International Coordination Group
IML	Initial Machine Load
IPL	Initial Program Load
ISDN	Integrated Services Digital Network
DDN	Digital Data Network
JUNOS	A routing operating system designed specifically for the Internet
KVM	Keyboard, Video Mouse switch
LDAP	Lightweight Directory Access Protocol
LPAR	Logical Partition
MIPS	Million Instructions per Minute
MNT	Multi-Use Network
MUX	Multiplexor
MVS	Multiple Virtual Storage
N20	Natural Application Change Management System
NCAR	National Center For Atmospheric Research
NE	North East
NOAA	National Oceanic and Atmospheric Administration
NOC	Network Operations Center
OC	Optical Carrier
OCIN	Open Colorado Information Network
PAC	Predict Application Control
PDU	Power Distribution Unit
PM	Preventive Maintenance
PROD LPAR	Production – Logical Partition
Q&As	Questions and Answers
RAID	Redundant array of independent disks
SAN	Storage Area Network
SMS	Storage Management System
SONET	Synchronous Optical Network
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSN	Social Security Number
SU	Service Unit
TEST LPAR	Test – Logical Partition
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol /Internet Protocol
TSS	Top Secret Security

Glossary of Acronyms

Acronym	Definition
UCAR	University Corporation for Atmospheric Research
UCB	Unit Control Block
UDP	Utility Distribution Panel
UDW	Utility Data Warehouse
UPSA or D	Uninterruptible Power Supply “A” or “D”
USPS	United States Postal Service
UW	University of Wyoming
VM	Virtual Machine
VSAM	Virtual Storage Access Method
VTS	Virtual Tape Storage
WAN	Wide Area Networking

This Page Intentionally Left Blank

Section VI
Information Provided by the Service Auditor

Findings and Recommendations

Introduction

Our responsibility was to express an opinion about whether

- The description of controls outlined in Section IV and V present fairly, in all material respects, the relevant aspects of the Division of Information Technologies (DoIT) Data Center and the Technology Management Unit's controls that had been placed in operation as of June 30, 2005.
- The controls, as described in the Division of Information Technologies Data Center and Technology Management Unit's description of controls, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and the client organizations applied the internal control contemplated in the Division of Information Technologies Data Center and Technology Management Unit's controls.
- The controls were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives, specified by DoIT management, were achieved during the period covered by our report.

We identified opportunities for improving the controls associated with the Division of Information Technologies Data Center and the Technology Management Unit. This section contains recommendations regarding the effectiveness of controls specified by Division of Information Technologies management.

It should be noted that in most instances, the recommendations are the logical result of an exception noted during the examination. However, a number of recommendations refer to control objectives and activities that did not exhibit an exception during the examination. This is a result of the Division of Information Technologies successfully meeting the objective, but a best practice recommendation is being made to offer improvements to current established controls.

A complete listing of our recommendations from this year's examination and management's responses may be found in Section III – Recommendation Locator.

Provide Centralized Review and Guidance for all DoIT Backups of User Data

DoIT manages the mainframe as well as the statewide information systems that reside on the mainframe such as the Colorado Financial Reporting System (COFRS), Colorado Personnel Payroll System (CPPS) and Employee Data Base (EMPL). DoIT's responsibilities for these statewide systems include data backup and recovery. Some agencies have applications systems and application data on the DoIT-managed mainframe (e.g., Colorado Department of Human Services, Colorado Department of Revenue and the Colorado Department of Labor and Employment); however, the agencies have not contracted with DoIT to back up or restore these application systems or their application data. This responsibility falls on to the individual user agencies in accordance with their own guidelines and specifications. During our review, we noted that some entities responsible for their own data backup were not successful in restoring operations during a disaster recovery test. In other words, DoIT successfully restored the statewide systems on the mainframe at the "hot site," but data and systems restoration was problematic for some user agencies.

Similarly, DoIT provides non-mainframe server housing and hosting services for individual department and agency systems. Data backup and recovery is an additional level of service DoIT can provide to its server housing and hosting clients if these specifications are included in the service level agreement between the agency and DoIT. If an agency does not contract for these additional services, DoIT provides only power and network connections for the user agencies servers and, therefore, has no responsibility for backing up and restoring the data on these systems. Inquiry indicated that the backup processes specified by some departments and agencies lacked continuity and reliability. However, we did not test this as it was outside the scope of this engagement.

Recommendation 1

We recommend that DoIT provide for more centralized review and guidance for backup and restoration procedures for all systems housed and hosted at DoIT. Specifically:

a. For those user agencies that do not contract with DoIT for data backup and recovery services, confirm with all agency managers that the agency has implemented data backup and restoration policies and procedures to provide the required level of assurance that all data systems are successfully being backed up and are capable of being restored. As part of this process, DoIT should inquire whether agencies require any additional assistance from DoIT to ensure that all mainframe and server-based applications and data are being adequately backed up.

b. DoIT should designate or create an appropriate oversight group composed of DoIT and user agency representatives that meet on a regular basis to review consistency of backup and recovery processes for data housed and hosted on mainframe and non-mainframe systems.

Department of Personnel and Administration's Response

Agree. Implementation Date: July 31, 2006.

The Computing Services organization was restructured on April 1, 2006, to meet this need. A new storage management group has been formed and a job announcement has been posted to hire a storage manager.

Implement Regular Data Recovery Testing

Regular testing of backup processes and media is necessary in order to ensure reliable data are available in the event of a disaster or any necessary data recovery process. Although the annual disaster recovery test supplies an excellent benchmark for DoIT to assess data recovery, we believe that conducting the test once a year, as is currently done, is not adequate. We are not recommending multiple disaster recovery tests each year. A lower scale of testing is possible and appropriate and can be performed on a quarterly basis.

We also observed that individual departments are responsible for maintaining and designing their backup testing requirements. We observed a lack of continuity in their processes.

Recommendation 2

We recommend that DoIT implement regular internal data recovery testing on a sampling basis in addition to the formal annual data recovery test. Specifically:

a. Tapes and CD backup materials should be tested on drives other than the creating drives.

b. Such testing should be performed at least quarterly.

c. Testing should be designed in consultation with DoIT and the affected department or agency.

Department of Personnel & Administration's Response

Agree. Implementation Date: June 30, 2006.

Standard operating procedures executed by the storage management group to meet backup service level commitments will be modified by June 30, 2006, to perform the suggested recovery testing.

Segregation of Duties

Systems development life cycle (SDLC) is the process of developing information systems through investigation, analysis, design, implementation and maintenance. SDLC is also known as "information systems development or application development." SDLC is a systems approach to problem solving and is made up of several phases including design, programming, testing and implementation. These functions are a regular component of the activities performed within DoIT in support of COFRS and CPPS, but it was noted during our review that unit and system testing is often the responsibility of an individual or small group of programming staff. Segregation of these duties among separate staff enhances the reliability and control of the SDLC or change management functions.

Recommendation 3

We recommend that DoIT review and enhance segregation of duties among programming and testing staff. Specifically:

a. Management should review the current distribution of duties among programmers in the design and testing of programs.

b. The design and testing of programs should be separate functions within the organization.

Department of Personnel & Administration's Response

Partially Agree. Implementation Date: June 30, 2006.

a. For CPPS, software testing and approval is always required by the requestor of the software change. In most cases, this is a representative from either the central payroll unit of the State Controller's Office or from the Division of Human Resources. In all other cases testing and approval goes back the requesting agency. Resource constraints prohibit the segregation of duties between design and programming. Changes will be instituted to require a design review by management for large or high-impact projects. These changes will take effect not later than June 30, 2006. For COFRS, implementation (the move of software into production) is a separate function.

b. The complete separation of design and testing is not practical because of the maturity of the system, the budgeted level of staff and the volume of work. However, mitigating con-

trols have been implemented. For example, the financial management systems manager reviews and approves design and system testing.

Improve Monitoring of Third-Party Service Agreements

DoIT often obtains the services of outside vendors to augment its functions or provide additional expertise. When contracts for third-party services are below a stated dollar threshold, DoIT is not required to submit the contract for upper management review. For example, this applied to purchase orders executed during the audit period for third-party services related to (1) review, remediation and training of security incidents and intrusion detection; (2) rate refresh and master planning; and (3) assistance with server projects. During our examination, we noted that review and monitoring by DoIT of third-party services that fall under the $50,000 dollar threshold is limited. Because third-party services such as those mentioned above can still be significant, services contracted through purchase orders should include more detail and use vendors that have gone through an approval process. In addition, services obtained under larger-dollar State contracts should be defined with specific service expectations appropriate to the needs of DoIT in the context of the State agreement.

While an appropriate cascade of monitoring controls are specified in Figure 16 of this section, evidence of regular monitoring or the assignment of responsibilities to a designated individual was found to be lacking. Through our review, we found no evidence that there is an individual responsible for monitoring third-party services. This lack of monitoring ranged from review of purchase orders to verification of qualifications to ensuring that purchase order and contract terms appropriately reference security controls and procedures for information systems and networks.

Recommendation 4

We recommend that DoIT improve its management of third-party service contracts by the following:

a. Designating an individual within the organization to manage and monitor all third-party agreements, including those falling below the State threshold for upper management contract involvement. Service level agreement and monitoring criteria in support of control objectives 16.1 through 16.6 should also be included in this individual's duties.

b. Preparing and submitting regular reports to DoIT management regarding the above noted monitoring activities.

c. Defining service levels and monitoring that is appropriate to the needs of DoIT for services acquired under existing State contracts.

Department of Personnel & Administration's Response

Partially Agree. Implementation Date: December 31, 2006.

Currently, this process is being done by several individuals on a risk-based approach. We believe this is an appropriate practice at this time. The Department will review its control objectives and revise them as appropriate.

Centralize the Top Secret Security Administration Function

Top Secret is a software package used to manage security of resources on the mainframe, including COFRS and CPPS. The Top Secret security administration function is currently distributed among users. That is, DoIT manages and assigns Top Secret administrator accounts to departments and agencies. The individual department or agency Top Secret administrators then manage and assign security to users they determine are authorized to access mainframe resources where material applications reside. Control of Top Secret functions is paramount and central to the effective management of COFRS and CPPS application security. Control and monitoring of the usage of these assets, resources and security can be enhanced when the security function is centralized rather than distributed. More detailed and regular monitoring of system security is possible with a centralized approach controlled and monitored by professional DoIT security staff.

Recommendation 5

We recommend that DoIT strengthen the Top Secret security administration function by

a. Considering centralizing Top Secret security administrator responsibilities within DoIT in order to control and monitor usage of assets and assign security. If Top Secret Administrator responsibilities cannot be centralized, then DoIT needs to conduct more regular monitoring and review of Top Secret administrator activities at user departments and agencies.

b. Providing additional Top Secret security administrator training to Security Operations Center staff, including key top management, in order to add depth of knowledge to key security positions and enhance management's ability to manage and monitor operations.

c. Implementing additional depth in staffing of the DoIT Top Secret administrator position to enhance review of security administration and backup of responsibilities.

Department of Personnel & Administration's Response

Agree. Implementation Date: June 30, 2006.

a. The Information Security Operations Center (ISOC) has assumed all TSS responsibility for DoIT at this time except for very basic administration functions such as password resets and access to some datasets, which are performed by the Service Center. The ISOC is working on documenting procedures to formalize these roles.

b. Our primary administrator is registered for advanced TSS training next week.

c. The ISOC has documented several basic procedures and started to train additional personnel. The ISOC has also added more permanent technical personnel and will send at least one other person to training.

Implement Incident Response and Escalation Processes

Daily mainframe violation reports are generated and dispersed to the Top Secret administrator. While these violation reports are dealt with as a part of the position's responsibility, there is no formal review of the logs of daily violations. These logs contain indications of suspicious activity such as failed attempts to gain access to a part of the system to which an individual is not author-

ized. The logs also contain general system integrity events such as password changes and password expirations. Furthermore, a formal incidence response process, approved by management, that outlines what constitutes a violation and what the appropriate steps are to communicate and/or escalate to management and/or the appropriate business process owner does not exist. Such steps are critical to maintaining system security and minimizing security risks.

Recommendation 6

We recommend that DoIT institute documented incident response criteria and response escalation procedures.

Department of Personnel & Administration's Response

Agree. Implementation Date: June 30, 2006.

We have developed and tested incident response and escalation procedures over the past few months. These procedures involve logging all security events that the ISOC investigates in a ticketing system and measuring response time through that system. We are in the process of hiring a contractor to help accelerate this development and to write a formal incident response procedure. We expect to publish draft service level agreements for our customers by June 30, 2006.

Improve Warrant Security

Control procedures are in place to limit access to the inventory of blank checks. There are procedures in place for obtaining a key from the Computer Operations Center. However, once access to the inventory is obtained, there is no physical control restricting access to specific processing periods. This means that unauthorized staff could have access to warrant stock during processing, increasing the risk for fraud.

Recommendation 7

We recommend that DoIT evaluate and improve physical security around warrant stock during processing. This should include tracking individuals who access the Computer Operations Center during defined processing periods and determining whether the purpose of their access was appropriate for warrant processing.

Department of Personnel & Administration's Response

Agree. Implementation Date: May 1, 2006.

Additional controls have been implemented. For example, there is now a combination lock on the vault door accessed by individually-assigned codes. Individual access can be monitored via access logs and access can be verified as to being in response to valid processing activity.

Establish and Monitor User Customer Service Levels

DoIT provides multiple levels of service to department and agency customers, including services related to COFRS, CPPS and technology housing and hosting services. For the housing and hosting services, there are many variations in service expectations among DoIT and DoIT customers. Many service expectations are not well defined. In addition, formal monitoring is not in place to measure or validate the provision and performance of expected services. (Related prior year recommenda-

tions can be found in Section VII, September 2001 performance measure recommendations #1 and #3.) The establishment of service level agreements (SLA) for all DoIT customers can provide a more clear indication of service to be provided by DoIT, clarify residual user responsibilities and assist in SLA performance assessments.

Recommendation 8

We recommend that DoIT implement and track service level agreements for all DoIT clients. Specifically, we recommend the following:

a. Specific services and available service levels provided by DoIT should be reviewed, refined and documented.

b. Service level agreements should be established with all DoIT customers.

c. Service level performance monitoring indicators should be established and reported to the affected DoIT customers.

d. Specific and aggregate service level performance should be reported to DoIT management.

Department of Personnel & Administration's Response

Agree. Implementation Date: April 1, 2006, and ongoing.

The Computing Services organization was restructured on April 1, 2006, to meet this need. An individual has been identified as responsible for establishing service-level performance monitoring and reporting to DoIT management.

Retention of Documentation

The creation of documentation that supports and verifies the completion of control activities is central to monitoring and validating the effectiveness of established controls over time. There are a number of areas in which source documentation was not maintained by DoIT. Missing or incomplete documentation included such things as checklists used to monitor activities for separated or terminated employees, spreadsheets that track annual Top Secret access reviews and documentation of State Controller's Office authorization for manual changes to ledger records in COFRS. The utility of the documentation to the service organization includes the following:

- Provision of source data for management reporting and tracking
- Support for routine and ad hoc inquiries, audits and investigations
- Verification of appropriate completion of required processes
- Staff accountability for required activities

Recommendation 9

We recommend that DoIT institute a process to retain source documents for reference and audit for an appropriate period commensurate with the data. At a minimum:

a. Management should review noted instances of documentation exceptions and take steps to implement appropriate document retention procedures.

b. Train affected staff in the proper handling and storage of source documentation.

Department of Personnel & Administration's Response

Agree. Implementation Date: June 30, 2006.

Source documents will be scanned and kept electronically.

Internal Communication

Communication of key operating and performance expectations and results among DoIT staff and management is an important component of quality management. Instances were observed in which changes to standard operating procedures (SOPs) were not communicated reliably to affected staff. For example, signed approval and review forms for changes to standard operating procedures were not retained after final approval, which limited DoIT's ability to ensure that SOPs were distributed to and reviewed by all affected staff. In addition, meeting agendas and documentation of key points were not consistently distributed after monthly staff meetings.

Recommendation 10

We recommend that DoIT ensure critical information and decisions are communicated and reinforced with affected employees by

a. Implementing a method to ensure distributed SOPs are communicated to all employees.

b. Creating meeting agendas and e-mails reiterating key points or follow-up items for each monthly general staff meeting.

Department of Personnel & Administration's Response

Agree. Implementation Date: June 30, 2006.

When SOPs are published, an e-mail will be sent to Computing Services staff notifying them of the updates. General staff meeting agendas and follow-up comments will be implemented by fiscal year end.

Consistency of Documentation

Consistent and accurate documentation of standard operating procedures (SOPs) is critical to the ability of an organization such as DoIT to perform its responsibilities reliably and consistently. Inherent in the development of SOPs is the need for regular management review to ensure clarity, consistency with current operations, and to identify the need for training on SOP changes and updates. Examples were noted where current practice may not be completely or properly reflected in the SOPs (e.g., documents reviewed did not actually contain a description of the three areas within the Data Center computing facility as referenced in Control Activity 7.4). Regular review of SOP and related policy and procedures should occur upon any change in system or processes, and at least annually.

Recommendation 11

We recommend that DoIT review documentation against control objectives and current operations to ensure consistency with current practice. Specifically, management should

a. Review the standard operating procedures referenced in Figures 7.4, 7.5, 9.1 and 17.31.

b. Perform an annual review of standard operating procedures.

Department of Personnel & Administration's Response

Agree. Implementation Date: June 30, 2006. and ongoing.

a. Review of SOPs 2900 and 8806 will be completed by June 30, 2006. New standard format has already been implemented and is replacing old/varied formats as updates are made.

b. As SOPs are reviewed, the next review date will be set to one year in the future and reviewed annually thereafter.

Consolidate Outage Tracking Systems and Identify Responsible Parties

The ability to track issues to completion and report on issues identified, resolved or pending is an important management tool. There appears to be redundancy between the outage notification and remedy issue tracking systems. This can result in issues not being sufficiently tracked, duplication of effort, and the inability to provide comprehensive reporting and identification of trends. Prior to January 2005, the outage notification system was not in place. It was noted that the system did not track long-term solutions to completion. Responsible parties were not identified for remediation responsibilities. The problem is twofold: (1) there is an overlap in some system functions, and (2) neither system is tracking everything that should be tracked.

Recommendation 12

We recommend that DoIT eliminate the redundancy between the outage notification and remedy issue tracking system by

a. Consolidating outage notification and remedy issue tracking system to track outages and assign responsibility within a single system.

b. Identifying responsible parties to track solutions to completion.

Department of Personnel & Administration's Response

Agree. Implementation Date: April 1, 2006, and ongoing.

The Computing Services organization was restructured on April 1, 2006, to meet this need. An individual has been identified as responsible for the consolidation of outage reporting and defining processes for remedy issue tracking.

Control Objectives, Control Activities, Tests of Operating Effectiveness and Results of Tests

Our examination was restricted to selected services provided to system users by DoIT (DC/TMU) including users of the COFRS and CPPS applications and, accordingly, did not extend to controls in effect at user locations. It is each interested party's responsibility to evaluate this information in relation to controls in place at each user location in order to assess the total system of internal control. The user and DC/TMU portions of the system must be evaluated together. If effective user controls are not in place, DC/TMU controls may not compensate for such weakness.

Our examination included interviews with key personnel, inspection of available documentation and records, and observation of certain security procedures and controls surrounding and provided by the DC/TMU systems. Our examinations were performed as of June 30, 2005, and were designed only to clarify your understanding of the information contained in the attached description. In addition, we applied tests to specific controls to obtain evidence about their effectiveness in meeting the related control objectives, described in this section of the report, during the period from July 1, 2004 to June 30, 2005.

The objective of data processing controls is to provide reasonable, but not absolute, assurance about such things as the following:

- Protection of data files, programs and equipment against loss or destruction
- Prevention of unauthorized use of data records, programs and equipment
- Proper handling of input and output data records
- Reliable processing of data records

The concept of reasonable assurance recognizes that the cost of a system of internal control should not exceed the benefits derived and, additionally, that evaluation of internal control necessarily requires estimates and judgments by management.

Figure 1: Define the IT Strategic Plan			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that the strategic planning process is in place to provide the direction and mandate for helping the business achieve its objectives.	1.1 – Management prepares strategic plans for IT that aligns business objectives with IT strategies. The planning approach includes mechanisms to solicit input from relevant internal and external stakeholders impacted by the IT strategic plans.	Obtained and reviewed DoIT strategic plan for current three-year term.	No exceptions noted.
	1.2 – Management obtains feedback from business process owners and users regarding the quality and usefulness of its IT plans for use in the ongoing risk assessment process.	Obtained and reviewed agendas and minutes for management meetings and observed management meeting.	No exceptions noted.
	1.3 – An IT planning or steering committee exists to oversee the IT function and its activities. Committee membership includes representatives from senior management, user management and the IT function.	Obtained and reviewed Change Review Board agendas and minutes for validation. Noted the attendees and confirmed they are senior management or representatives thereof.	No exceptions noted.
	1.4 – The IT organization ensures that IT plans are communicated to business process owners and other relevant parties across the organization.	Obtained and reviewed CIO Forum documentation as well as various publications from DoIT to its customers and internal employees.	No exceptions noted.
	1.5 – IT management communicates its activities, challenges and risks on a regular basis with the executive director.	Obtained and reviewed relevant documentation from the director of DoIT. Ascertained that this information is disseminated to the governor, governors' staff, executive director, DoIT staff, DPA management team and other partners on a routine basis.	No exceptions noted.

Figure 1: Define the IT Strategic Plan			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	1.6 – The IT organization monitors its progress against the strategic plan and reacts accordingly to meet established objectives.	Obtained and reviewed the strategic plan. Noted that the plan has been revised to meet the established objec-tives.	No exceptions noted.

Figure 2: Define the IT Organization and Relationships			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that the IT organization is responsible for managing all aspects of the system environment.	2.1 – Key systems and data have been inventoried and their owners identified.	Obtained and reviewed the inventory listing of software.	No exceptions noted.
	2.2 – Contracted staff and other contract personnel are subject to policies and procedures, created to control their activities by the IT function, to assure the protection of the organization's information assets.	Obtained and inspected related policy and procedures and ascertained that contracted staff and personnel are subject to DoIT policies and procedures.	No exceptions noted.
	2.3 – IT strategies and ongoing operations are formally defined and communicated to senior management and customer CIOs through periodic meetings of an IT steering committee.	Obtained and inspected meeting agendas, minutes and the multi-year plans and ascertained that DoIT maintains communication links to its customers.	No exceptions noted.
	2.4 – Significant IT events or failures, e.g., security breaches, major system failures or regulatory failures, are reported to senior management or the board.	Obtained and reviewed documentation related to outage notification. Noted all items are assigned an "owner" or responsible party, prioritized, and a date of input and status if assigned or unassigned. No significant security breaches, system failures or regulatory failures were observed.	No exceptions noted.

Figure 3: Manage Human Resources			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
These controls provide reasonable assurance that hiring, training, performance evaluation, job responsibilities, vacation and termination practices are in accordance with established policy and that such policies are adequately communicated to personnel.	3.1 – State personnel rules and procedures are followed in all hiring, training, performance evaluation, job responsibilities, vacation and termination practices.	Obtained and reviewed CO personnel rules and procedures. Validated that they are followed. Obtained blank separation checklist. Obtained and inspected a copy of the terminated employee checklist.	No exceptions noted.
	3.2 – A checklist is used for all departing employees to ensure that separation and termination activities are conducted according to policy.	Obtained and reviewed a copy of the checklist used for termination and separation. Obtained listing of employees terminated or separated from DoIT during examination period. Selected a sample of terminated or separated employees for verification of activities conducted according to policy. Of sampled records, no exceptions noted to using checklist for departing employees as part of policy.	No exceptions noted. (See recommendations #9.)
	3.3 – New employees attend departmental and divisional orientation sessions.	Obtained and reviewed listing of new employees hired during the examination period and inspected sample noting documentation on orientation sessions.	No exceptions noted. (See recommendation #9.)
	3.4 – New employees sign a statement of compliance indicating they have received and agree to the computer usage and data security policy.	Obtained listing of new hires and inspected sample of new hires noting signed statement of compliance.	No exceptions noted.

Figure 3: Manage Human Resources			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	3.5 – Vacation usage is tracked, balances posted and "use or lose" balances are distributed to employees and managers.	Observed demonstration of process of KRONOS used by employees for vacation time tracking. Based on inquiry with HR director, ascertained employees are notified of "use or lose" balances via three different notices for these balances outside of the KRONOS system that can be viewed by employees.	No exceptions noted.
	3.6 – Formal job descriptions exist and are kept current.	Obtained listing of current employees with DoIT and inspected a sample from listing and verified that the job descriptions are current.	No exceptions noted.
	3.7 – A performance appraisal system is in place. Semiannual reviews are required and annual ratings are performed in April.	Obtained and reviewed blank performance management forms for 1) employee, 2) manager, and 3) supervisor. Obtained listing of current employees with DoIT. Inspected sample from listing and verified that appraisals are conducted in the stipulated time period.	No exceptions noted.
	3.8 – An organization chart is published and kept current.	Obtained and reviewed organizational chart for DoIT.	No exceptions noted.
	3.9 – Standard operating procedure (SOP) manuals exist and are used by Data Center and statewide application systems personnel.	Obtained and reviewed SOPs. Through corroborative inquiry with employees, noted familiarity with the SOPs and their application to job duties.	No exceptions noted.

Figure 3: Manage Human Resources			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	3.10 – Employees are trained in accordance with job responsibilities.	Obtained and reviewed training documentation from HR. Ascertained training is specific to level within DoIT. Noted employee must meet job requirements at hire. Noted mandatory training requirements offered by the department as well as customized training for employees.	No exceptions noted.
	3.11 – Data Center staff meetings are held monthly or as deemed appropriate by management. These meetings have an open forum and relevant changes to the organization are presented.	Per inquiry with HR, determined the division director holds three types of monthly meetings: one with the full staff, another with his direct reports supervisors and the last with his direct reports. Inspected documentation maintained for these meetings.	No exceptions noted.

(Figure 4 page intentionally left blank.)

Figure 5: Communicate Management Aims and Direction			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that the established reliable system requires participation from all members of the IT organization.	5.1 – IT management has formulated developed and documented policies and procedures governing the IT organization's activities.	Inspected related policies and procedures and ascertained procedure for creating policies is followed.	Noted that signed approval forms for new SOPs are not retained once final approval is received. No review documents were available. Exception noted. (See recommendations #9 and #10.)
	5.2 – IT management periodically reviews its policies, procedures and standards to reflect changing business conditions.	Through inquiry and inspection of documents, verified that a procedure for review of SOPs every two years is followed.	Noted that signed approval forms for reviewed SOP's are not retained once final approval is received. No review documents were available. Exceptions noted. (See recommendations #9 and #10..)
	5.3 – IT management has communicated policies and procedures governing the IT organization's activities.	Through corroborative inquiry, ascertained that monthly meetings are scheduled and are made available via videoconference so all locations are included. Ascertained that team-building meetings are conducted quarterly.	Noted that no meeting agendas or minutes are created. (See recommendations #9 and #10.)

Figure 6: Assess Risks			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that a risk assessment is defined as "the identification and analysis of relevant risks to achievement of the objectives."	6.1- The IT organization has an entity- and activity-level risk assessment framework, which is used periodically to assess information risk to achieving business objectives.	Through inquiry and inspection, reviewed new project request process and documents. Noted that current process was begun in May 2005. Prior to May 2005, there was no formal process.	Noted process in place at end of examination period. No additional exceptions noted. (See recommendation #9.)

Figure 7: Manage Facilities			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that security and related controls help the service organization maintain the security and availability of their systems.	7.1 – All visitors must enter the DoIT building through the front entrance and pass through two secured staging areas, which are controlled by building reception. All other building entrances are controlled by scramble padlock combination and are for use by employees.	Inspected and verified that the SOP states, "The west door, referred to as the main entrance, is staffed by DoIT personnel during normal workdays. It is to be used by all DoIT/CBI employees and visitors to the facility; except as indicated in the building." Further, the SOP describes the "scramble padlock combination" as access codes. It is noted by observation with DoIT employees, the "scramble padlock combination" is in fact accurately stated as such and working as described.	No exceptions noted.
	7.2 – Employees and visitors must wear badges at all times while in the building.	Read and verified that the SOP states, "All authorized visitors to the computer room will wear their agency/company ID badge or a visitor badge." Through observation and performance, it was ascertained visitors are provided and wear visitor badges.	No exceptions noted.
	7.3 – Visitors must check in with reception to pass through two staging areas and complete the roster with their name, time in and whom they are seeing. Visitors must be escorted at all times unless granted specific permission in person. Badges must be turned in before leaving the building and visitor time out is recorded on the roster.	Obtained, inspected and verified that the SOP states, "DoIT visitors and guest[s] will enter the building and state their business to the Receptionist, and all guests will sign in and be assigned the appropriate badge(s)…all guests and visitors will be escorted to any place in the building." Observed controls in place.	No exceptions noted.

Figure 7: Manage Facilities			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	7.4 – The Data Center computing facility is composed of three areas (print/copy/service center rooms, telecommunications room and the computer room). A unique-combination cipher lock secures each area.	Obtained and inspected SOP and service level announcement. It is noted that while neither document describes the three areas within the Data Center computing facility, inquiry with DoIT employees and observations confirmed that each area has a unique combination cipher lock to secure each area.	No exceptions noted. (See recommendation #11.)
	7.5 – The Data Center has 24/7 operations and someone is on site at all times and would note and investigate any unfamiliar or unusual activity.	Obtained and inspected the SOP for 24/7 operations. Through corroborative inquiry, noted that the Data Center is staffed 24/7.	No exceptions noted. (See recommendation #11.)
	7.6 – Visitors enter the computing facility only through the print/copy room. Visitors must complete a sign-in/out roster and obtain permission from the shift supervisor, who confirms the visitor's reason for being in the computing facility.	Obtained and inspected the SOP. Noted, through observation and experience, that visitors sign roster and are escorted with notification by escort the reason for the visitor to be in the print/copy room.	No exceptions noted.
	7.7 – Cipher lock combinations are changed when an employee terminates. Additional changes are made at management's discretion.	Obtained and inspected termination documentation and cipher lock sign-in sheet, and ascertained that the combinations were changed following the last termination.	No exceptions noted.

Figure 7: Manage Facilities			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	7.8 – A distribution list is used to inform employees of new combination changes. Employees must sign the distribution list indicating they received the new combinations. Employees receive new cipher combinations for only those areas to which they are authorized.	Obtained and verified the listing of employees who have access to specified restricted areas. Noted that employees must initial that they have received the new combinations. Noted the listing also indicates the new combination and when the combination will be changed.	No exceptions noted.
	7.9 – There are standard procedures for accepting and transferring materials (data products or common deliveries) in and out of the Data Center.	Obtained, inspected and verified the SOP noting the procedures for accepting and transferring of materials. Observed the dock area for this type of action. Dock area is monitored by cameras for any suspicious activity.	No exceptions noted.
	7.10 – The computing facility is equipped with smoke detectors located above and below the raised flooring and are directly linked to the fire suppression system.	Verified through observation that the Data Center is equipped with smoke detectors located both on the ceiling and below the floor tiles. Through inquiry, determined the detectors are linked to the fire suppression system in the event of an incident.	No exceptions noted.
	7.11 – The computing facility is equipped with an FM200 gas fire suppression system.	Verified through physical observation that the Data Center is equipped with FM200 gas as the fire suppression system.	No exceptions noted.
	7.12 – The gas fire suppression system is inspected annually by a third-party service and it has an automated monitoring system that is checked regularly by Data Center personnel.	Obtained, inspected and verified documentation noting that the FM200 has been inspected regularly.	No exceptions noted.

Figure 7: Manage Facilities			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	7.13 – Climate controls are installed in the Data Center.	Observed through physical inspection of the Data Center that climate controls are installed in the three main areas.	No exceptions noted.
	7.14 – The Data Center has an uninterruptible power supply (UPS) system with a generator alternate power source, which is connected, and operation on the Data Center's power grid.	Observed through physical inspection that the Data Center has an uninterruptible power supply system in place.	No exceptions noted.
	7.15 – Central monitoring of the building fire alarms is provided by State Patrol headquarters, who will notify the fire department if an alarm is activated.	Verified, through corroborative inquiry with management as well as staff at Capital Complex, that the responsibility for alarm notification is monitored by State Patrol headquarters and that the State Patrol monitors all aspects of the building.	No exceptions noted.
	7.16 – The second floor is provided with power outlets (for personal computers) that are connected to the UPS/generator backup power supply.	Observed and noted during physical walk-through the specified outlets noted for UPS/generator backup power in the event it is needed.	No exceptions noted.

(Figure 8 page intentionally left blank.)

Figure 9: Manage Quality			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that quality programs address both general and project-specific quality assurance activities and should prescribe the type(s) of quality assurance activities (such as reviews, audits, inspections, etc.) to be performed.	9.1 – The service level manager researches all known major system outages, completes an outage notification and distributes it to senior management.	Samples of the outage notification forms were obtained and reviewed. Use of the outage notification form began in January 2005. No formal tracking was performed prior to January 2005. Reviewed copy of tracking form sent to senior management on a monthly basis.	While outage notification is provided to senior management, the tracking form did not track long-term solutions to completion, nor were parties responsible for remediation identified. No additional exceptions noted. (See recommendations #11 and #12.)
	9.2 – A monthly executive dashboard is completed and posted on the division intranet site.	Viewed executive dashboard on intranet and inspected printed copies of the current month.	No exceptions noted.
	9.3 – An annual Top Secret access review for Computing Services is completed.	Inspected TS audit notebooks and obtained samples of manager approval forms and a copy of one user's access printout. Noted that a spreadsheet is to be kept during the review process to ensure manager's approval of all employees' forms.	A copy of the spreadsheet was not kept. Exception noted. (See recommendation #9.)

Figure 10: Acquire or Develop Application Software			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that application and system software is acquired or developed that effectively supports financial reporting requirements.	10.1 – Documented procedures have been developed and are followed in the requisition, bidding and purchase of new utilities software.	Inquired with administrative/finance & HR Manager and inspected procurement request for over $5,000 purchase during test period. Reviewed a purchase requiring an RFP and bid. Reviewed procurement for purchases under $5,000.	No exceptions noted.
	10.2 – Appropriate justification and management approval is required before the acquisition of new utilities software.	Through inquiry with administrative/finance & HR manager and inspection of documentation, noted that the required justification was supplied for selection of software. Inspected documentation of software purchases during the test period was met. Ascertained that the controls are operating as designed.	No exceptions noted.

Figure 11: Acquire Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that technology infrastructure is acquired so that it provides the appropriate platforms.	11.1 – System management facility (SMF) recording options are appropriate to capture and monitor capacity and performance.	By inquiry and observation with technical support manager and review of SNF SYS1.PARAMLIB, noted the SMF recording options are sufficient to capture and monitor mainframe platform performance.	No exceptions noted.
	11.2 – Data Center personnel review SMF information on a regular basis.	By inquiry and observation with technical support manager, noted that Data Center personnel are alerted to critical events.	Documentation to confirm that reviews were actually performed was not noted. Exception noted. (See recommendation #9.)
	11.3 – SMF data capture is retained and presented in graphical format for management review.	Viewed computing services dashboard and noted the document displays system resource use and parameters in a graphical format.	No exceptions noted.
	11.4 – A NetMan server (SNMP Manager) monitors NT, UNIX and the mainframe for availability. If a system is unavailable, Service Center personnel notify the network support group, who use Event Viewer (log viewing program) to access server logs to identify the problem.	Performed inquiry, observation and walk-through of network operations center (NOC). Inquired of NOC personnel on chain of events to resolve NetMan events. Reviewed screen prints of NetMan for current events.	No exceptions noted.

Figure 12: Develop and Maintain Policies and Procedures			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that policies and procedures that define required acquisition and maintenance processes have been developed and are maintained, and that they define the documentation needed to support the proper use of the applications and the technological solutions put in place.	12.1 – Hardware acquisitions include pre-paid maintenance and support is renewed in COFRS at the beginning of each fiscal year.	Obtained and reviewed documentation noting pre-paid maintenance and support for COFRS. Per inquiry with internal HR, this information has been noted on the documents received as supporting information.	No exceptions noted.
	12.2 – Software acquisitions include annual support and are renewed in COFRS at the beginning of each fiscal year.	Obtained and reviewed documentation noting pre-paid maintenance and support for COFRS. Per inquiry with internal HR, this information has been noted on the documents indicating when maintenance and support is to be paid and in what amount.	No exceptions noted.

Figure 13: Install and Test Application Software and Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that the systems are appropriately tested and validated prior to being placed into production processes and associated controls operate as intended.	13.1 – A formal change-management methodology is used to control and document changes to application software.	By inquiry and observation with the manager of HR/Payroll Systems and the financial systems manager, reviewed process for change management. Noted that the department currently uses an in-house MS Access database to track and manage change requests and that this system is being migrated to the Remedy platform. Ascertained that the change management system functions in similar fashion for COFRS, CPPC and mainframe platform software, differing only in the details in that COFRS changes are managed using the TMU request form, CPPS changes are managed by the State Controllers Office (SCO) that are forwarded to CPPS personnel for action and DPA/DoIT changes require a project proposal form that tracks the project.	No exceptions Noted.
	13.2 – Client support staff identify, analyze and evaluate the functional specifications and user requirements by conducting internal and external meetings to elicit comments on proposed changes.	Reviewed methodology of current MS Access database used to track changes during the test period, noting staff sign-off is required for each stage of the process.	No exceptions noted.

Figure 13: Install and Test Application Software and Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.3 – Proposed changes to software are reviewed and approved prior to modification of source code.	Reviewed methodology of current MS Access database used to track changes during the test period. Inspected a sample of randomly selected change requests and noted user and staff sign-off and approval are required for each stage of the process.	No exceptions noted.
	13.4 – Upon completion of software changes, software modifications are tested and formal acceptance is granted.	Reviewed methodology of current MS Access database used to track changes during the test period. Noted unit and system testing are performed by programming staff. Reviewed a sample of change requests randomly selected from the test period, noting staff sign-off and approval are required for each stage of the process. It was noted through inquiry of manager of HR/Payroll Systems and the financial systems manager that because programming staff has extensive knowledge of software systems, their processes do not require user sign-off prior to implementation.	No exceptions noted. (See recommendation #3.)
	13.5 – Managerial or Requestor review of functionality, unit testing, and acceptance testing is performed prior to implementation.	Though inspection of a sample of randomly selected change requests and the MS Access database, noted that management review of unit and system testing are documented in the MS Access database.	No exceptions noted.

Figure 13: Install and Test Application Software and Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.6 – Manual controls are used to ensure the correct version of software is being modified. These include • Separate development, test and production libraries • The source code is copied directly from production and used to make the modifications • The modified source code is then moved, not copied, from development to test and then to production	Through review of a sample of TMU documents, noted that the system administrator (COFRS) signs off project checklist after verifying code and moves software to production, and noted that for CPPS changes are implemented at the request and direction of SCO.	No exceptions noted.
	13.7 – Complete application documentation and user manuals are maintained and updated, as appropriate, to reflect modifications made to the application.	Through review of a sample of TMU documents, noted that, for COFRS, documentation changes are signed off on the project checklist, and for CPPS, documentation is maintained by SCO as part of SCO control of CPPS system. Viewed associated documentation maintained online.	No exceptions noted.
	13.8 – Clients are notified of changes to the application if it will affect their interaction with the application.	Through corroborative inquiry, ascertained that e-mails are required by TMU request form and that e-mails are generated and sent to all affected clients (agencies) prior to a change being implemented. No historical e-mail examples available.	No exceptions noted. (See recommendation #9.)
	13.9 – A formal change management system is used to control and document changes to system software.	Reviewed TMU requests and DPA/DoIT project proposal samples.	No exceptions noted.

Figure 13: Install and Test Application Software and Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.10 – Prior to modifying system software, the modifications are authorized by appropriate personnel.	Reviewed completed TMU requests and DPA/DoIT Project proposal samples and noted appropriate signatures appear in the required sections of the documents.	No exceptions noted.
	13.11 – System software modifications and additions are thoroughly tested and approved before introduction into the production environment.	By inquiry and observation, noted that software changes (primarily reports, jobs and database changes) are assigned to a programmer for testing and implementation.	No exceptions noted. (See recommendation #3.)
	13.12 – An independent test LPAR residency (partitioned disk space separate from the operation's partition) and test plans are used by software programmers and clients to functionally evaluate system change modifications.	Obtained and inspected a complete system configuration of the Z/390 mainframe and validated the existence of an LPAR used for testing and development. Through inquiry, we discerned that development and testing was conducted within the confines of the aforementioned LPAR.	No exceptions noted.
	13.13 – An implementation schedule is published for the customers.	Through corroborative inquiry, ascertained that e-mails are required by TMU request form and that e-mails are generated and sent to all affected clients (agencies) prior to a change being implemented. No historical e-mail examples available.	No exceptions noted.
	13.14 – Affected clients are notified via e-mail, telephone, or broadcast message prior to placing a modification into production.	Through corroborative inquiry, ascertained that e-mails are required by TMU request form and that e-mails are generated and sent to all affected clients (agencies) prior to a change being implemented. No historical e-mail examples available.	No exceptions noted.

Figure 13: Install and Test Application Software and Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.15 – Prior to implementation, management assesses the impact of systems software modifications to client processing.	Reviewed DoIT SOPs and completed TMU request forms including user sign-offs and noted the process is completed online.	No exceptions noted.
	13.16 – Back-out procedures are written to return the system's configuration back to its pre-implementation condition.	By inquiry, observation and inspection of SOPs and resulting documentation, noted back-out procedures are mandated prior to any implementation rated at a risk level 1 or 2.	No exceptions noted.
	13.17 – Documentation for system software products is available and current.	Reviewed software inventory and noted inventory list is being checked against in-use systems for currency.	No exceptions noted.
	13.18 – The installation process for system software includes a review/update of associated documentation.	Through inquiry, observation and review of SOPs, ascertained that software documentation is updated and maintained on line.	No exceptions noted.
	13.19 – The inventory of systems is updated for system software modifications.	Obtained and reviewed the inventory listing of software.	No exceptions noted.
	13.20 – All interfaced transactions by agencies to COFRS/CPPS require advance authorization from the State Controller's Office (SCO).	Though inquiry and inspection of requests for interfaces, determined that COFRS/CPPS Interfaces are managed at SCO.	No exceptions noted.
	13.21 – A user ID and password are required to enter or modify transactions in COFRS, CPPS and payroll systems.	Observed process requiring login and sign-on to modify transaction within COFRS, and noted that CPPS transactions are modified at SCO level.	No exceptions noted.

Figure 13: Install and Test Application Software and Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.22 – One person in each agency is appointed as the agency security administrator. The agency security administrator has update rights for only users in their agency on the main security table for COFRS, the ASEC table.	Reviewed lists of agency security administrators. Through interview, observation and programmatic testing, noted each department has a designated TSS security administrator who has access to add and remove users to his or her assigned department facility only.	No exceptions noted.
	13.23 – The 1RC01R reports in COFRS are generated and are available to agencies so they can monitor the number of transactions received in each agency interface file and to determine if they were received on a timely basis and were properly authorized.	Reviewed JCL scripts for 1RC01R reports.	No exceptions noted.
	13.24 – Errors detected in COFRS/CPPS input cannot be processed until the user corrects them online.	By inquiry and observation with the manager of HR/Payroll Systems and the financial systems manager, reviewed procedures and ascertained CPPS transactions are handled at the SCO/agency level and COFRS transactions are performed at DoIT. Ascertained that inputs are not processed until transactions are correct.	No exceptions noted.
	13.25 – The CORE supervisory routines require that all transactions be edited and approved prior to acceptance in COFRS.	By interview and observation with the financial systems manager and review of procedures, ascertained that inputs are not processed until transactions are correct.	No exceptions noted.

Figure 13: Install and Test Application Software and Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.26 – Batches are rejected in COFRS if the transaction count and total amount of the batch do not match the proof totals.	By interview and observation with the financial systems manager and review of procedures, ascertained that transaction/batch counts must total.	No exceptions noted. (See recommendation #9.)
	13.27 – In the rare case that a transaction is clearly erroneous and prevents balancing of the ledgers, statewide application services staff will manually modify the ledger record. The statewide application service maintains a manual log detailing all such changes. A representative of the State Controller's Office authorizes all changes to the ledgers in writing.	By interview and observation with the manager of HR/Payroll Systems and the financial systems manager and review of procedures, ascertained that SCO representative must authorize changes. No examples retained from the test period.	No exceptions noted. (See recommendation #9.)
	13.28 – The SUSF table in COFRS displays the current status (accepted, waiting for approval, on hold or failed edits) of all transactions for five days after acceptance and holds all unaccepted transactions for six months.	By inquiry and observation with the manager of HR/Payroll Systems and the financial systems manager reviewed procedures, ascertained CPPS transactions are handled at the SCO/Agency level and that COFRS transactions are performed at DoIT. Ascertained that inputs are not processed until transactions are correct.	No exceptions noted.
	13.29 – Transactions have a unique ID and users are not able to enter two transactions with the same transaction ID within the same accounting period.	Reviewed account transaction IDs and noted IDs are edited against an ID table, batch numbers are unique and IDs must be unique during accounting period.	No exceptions noted.

Figure 13: Install and Test Application Software and Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.30 – All critical programs in the nightly cycle issue termination codes identify any processing errors detected by the program. Condition code checking in the JCL and CA7 prevents further processing after serious errors have occurred.	Reviewed screen print of jobs running and associated error codes. Observed that processing stops. Reviewed example involving entry of wrong accounting code that put system out of balance.	No exceptions noted.
	13.31 – Each morning, system analysts review system assurance reports, which compare balances, and other reports, which will indicate that transactions were processed completely and accurately.	By inquiry and observation, observed that COFRS system administrator reviews daily logs. By inquiry and observation, observed that CPPS SCO personnel review daily logs. No logs retained from test period as documentation is not retained after review.	No exceptions noted.
	13.32 – The Data Center maintains a record of each printed warrant number and before printing a new batch of warrants, a computer center operator must visually verify the starting warrant number.	By inquiry and observation, reviewed warrants in vaults, warrant check-out logs, warrant use logs and warrant exceptions (misprints, etc.).	No exceptions noted.
	13.33 – EFT information is transmitted to the bank via a private network during nightly processing.	By inquiry and observation, confirmed that data are transmitted to bank when required by processing. Amounts are validated by bank with SCO office as independent control.	No exceptions noted.

Figure 13: Install and Test Application Software and Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.34 – Table and ledger extracts are prepared by COFRS programs and file extracts are prepared by HR/payroll programmers each night on the Data Center mainframe. Agencies are responsible for importing, storing, or otherwise disposing of extract files before they are overwritten by the next set of extracts.	By inquiry and observation, confirmed that files are prepared each night. Confirmed that it is the responsibility of each agency for disposition.	No exceptions noted.
	13.35 – Reports are printed via INFOPAC and distributed to user agencies the next business day. User agencies review reports for accuracy.	By inquiry and observation, confirmed that files are prepared each night. Hard copy reports are shipped to requesting agency for review.	No exceptions noted.
	13.36 – Weekly COFRS and CPPS reports are made available to user agencies so that agencies can review the reports for accuracy and completeness.	By inquiry and observation, confirmed that files are prepared each night. Hard copy reports are shipped to requesting agency for review.	No exceptions noted.
	13.37 – Batch balancing is performed and the system verifies resultant (output) reports by matching them against the input data and control totals.	Obtained and reviewed system assurance reports.	No exceptions noted.
	13.38 – All reports are logged prior to distribution.	Obtained and reviewed document direct and interviewed manager. Observed logs of document distribution.	No exceptions noted.
	13.39 – INFOPAC is used to control the output of COFRS, HR/payroll reports. All reports are batched by user ID.	By inquiry and observation, confirmed that files are prepared each night. Hard copy reports are shipped to requesting agency for review.	No exceptions noted.

Figure 13: Install and Test Application Software and Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.40 – For reports printed at the Data Center, a header sheet is generated between batches and printing commands are sent to the high-speed printers. Reports are then logged and sent to the user indicated on the header sheet.	By inquiry and observation, observed that print job/spool separator pages are inserted between all jobs.	No exceptions noted.
	13.41 – Reports accessed online by users through INFOPAC are restricted to user ID. Users may only access reports assigned to their ID.	By inquiry and observation, observed login security with manager of HR/Payroll Systems and the financial systems manager. Observed that online reports are restricted by user ID.	No exceptions noted.
	13.42 – Agency security administrators are responsible for granting and revoking user access rights to COFRS, CPPS and HR/payroll reports.	By inquiry and observation, observed login security with manager of HR/Payroll Systems and the financial systems manager. Observed that agency security administrators have the authority to grant or revoke user access rights for their agencies, including report access rights.	No exceptions noted.
	13.43 – Forms are inspected upon receipt of shipment.	Inspected documents in the storage vault accompanied by computer operations manager. Observed that the key must be checked out from the key safe in the computer operations center. Unused forms are sequentially numbered and stored in sealed boxes.	No exceptions noted.

Figure 13: Install and Test Application Software and Technology Infrastructure			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	13.44 – Forms are stored in a secure space.	Observed the storage vault accompanied by computer operations manager. Observed that the key must be checked out from the key safe in the computer operations center. Observed that the vault has but one entrance and that that entrance is within a secured area.	No exceptions noted.
	13.45 – Standard operating procedures require that access to warrant forms are limited to computer operations staff and only at appropriate processing times.	Observed the storage vault accompanied by computer operations manager. Observed that the key must be checked out from the key safe in the computer operations center.	There is limited physical control restricting access to specific (appropriate) processing periods. Exceptions noted. (See recommendation #7.)
	13.46 – Stock number series are verified prior to and after print processing.	Inspected documents in the storage vault accompanied by Computer Operations Manager. Obtained copies of form inventory and check-out logs for test period.	No exceptions noted.

Figure 14: Manage Service Levels			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that service levels are defined and managed in a manner that provides a common understanding of performance levels with which the quality of services will be measured.	14.1 – SLAs are executed for Data Center operations.	Obtained and reviewed the service level agreements (SLA) for the clients who have SLAs in place and noted data center performance indicators are included in documentation.	No exceptions noted. (See recommendation #8.)
	14.2 – SLAs are executed for all new customers.	Obtained and reviewed the service level agreements (SLA) for the new clients who have SLAs in place and noted Data Center performance indicators are included in documentation.	No exceptions noted.

Figure 15: Define and Manage Service Levels			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that service levels are defined and managed in a manner that satisfies financial reporting system requirements and provides a common understanding of performance levels with which the quality of services will be measured.	15.1 – Service levels are defined and managed to support system requirements.	Obtained and reviewed the service level announcements from DoIT.	No exceptions noted.
	15.2 – A framework is defined to establish key performance indicators to manage service level agreements, both internally and externally.	Through inquiry and inspection, noted that currently, there is only the internal monitoring of the systems in regards to downtime and response.	There does not appear to be any external response from the client being serviced to measure performance by DoIT. Exception noted. (See recommendation #8.)

Figure 16: Manage Third-Party Services			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that third-party services are secure, accurate and available, support processing integrity and are defined appropriately in performance contracts.	16.1- A designated individual is responsible for regular monitoring and reporting on the achievement of the third-party service level performance criteria.	Reviewed purchase orders and statements of work for services during the audit period.	All purchase orders for services for the audit period were below the DPA threshold so no formal controls were required by DoIT. Evidence was not found that there is a designated individual responsible for monitoring third-party services. Exception noted. (See recommendation #4.)
	16.2- Selection of vendors for outsourced services is performed in accordance with the organization's vendor management policy.	Reviewed purchase orders and statements of work for services during the period. All Purchase Orders for services for the period were below the DPA threshold so no formal processes were required by DoIT. Documentation was reviewed for request for proposal (RFP) and contract process for services over DPA threshold.	No exceptions noted. (See recommendation #4.)
	16.3- IT management determines that, before selection, potential third parties are properly qualified through an assessment of their capability to deliver the required service and through a review of their financial viability.	Reviewed procurement requests, purchase orders and statements of work.	No evidence was found that IT management has a process in place to verify qualifications of third parties. Exception noted. (See recommendation #4.)

Figure 16: Manage Third-Party Services			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	16.4 – Third-party service contracts address the risks, security controls and procedures for information systems and networks in the contract between the parties.	Reviewed purchase order and contract terms and conditions and did not find reference to risks, security controls or procedures for information systems and networks.	Exceptions noted. (See recommendation #4.)
	16.5 – Procedures exist and are followed to ensure that a formal contract is defined and agreed for all third-party services before work is initiated, including definition of internal control requirements and acceptance of the organization's policies and procedures.	No evidence was found that a procedure exists to ensure there is a formal contract in place for third-party services unless services are over the DPA dollar threshold.	Exceptions noted. (See recommendation #4.)
	16.6 – A regular review of security, availability and processing integrity is performed for service level agreements and related contracts with third-party service providers.	Inquiry revealed that there is no review performed to ensure security, availability or integrity.	Exceptions noted. (See recommendation #4.)

Figure 17: Enhance System Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that financial reporting systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.	17.1 – Computer operators are prohibited from making changes to systems and data.	We obtained a complete list of Top Secret ACIDS and reviewed a complete list of privileged accounts. Reviewed TSSAUDIT to validate that changes made in production were warranted.	No exceptions noted.
	17.2 – Application programmers are not permitted access to production systems and data.	We obtained a complete list of Top Secret ACIDS and reviewed a complete list of privileged accounts. Reviewed the output of ACIDS permitted with special administrative privileges.	No exceptions noted.
	17.3 – Access to security administration functions is appropriately limited to authorized individuals.	Through inquiry, observation and programmatic testing, we validated that all passwords belong to Top Secret Administrators and that all keys are owned by the root account. DoIT possesses the ability to traverse all TSS facilities and keys. Each department has a designated TSS security administrator who has access to add and remove users to their assigned department facility only.	No exceptions noted. (See recommendation #5.)

Figure 17: Enhance System Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	17.4 – Top Secret is used to restrict access to system software to appropriate individuals.	Through testing and observation, we validated that Top Secret is configured to restrict access to production software.	An exception was noted when reviewing the terminated employee access list. Of 18 employees, one employee had a valid TSS account on the mainframe. The exception was due to a change in status from contract to employee not being updated appropriately. Exception noted. (See recommendation #10.)
	17.5 – Top Secret is used to restrict access to those system programs that allow bypassing of normal system or application controls (e.g., Super Zap).	We obtained the output from the SYS1.PARMLIB and validated all protected dataset. Furthermore, used the TSS WHOHAS PGM access to validate the security and usage of special program utilities.	No exceptions noted.
	17.6 – The System Security and Use Standard Operating Procedure (SOP) #8808 provides clear guidance regarding the responsibilities of Top Secret security administrators and the issuance of access permissions.	Reviewed SOP 8808.	No exceptions noted.
	17.7 – Employees receiving logical access to the mainframe are required to sign a compliance statement, referencing and acknowledging the computer usage and data security policy.	Reviewed copies of forms signed by employees and noted the forms are kept in each employee's personnel file. Reviewed copies from sampled employee files.	No exceptions noted.

Figure 17: Enhance System Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	17.8 – Computer security information is listed in the SOP.	Reviewed SOP 8808.	No exceptions noted.
	17.9 – Security administrators are required to sign an additional statement of compliance referencing and acknowledging responsibilities relative to Top Secret security administration.	Reviewed copies of forms signed by security administrators and noted the forms are kept in each employee's personnel file. Viewed entries for a sample of employees.	No exceptions noted.
	17.10 – Top Secret is used to restrict access to mainframe.	We obtained the output from TSSWHOHAS DSN (SYS1) and validated that all critical operating system files are properly secured.	No exceptions noted.
	17.11 – Data Center Top Secret administration privileges are limited to authorized personnel.	Reviewed copies of forms signed by security administrators. The forms are kept in each employee's personnel file. Viewed entries for a sample of employees.	No exceptions noted.
	17.12 – Standard operating policies require that the users have access to only those resources necessary and appropriate to user's job duties.	Reviewed SOP 8808 for policy requirement.	No exceptions noted.
	17.13 – Human Resources coordinate through the Help Desk to arrange logical access to mainframe and datasets for new Data Center personnel. The employee's supervisor defines the initial access to be granted and minimum permission rights based on the employee's position.	Reviewed user access request forms used to coordinate user privileges. Noted appropriate supervisor sign-off and that user access is granted through the security team.	No exceptions noted.

Figure 17: Enhance System Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	17.14 – New personnel receive a unique ACID and temporary password. The password must be changed on their first logon attempt or their account will be suspended (locked out).	Through review of the TSS PARMS report, inquiry and observation, we validated that new user accounts are set up with temporary passwords, which force password change upon first login attempt to the mainframe.	No exceptions noted.
	17.15 – Use of ACIDs and passwords are assigned to individuals to provide accountability.	Validated through inquiry and observation of settings within TSS that all ACIDs require the use of passwords.	No exceptions noted.
	17.16 – Top Secret is configured to enforce password controls including minimum length, defined password expiration, minimum re-use of password generation and account suspension/lockout after maximum failed login attempts.	Obtained and reviewed a copy of the TSS PARMS report and validated password controls enforce a minimum password length and a maximum for failed login attempts.	No exceptions noted.
	17.17 – The help desk unlocks accounts only after verifying a user's identity using additional private information from INSTADATA.	Made inquiries and observed the security team administers Top Secret and user access. Top Secret locks user access after three attempts. Employees must contact DoIT help desk for reactivation using two personal "safe" words.	No exceptions noted.
	17.18 – Future permission changes/enhancements require an E-mail or other written communication from the user's supervisor to the Help Desk explaining the reason for the permission change request.	By inquiry and observation with Top Secret security administrator, determined the security team administers Top Secret and user access. Ascertained that users within DoIT access will be changed only after receipt of an appropriate e-mail.	No exceptions noted.

Figure 17: Enhance System Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	17.19 – The system automatically disconnects a login session if inactive for 15 minutes.	Obtained and inspected a copy of the TSS PARMS report and validated a 15 minute session disconnect setting was in effect on the mainframe.	No exceptions noted.
	17.20 – Top Secret is operating in fail mode, meaning that unauthorized attempts to access data sets are aborted.	Obtained and inspected a copy of the TSS PARMS report and validated that TSS was operating in fail mode.	No exceptions noted.
	17.21 – Top Secret logs security violations; logs are reviewed periodically and action is taken to investigate violations.	Randomly selected a sample of security violations logs and reviewed for suspicious activity. Observed that there is no formal review of the logs, and the SOPs in force do not have an incidence response mechanism that is formalized by management to communicate unusual or suspicious activity.	There was no evidence to support management's review of security violations on a periodic basis. Furthermore, no incidence response plan exists to communicate unusual or suspicious activity to management. Exceptions noted. (See recommendation #6.)
	17.22 – Top Secret logs security profile changes; logs are reviewed periodically and unusual items are identified and investigated.	Randomly selected a sample of security violations logs and reviewed for suspicious activity. Observed that there is no formal review of the logs, and the SOPs in force do not have an incidence response mechanism that is formalized by management to communicate unusual or suspicious activity.	Exceptions noted. (See recommendation #6.)

Figure 17: Enhance System Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	17.23 – The administrative staff utilizes a departing employee checklist to ensure that the departing personnel's user mainframe account is deleted in a timely manner.	We obtained a copy of the JCL that runs the sweeper job to remove unused AC-IDs and validated its job position in CA-7. See 17.4 for information pertaining to terminated employees.	No exceptions noted.
	17.24 – The network is administered by agency network security administrators. Only network security administrators have the ability to create network accounts and grant access to the network.	By inquiry and observation, noted the security team administers Top Secret and user access.	No exceptions noted.
	17.25 – Each person is given a user ID and temporary password. The password must be changed on his or her first login attempt or the user's account will be suspended (locked out).	By interview and observation, noted the security team administers Top Secret and user access. Observed process with Top Secret administrator. Noted new users are given a onetime temporary password, the system requires that the password be changed, and if the user fails in the attempt, a new random password is generated. Noted the user will not be given access beyond the login screen until the password is changed.	No exceptions noted.
	17.26 – Control settings enforce adequate account and password controls for the network.	By interview and observation, observed that control settings support the control activity.	No exceptions noted.

Figure 17: Enhance System Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	17.27 – The following logs are reviewed on a monthly basis: • Logon/logoff failures • File and object access failures • Security profile changes • Restart, shutdown and system successes/failures	Obtained and inspected copies of logs and supervisor review.	No exceptions noted.
	17.28 – The administrative staff utilizes a departing employee checklist to ensure that departing personnel's network account is deleted in a timely manner.	Reviewed listing of departing employees for period and noted that supervisor checklist had been completed.	No exceptions noted.
	17.29 – Batch jobs are run on a pre-determined schedule and tracked automatically.	Reviewed SOP8808 and observed the job scheduling process and obtained a complete sample of jobs scheduled on the mainframe, both routine and single use, and validated that jobs must be scheduled through CA-7. Obtained a list of authorized users of the CA-7 scheduling software and compared against the terminated employees list.	No exceptions noted.

Figure 17: Enhance System Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	17.30 – Routine jobs that are processed outside of their normal schedule are checked off by schedulers as they are completed.	Reviewed SOP8808 and observed the job scheduling process and obtained a complete sample of jobs scheduled on the mainframe, both routine and single use, and validated that jobs must be scheduled through CA-7. Obtained a list of authorized users of the CA-7 scheduling software and compared against the terminated employees list.	No exceptions noted.
	17.31 – Scheduling deviations are reported by schedulers and published for management review on a daily activity history report.	Through review of procedure, noted that DoIT uses a formal CPP (control processing procedure), which is filled out by each job owner, which states what to do in the event of an Abend; however, there were inconsistencies when comparing the implementation date to the DoIT review date. Thirty days yielded 12 CCPs for review. Of the 12 CCPs, six had inconsistent review dates and 100% of the 12 CCPs did not have the appropriate DoIT review signature.	Two of the 12 CPPs did not appear to have any actionable information in the event of an abend (DXATCPD, DTFLICK) and did not follow the same or similar format as the sample. Exception noted. (See recommendation #11.)
	17.32 – The Data Center has documented control processing procedures, which provide detailed guidance to address processing problems, including whom to contact for system and application-specific troubleshooting information.	Reviewed batch job logs for availability of "on call" staff for problem resolution. Reviewed events that did not require escalation by calling programmer.	No exceptions noted.

Figure 17: Enhance System Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	17.33 – Problems identified are immediately entered into Remedy, defining the problem and corrective procedures undertaken.	Reviewed SOP8802 for framework of problem management resolution and ascertained the problem resolution/management process was operating effectively.	No exceptions noted.
	17.34 – Exceptions to normal operations as they relate to processing and tracking of problems are reported by schedulers and are published for management review on the daily activity history report.	Selected a sample of the daily activity history report to validate that exceptions to normal operations were being tracked in INFOSYS/Remedy.	No exceptions noted.
	17.35 – The following are backed up on a defined schedule: • Critical disk packs • System data sets and catalogs • Source program libraries • Databases for which the Data Center staff function as the database administrator (DBA)	Reviewed SOP for tape backup. Carried out inquiries with key personnel. Noted that tapes are being backed up on schedule. Sever centric network tapes are backed up on a recurring schedule. Server centric network backup configuration and schedule are set by individual departments and data owners.	No exceptions noted. (See recommendation #1.)
	17.36 – All backup media requiring off site storage have been adequately contracted for.	The State of Colorado has a contract for record storage. Copies of the contract were not available for our inspection. We were provided with copies of the State agreement that defines the contractual obligations required of a supplier.	No exceptions noted. (See recommendation #4.)

Figure 17: Enhance System Security			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	17.37 – The off-site facility has been properly contracted for physical security and access.	Though inquiry, noted the State of Colorado has a contract for record storage. The storage facility is contractually required to meet certain standards for data security. The standards in the State agreement define the requirements required by the State of Colorado. Copies of the contract were not available for our review.	No exceptions noted. (See recommendation #4.)

Figure 18: Manage the Configuration			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that all IT components, as they relate to security, processing and availability, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration.	18.1 – Only authorized software is permitted for use by employees using company IT assets.	By interview and observation, determined employees are restricted from installing software. Software inventories are maintained.	No exceptions noted.
	18.2 – System infrastructure, including firewalls, routers, switches, network operating systems, servers and other related devices, are properly configured to prevent unauthorized access.	Obtained and inspected a copy of the running configuration from both perimeter firewall configurations (HSRP) and the switch that the firewalls interconnected on. We conducted an unauthenticated scan of selected UNIX servers and selected Windows Servers to validate that potential vulnerabilities have been addressed and undue security risk had been mitigated to prevent unauthorized access.	No exceptions noted.
	18.3 – IT management has implemented antivirus and antispam protection across the organization to protect information systems and technology from computer viruses.	By interview and observation, noted antivirus software is maintained on the DoIT workstations and that virus signature files are updated at appropriate intervals.	No exceptions noted.
	18.4 – A biannual assessment is performed to confirm that the software and network infrastructures are appropriately configured.	Reviewed DoIT changed activities schedule and ISOC Visio documentation.	No exceptions noted.

Figure 18: Manage the Configuration			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	18.5 – Access control server (ACS) used to monitor changes to critical network equipment.	ACS logs for the period were reviewed.	No exceptions noted.

Figure 19: Manage Problems and Incidents			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution.	19.1 – Outage notifications are documented.	We reviewed a sample of outage notification forms and ascertained documentation of outages. The outage notification form was implemented by management in January 2005.	No exceptions noted.
	19.2 – Outage notification short- and long-term resolution are reviewed by management.	Through inquiry and inspection of reports, ascertained management receives monthly reports and resolutions.	No exceptions noted.

Figure 20: Manage Data			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.	20.1 – Procedures exist and are followed to periodically test the effectiveness of the restoration process and the quality of backup media.	Through inquiry and inspection of documentation, noted the quality of data backup tapes used by DFDSS is monitored by the systems and that if three errors occur within a 30-day period for any tape, the tape is replaced. Noted that if three errors occur on any tape drive within a 30-day period, a maintenance request is generated. Ascertained that once a year, data backups are tested at the IBM hot site and that this year's test was performed on February 15–18, 2005. Noted that data within the responsibility of DoIT was successfully restored.	No exceptions noted. (See recommendations #1 and #2.)

Figure 21: Manage Operations			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing, error monitoring and system availability.	21.1 – Top Secret is used to restrict access to scheduling software (CA-7) to appropriate personnel.	Reviewed SOP8808 and observed the job scheduling process and obtained a complete sample of jobs scheduled on the mainframe, both routine and single-use, and validated that jobs must be scheduled through CA-7. Obtained a list of authorized users of the CA-7 scheduling software and compared against the terminated employees list.	No exceptions noted.
	21.2 – Automated operation of scheduling software is used.	Reviewed SOP8808 and observed the job scheduling process and obtained a complete sample of jobs scheduled on the mainframe, both routine and single use, and validated that jobs must be scheduled through CA-7. Obtained a list of authorized users of the CA-7 scheduling software and compared against the terminated employees list.	No exceptions noted.
	21.3 – Operator activities are recorded on the console log.	Reviewed operator console logs for jobs/activities.	No exceptions noted.
	21.4 – Exceptions to normal operations as they relate to data center staff use of computers are reported by schedulers and published for management review on a daily activity history report.	Selected a sample of the daily activity history report to validate that exceptions to normal operations were being tracked in INFOSYS/Remedy.	No exceptions noted.

Figure 21: Manage Operations			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	21.5 – Batch jobs are run on a pre-determined schedule and tracked automatically.	Reviewed SOP8808 and observed the job scheduling process and obtained a complete sample of jobs scheduled on the mainframe, both routine and single-use, and validated that jobs must be scheduled through CA-7. Obtained a list of authorized users of the CA-7 scheduling software and compared against the terminated employees list.	No exceptions noted.
	21.6 – Routine jobs that are processed outside of their normal schedule are checked off by schedulers as they are completed.	Reviewed SOP8808 and observed the job scheduling process and obtained a complete sample of jobs scheduled on the mainframe, both routine and single use, and validated that jobs must be scheduled through CA-7. Obtained a list of authorized users of the CA-7 scheduling software and compared against the terminated employees list.	No exceptions noted.
	21.7 – Scheduling deviations are reported by schedulers and published for management review on a daily activity history report.	Selected a sample of the daily activity history report to validate that exceptions to normal operations were being tracked in INFOSYS/Remedy.	No exceptions noted.
	21.8 – A problem management system (Remedy) is used to record, track, and resolve identified problems.	Reviewed SOP8802 for framework of problem management resolution and ascertained the problem resolution/management process was operating effectively.	No exceptions noted.

Figure 21: Manage Operations			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	21.9 – The Data Center has documented control processing procedures, which provide detailed guidance to address processing problems, including whom to contact for system and application-specific troubleshooting information.	Reviewed related documentation including operator console logs for jobs and activities, call staff listings and results documentation.	No exceptions noted.
	21.10 – Problems identified are immediately entered into Remedy, defining the problem and corrective procedures undertaken.	Reviewed SOP8802 for framework of problem management resolution and ascertained the problem resolution/management process was operating effectively.	No exceptions noted.
	21.11 – Exceptions to normal operations as they relate to processing and tracking of problems are reported by schedulers and are published for management review on the daily activity history report.	Selected a sample of the daily activity history report to validate that exceptions to normal operations were being tracked in INFOSYS/Remedy.	No exceptions noted.

Figure 22: Human Resource/Payroll System			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
Human resource application processing controls are in place.	22.1 – Changes to the payroll master files are processed in a timely manner.	Through inquiry and observation with the manager of HR/Payroll Systems and review of a sample of the SCO CDB change register, noted changes are entered into the Integral Systems, Inc. human resource management system (HRMS) online and changes are immediate. Noted that changes are entered by SCO and agency payroll officers and the changes take effect immediately. Noted that batch file confirming reports are generated nightly and that DoIT personnel are not permitted to change data. Ascertained that all changes are reviewed daily by SCO and agency personnel.	No exceptions noted.

Figure 22: Human Resource/Payroll System			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	22.2 – Payroll master file data remain up-to-date.	Through inquiry and observation with the manager of HR/Payroll Systems and review of a sample of the SCO CDB change register, noted changes are entered into the Integral Systems, Inc. human resource management system (HRMS) online and changes are immediate. Noted that changes are entered by SCO and agency payroll officers and the changes take effect immediately. Noted that batch file confirming reports are generated nightly and that DoIT personnel are not permitted to change data. Ascertained that all changes are reviewed daily by SCO and agency personnel.	No exceptions noted.

Figure 22: Human Resource/Payroll System			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	22.3 – Only valid changes are made to the payroll withholding tables.	Through inquiry and observation with the manager of HR/Payroll Systems and review of a sample of the SCO CDB change register, noted changes are entered into the Integral Systems, Inc. human resource management system (HRMS) online and changes are immediate. Noted that changes are entered by SCO and agency payroll officers and the changes take effect immediately and that DoIT personnel are not permitted to change data. Noted that change reports are reviewed by SCO and agency payroll officers daily. Ascertained that all changes are reviewed daily by SCO and agency personnel.	No exceptions noted.

Figure 22: Human Resource/Payroll System			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	22.4 – All valid changes to the payroll withholding tables are input and processed.	Through inquiry and observation with the manager of HR/Payroll Systems and review of a sample of the SCO CDB change register, noted that changes are entered into the Integral Systems, Inc. human resource management system (HRMS) online and changes are immediate. Noted that changes are entered by SCO and agency payroll officers and that changes take effect immediately. Noted batch file confirming reports are generated nightly. Noted change reports are reviewed by SCO and agency payroll officers daily. Ascertained that DoIT personnel are not permitted to change data. Noted that payroll processing parameters prevent the processing of amounts and withholdings outside specified ranges. Noted all changes are reviewed daily by SCO and agency personnel.	No exceptions noted.

Figure 22: Human Resource/Payroll System			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	22.5 – Changes to the payroll withholding tables are accurate.	Through inquiry and observation with the manager of HR/Payroll Systems and review of a sample of the SCO CDB change register, noted changes are entered into the Integral Systems, Inc. human resource management system (HRMS) online and changes are immediate. Noted that changes are entered by SCO and agency payroll officers and the changes take effect immediately and that DoIT personnel are not permitted to change data. Noted that change reports are reviewed by SCO and agency payroll officers daily. Ascertained that all changes are reviewed daily by SCO and agency personnel.	No exceptions noted.

Figure 22: Human Resource/Payroll System			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	22.6 – Changes to the payroll withholding tables are promptly processed.	Through inquiry and observation with the manager of HR/Payroll Systems and review of a sample of the SCO CDB change register, noted changes are entered into the Integral Systems, Inc. human resource management system (HRMS) online and changes are immediate. Noted that changes are entered by SCO and agency payroll officers and the changes take effect immediately. Noted that batch file confirming reports are generated nightly and that DoIT personnel are not permitted to change data. Ascertained that all changes are reviewed daily by SCO and agency personnel.	No exceptions noted.

Figure 22: Human Resource/Payroll System			
Provided by DoIT		**Provided by BKD**	
Control Objective	**Control Activity**	**Testing Procedures**	**Results**
	22.7 – Payroll withholding table data remain up-to-date.	Through inquiry and observation with the manager of HR/Payroll Systems and review of a sample of the SCO CDB change register, noted changes are entered into the Integral Systems, Inc. human resource management system (HRMS) online and changes are immediate. Noted that changes are entered by SCO and agency payroll officers and the changes take effect immediately and that DoIT personnel are not permitted to change data. Noted that change reports are reviewed by SCO and agency payroll officers daily. Ascertained that all changes are reviewed daily by SCO and agency personnel.	No exceptions noted.

Section VII
Status of Implementation of Prior Recommendations

Status of Prior Audit Recommendations

No.	Recommendations	Prior Audit Report Status	September 2005 DoIT Update/Comments
	From the Report of the State Auditor for Fiscal Year Ended June 30, 2004		
17a	The Department of Personnel & Administration should ensure that the technology management unit improve its controls over COFRS access by requiring financial system team management to provide end dates enabling the automated process to suspend contractors' access.	**Implementation Date: February 2005.** The Top Secret administrator within Technology Management Unit (Unit) grants access to COFRS for financial systems employees and contractors after receiving written/e-mail approval from the Financial System Team manager. If the request is for temporary access, an expiration date is required. The Top Secret administrator will enter this end date into the system, enabling the automated process to suspend access. If additional time is needed, a new request is required.	**Partially Implemented.** The controls implemented in February 2005 continue to be followed. However, note related current year exception 17.4.
17b	The Department of Personnel & Administration should ensure that the technology management unit improve its controls over COFRS access by implementing a process to ensure financial system team management reviews access privileges in a timely manner when employee and contractor assignments change.	**Implementation Date: February 2005.** The financial systems team manager has developed a checklist for when an employee or contractor leaves the team. One item on the checklist is for Top Secret access. The financial system team manager notifies the Top Secret administrator within the unit of the end date for the employee or contractor. The Top Secret administrator can then enter the end date into the system prior to the actual end date.	**Partially Implemented.** The controls implemented in February 2005 continue to be followed. However, note related current year exception 17.4.

No.	Recommendations	Prior Audit Report Status	September 2005 DoIT Update/Comments
	From the SAS 70 – March 2003		
1	Restrict security administration privileges to only those individuals who require it to perform their job functions. Limit user access to data and systems based on specific job responsibility. Segregate access to critical system functions.	**Implementation in Progress** The Data Center has made improvements to logical access; however, exceptions were noted in the current year. Current year recommendation No. 1.	**Implemented.** Standard Operating Procedure 8808 was modified to include paragraph 8808.7, "Periodic Review of Mainframe ACIDs." Required annual updates with supervisor sign-offs were accomplished in 2004 and 2005.
2	A thorough review should be performed of all profiles for existing users within the next 3-6 months. A process should be put in place for the ongoing review of access to specific critical functions or systems (i.e. security administration, system software, scheduling). A cyclical approach may be used whereby a portion of the population is reviewed at a defined interval, resulting in review of the entire population every two years. Management should implement an oversight function to ascertain compliance with the periodic review process.	**Partially Implemented** Certain profiles have been reviewed; however, exceptions were noted in the current year. Current year recommendation No. 1.	**Implemented.** Standard Operating Procedure 8808 was modified to include paragraph 8808.7, "Periodic Review of Mainframe ACIDs." Required annual updates with supervisor sign-offs were accomplished in 2004 and 2005.
3	Implement a security-awareness training program to supplement current security policies and procedures. All Data Center and TMU employees should be required to sign an annual statement of compliance acknowledging Data Center computer security policies and denoting completion of security awareness training.	**Partially Implemented**	**Partially Implemented.** A security awareness course was designed and implemented in 2003 but was not conducted in 2004. A DoIT specific security awareness training class with signoff is planned for 2006. Expected implementation date: December 31, 2006.

No.	Recommendations	Prior Audit Report Status	September 2005 DoIT Update/Comments
	From the SAS 70 – April 2002		
1	Restrict logical access to systems and data to only properly authorized individuals.	**Implementation in Progress** The Data Center has made improvements to logical access; however, exceptions were noted in the current year. Current year recommendation No. 1.	**Implemented**. Standard Operating Procedure 8808 was modified to include paragraph 8808.7, "Periodic Review of Mainframe ACIDs." Required annual updates with supervisor sign-offs were accomplished in 2004 and 2005.
2	Periodically review existing user profiles and access listings to ensure that access permissions are consistent with job responsibilities.	**Partially Implemented** Certain profiles have been reviewed; however, exceptions were noted in the current year. Current year recommendation No. 1.	**Implemented**. Standard Operating Procedure 8808 was modified to include paragraph 8808.7, "Periodic Review of Mainframe ACIDs." Required annual updates with supervisor sign-offs were accomplished in 2004 and 2005.
8	Consider the use of version control software for application changes.	**Not Implemented** The Technology Management Unit reports that it does not currently have the financial resources to implement this recommendation. No implementation date provided.	**Not Implemented.** DoIT reported it considered the purchase and use of automated version control software for COFRS but there is still not sufficient operating or FTE budget to accomplish this. Given the relatively few code changes that occur on a system as mature as COFRS, the return on investment is questionable even if the budget were available. No further action is planned. BKD Note: Version control software should be reconsidered in the context of all supported systems, not just COFRS. Such software can assist in overall code and version management, as well as contribute to management of segregation of duties and testing.

No.	Recommendations	Prior Audit Report Status	September 2005 DoIT Update/Comments
9	Implement a security awareness training program.	**Not Implemented** The Data Center reports that it did not have adequate personnel to implement this recommendation. Current year recommendation No. 3.	**Partially Implemented**. A security awareness course was designed and implemented in 2003 but was not conducted in 2004. A generic training class has been procured through a Homeland Security grant and will be implemented for 2006. Expected implementation date: December 31, 2006.
10	Create employee training and development plans.	**Implementation in Progress** A strategic planning group has been formed and Data Center personnel have created personal training goals. Next steps include management review of training goals, standardization by position and formalization of approved training and development plans.	**Implemented**. A training room has been constructed and appropriate training software has been procured. Annual training objectives are set forth in SOPs 6707, 6713, and 6714 and in each operation employee's performance plan. However, see September 2005 update for April 2002 recommendation #9 and March 2003 recommendation #3.
	From the Report on Performance Measures – September 2001		
1	Implement service level agreements with customers.	**Implementation Plan in Progress** Staff have been assigned to project. Draft service level agreement is being designed and was to be used on a pilot basis by September 2002; however, staffing limitations have made this a low-priority initiative. No implementation date provided.	**Partially Implemented**. Seven service level announcements have been created for mainframe computer operations. Service level agreements are generated for each new server housing or hosting customer effective July 1, 2004. Note: This is a focus of current year recommendation #8.

No.	Recommendations	Prior Audit Report Status	September 2005 DoIT Update/Comments
	From the Report on Performance Measures – September 2001		
3	Define problem management tool requirement and evaluate existing tool.	**Implementation in Progress** After issuing and then recalling an RFP for a new problem management tool, the Data Center determined that a new strategy was necessary to effectively implement this recommendation. The Data Center is seeking to extend the tool selection process by 90 days. In parallel with this extension, alternative organization approaches are being evaluated. This evaluation is critical to determining the most effective implementation of not only the tool, but of the business processes supported by the tool. A direction is therefore anticipated during the second quarter of the fiscal year.	**Implemented**. A new problem management tool, Remedy, was installed, tested and became fully operational in May 2005, including training for users. Note: This tool can be used to support recommendation #8.
5	Implement continuous feedback survey in the Service Center.	**Implementation in Progress** The Data Center expects to have this fully implemented by September 2003.	**Implemented**
12	Generate monthly security metrics.	**Implementation in Progress** Baseline security data have been obtained as a result of the recently completed statewide security assessment. Monthly metrics will be generated beginning approximately July 2003.	**Not Implemented.** According to DoIT, metrics were not implemented due to staffing limitations and intrusiveness of tools. Event correlation is under development. No implementation date provided.

No.	Recommendations	Prior Audit Report Status	September 2005 DoIT Update/Comments
	From the SAS 70 – April 2000		
10	As equipment changes in the Data Center or major renovations are performed, the Data Center should re-engineer both power and signal cable ducts to provide separation and safety.	**Implementation in Progress** Vendor estimates for power and signal duct re-engineering have been obtained for current year changes; however lack of financial resources have prohibited significant implementation. No implementation date provided.	**Not Implemented.** According to DoIT, preparations are underway to analyze power capacity and usage as part of a larger goal of implementing standards for power and signal cabling in the Data Center in general when a sufficient budget is available. No implementation date provided.

This Page Intentionally Left Blank

Section VIII
User Control Considerations

User Control Considerations

Colorado Financial Reporting System (COFRS) and Colorado Payroll and Personnel System (CPPS)

The processing of transactions for clients performed by the Data Center and the Technology Management Unit's (TMU) COFRS/CPPS applications and the control structure policies and procedures at the Data Center and within TMU's COFRS/CPPS applications cover only a portion of the overall internal control structure of the Data Center and TMU's COFRS/CPPS applications. It is not feasible for the control objectives relating to the processing of transactions to be solely achieved by the Data Center and TMU's COFRS/CPPS applications. Therefore, each user organization's internal controls must be evaluated in conjunction with the control policies and procedures of the Data Center and TMU's COFRS/CPPS applications and the testing summarized in Section VI – Information Provided by the Service Auditor.

The following identifies those control activities that the Data Center and Technology Management Unit believe should be in place at user organizations and were considered in developing policies and procedures described by the Data Center and Technology Management Unit in this report. In order for user organizations to rely on the control policies and procedures presented within this report, each user must evaluate its own internal controls to determine if the following controls are in place and operating effectively. Furthermore, the following controls are identified only to address those policies and procedures related to the processing of transactions at the Data Center and by TMU's COFRS/CPPS applications. Accordingly, the identified controls do not represent a complete listing of control policies and procedures that provide a basis for the assertions underlying the financial statements and personnel reports of user organizations.

The purpose of this section is to identify the general and application controls that must be tested as part of the auditor's review of internal controls at agencies that use Data Center services and TMU's COFRS/CPPS applications. This section also provides examples of specific control considerations that auditors of user agencies should include in their reviews of agency internal controls.

Application Controls

When reviewing an agency's control environment, the auditor should review the agency's controls over the use of its applications systems. Application controls are the responsibility of each user agency and are not the Data Center and TMU's responsibility. In general, these controls must ensure that

- Access to computer terminals, direct-dial phones, modems and official paper input documents are secured against unauthorized use.
- Data extracted from TMU-managed systems and stored in agency-managed systems are protected from unauthorized access.
- Requested changes to the COFRS and CPPS systems have been authorized by the appropriate agency personnel.
- Input data and transactions are authorized, complete, accurate and valid.

- Output reports received by the agency are secured, distributed and used according to management intent.
- Output reports are reviewed for accuracy and corrected promptly if errors are detected.
- Agencies actively participate with TMU in disaster recovery planning and testing.

Specific Control Considerations for User Auditors

We have compiled a list of specific activities that user auditors should complete as part of their agency internal control reviews. This list is not intended to be a comprehensive list of all steps needed to review internal controls. Individual agencies may require additional steps to complete the internal controls review. The activities we identified can be grouped according to the following control considerations:

- Security and access
- Input controls
- Output controls
- Disaster recovery planning

In addition to these categories of control considerations, user auditors should review the extent of the internal Information Technology (IT) auditing performed at the agency and the organization and management of the agency IT department.

Security and Access

Auditors should review the agency's use of Top Secret and any other security software available to the agency. The following steps should be included in an evaluation of an agency's security and access controls:

General Controls

1. Determine whether the agency has an agency security administrator and back-up agency security administrator or whether the agency relies on the Data Center for security administration duties.
2. Determine whether the agency has a database coordinator.
3. Review the responsibilities of the agency security administrator and the database coordinator to ensure that these individuals do not perform functions that are incompatible with their security administration duties.
4. Review Top Secret security settings established by the agency to control access, especially access to their own applications systems and data sets. These settings include, but are not limited to the following:

a. The Mode, which prevents access by unauthorized users or merely warns and then allows access.

b. The number of log-on attempts or unauthorized access attempts allowed before a user is locked out.

c. The automatic disconnect time limits for unused terminals.

Logical Access Controls

Review controls relating to the granting of access to resources. If any agency assigns its own access identifications, the auditor should review the agency security administrator controls relating to access identification assignments. The auditor should also confirm that all agency personnel assigned access identifications have signed a statement of compliance and that such statements are maintained in a file.

Physical Access Controls

1. Review the physical access controls over hardware, software, data, official input forms and official forms used to request and approve access identifications. Confirm that procedures exist to ensure that personnel do not leave logged-on terminals unattended, even if the agency uses automatic shut-off time limits.

2. Ensure that access to agency systems and to the Data Center mainframe computer system via terminals, modems, and direct-dial phone lines is limited.

Monitoring Activities

Confirm that a Top Secret security violations report is produced and reviewed by the agency security administrator on a regular basis. Agencies are responsible for investigating and correcting errors found on this report.

Input Controls

The Data Center and TMU have implemented procedures to ensure control over agency transactions and data that have been submitted for processing on the Data Center's mainframe computer system. However, it is the agency's responsibility to initiate transactions, control data and to submit both to the Data Center. In other words, agencies are responsible for ensuring that data and transactions are authorized, accurate and promptly submitted to the Data Center for processing. When reviewing input controls at the user agency, auditors should perform the following steps:

1. Confirm input documents are authorized and reviewed by an appropriate level of management.

2. Ensure control totals are used to verify that all transactions are entered.

3. Confirm that management reviews remote job entry documents before they are released for batch processing and that all remote job entry input documents or listings are canceled to prevent duplicate entries.

Output Controls

The Data Center's control procedures ensure that agency output is generated and distributed according to agency instructions. However, it is the agency's responsibility to ensure that output is accurate or that corrections are made promptly. When reviewing output controls at the agency, the auditor should

1. Confirm that exception reports are reviewed promptly and any necessary corrections are made in a timely manner.

2. Look for evidence of management's review of output reports for accuracy, completeness, reasonableness and mathematical accuracy.

3. Review agency procedures for ensuring that output is distributed only to appropriate personnel.

Disaster Recovery Planning

The Data Center has developed a disaster recovery plan to resume Data Center operations at a remote "hot site," including the migration to a "cold site" and a new "home site" in the event of a disaster affecting the Data Center. Auditors should review the agency's policies and procedures to coordinate the agency's disaster recovery plans with those established by the Data Center. Auditors should also review the agency's disaster recovery plans for its own application systems. Specifically, auditors should verify that agencies

1. Designate resources to be backed up and stored off-site, the frequency of such backups and the methods used to perform the backups.

2. Establish recovery and restart procedures, including coordination with the Data Center's recovery and restart efforts. The recovery and restart procedures should consider a system designed to establish a priority for critical systems applications.

3. Establish a formalized disaster recovery plan that is also coordinated with the Data Center's plan and is periodically reviewed and updated. Such plan should develop a formal disaster recovery plan document that is stored off-site, contains all necessary information for locating key personnel, procedures, application programs and data sets.

4. Participate in the Data Center hot-site tests and related forums.

5. Establish adequate contractual arrangements with vendors to replace equipment damaged by a disaster recovery event, subject to State self-insurance policies and procedures.

Distribution Page

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 1747 when requesting this report.