

THIRD PARTY REVIEW

**Department of Central Management Services
Bureau of Communication and
Computer Services**

July 2005

TABLE OF CONTENTS

Report Digest	i
Report on Third Party Review	1
Report Summary	5
Service Organization Description of Controls	7
Service Auditor Description of Tests and Operating Effectiveness	23
General Controls	25
Administration Controls	27
Continuous Service Controls	35
Computer Operations Controls	39
Security Controls	43
Application Systems Development Controls	47
Telecommunication Controls	51
Systems Software Controls	59
Application Controls	63
Accounting Information System	65
Central Payroll System	69
Central Inventory System	73
Central Time and Attendance System	77
Appendix A - Complementary User Organization Controls	81
Appendix B - List of User Agencies	85
Appendix C – Billing Allocation System	89
Appendix D – Acronym Glossary	91

REPORT DIGEST

**DEPARTMENT OF
CENTRAL MANAGEMENT
SERVICES
BUREAU OF
COMMUNICATION AND
COMPUTER SERVICES**

THIRD PARTY REVIEW

For the Year Ended:
June 30, 2005

Release Date:
July 6, 2005



State of Illinois
Office of the Auditor General
WILLIAM G. HOLLAND
AUDITOR GENERAL

To obtain a copy of the
Report contact:
Office of the Auditor General
Iles Park Plaza
740 E. Ash Street
Springfield, IL 62703
(217) 782-6046 or TTY (888) 261-2887

This Report Digest is also available on
the worldwide web at
<http://www.state.il.us/auditor>

INTRODUCTION

The Department of Central Management Services' (Department) Bureau of Communication and Computer Services carries out statutory responsibilities relating to data processing and telecommunication services (20 ILCS 405/405-10; 20 ILCS 405/405-20; 20 ILCS 405/405-250; 20 ILCS 405/405-255; 20 ILCS 405/405-260; and 20 ILCS 405/405-270). To fulfill its responsibilities, the Department operates the Central Computer Facility (CCF), the Communications Center, and branch facilities. A Springfield branch facility also serves as the primary backup site should a disaster prevent processing at the CCF. Through its facilities, the Department provides data processing services to approximately 96 user entities.

The CCF functions as a data processing service center, providing computing and telecommunication resources for State agencies' use. The Department and the agencies that use the Department's computer resources share the responsibility for maintaining the integrity and security of computerized data and functions.

We reviewed data processing general controls at the Department primarily during the period from January 10, 2005 to May 27, 2005. We performed tests to determine compliance with policies and procedures, conducted interviews, performed observations, and identified specific control objectives and procedures we considered necessary to evaluate the controls.

We also reviewed application controls for systems maintained by the Department for State agencies' use. The systems reviewed were the Accounting Information, Central Payroll, Central Inventory, and Central Time and Attendance Systems.

The Department's control procedures and the degree of compliance with the procedures were sufficient to provide reasonable, but not absolute, assurance that relevant control objectives were achieved.

To view an online version of the complete report, go to
<http://www.state.il.us/auditor/special.htm>

ILLINOIS DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
BUREAU OF COMMUNICATION AND COMPUTER SERVICES

STATISTICS	2005
Mainframes	3 Units Configured as 10 Production Systems and 4 Test Systems 1 Unit Configured for Disaster Recovery
Services/Workload	87.1 Million IMS Transactions per Month 1.3 Million Feet of Laser Printing per Month 316,000 Reel/Cartridge Tape Mounts per Month
State Agency Users	96
Bureau Employees	2002 -- 387 2003 -- 307 2004 -- 303 2005 -- 775 * * Increase due to IT consolidation into the Department per Executive Order 2003-10 and Public Act 93-839
Historical Growth Trend**	2002 -- 2,040 -- MIPS 2003 -- 2,700 -- MIPS 2004 -- 3,614 -- MIPS 2005 -- 3,217 -- MIPS MIPS -- Million Instructions Per Second ** In the month of April for each year listed

Information provided by the Department - Unaudited

AGENCY DIRECTOR AND DEPUTY DIRECTOR/BUREAU MANAGER
<p>During Audit Period: Director: Michael Rumman (7/1/2004 to 6/1/2005) Deputy Director/Bureau Manager: Jay Carlson</p> <p>Currently: Acting Director: Paul Campbell (6/2/2005 to present) Deputy Director/Bureau Manager: Jay Carlson</p>

REPORT SUMMARY

Disaster Contingency Planning

State Government Must Be Prepared

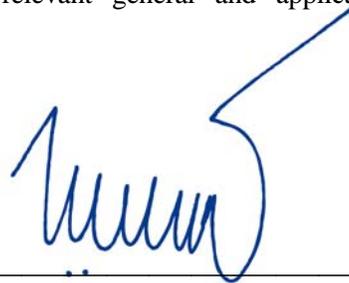
The Department has developed basic strategies to address the disaster contingency needs of the State's Central Computer Facility; however, the plans and operational provisions need to be enhanced to provide assurance that all of the State's critical applications and network operations can be recovered within required timeframes. Although continuity plans exist to guide recovery activities, management has not approved the plans, nor has the Department performed testing to identify any deficiencies in the plans and determine if the plans would effectively guide recovery efforts in the event of a disaster.

The Department should ensure the necessary components (plans, equipment, and facilities) are available to provide for continuation of critical computer operations in the event of a disaster. In addition, the Department should conduct comprehensive tests of the plans on an annual basis.

The Department concurred with our recommendation. In addition, the Department stated it has designated Disaster Contingency Planning as one of the top priorities for the upcoming fiscal year.

AUDITORS' OPINION

Procedures were generally sufficient to provide reasonable, but not absolute, assurance that relevant general and application control objectives were achieved.

A handwritten signature in blue ink, appearing to read "William G. Holland", with a long arrow pointing from the end of the signature towards the top right of the page.

WILLIAM G. HOLLAND, Auditor General

WGH:WJS:ap

AUDITOR'S REPORT

The Honorable William G. Holland
Auditor General
State of Illinois

We have examined the accompanying description of controls related to the systems and procedures used to control data processing operations at the Bureau of Communication and Computer Services of the Department of Central Management Services (Department). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the Department's controls that may be relevant to a user organization's internal control structure; (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 the Department's controls; and (3) such controls had been placed in operation as of May 27, 2005. Our review, started in the summer of 2004 and primarily performed between January 10, 2005 through May 27, 2005, was limited to controls at the Department's Central Computer Facility, the Department's Communications Center, and its branch facilities. The control objectives were specified by management of the Department. Our examination was performed in accordance with the Illinois State Auditing Act, applicable generally accepted auditing standards, and "Government Auditing Standards" issued by the Comptroller General of the United States. We included those procedures considered necessary under the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the aforementioned systems and procedures presents fairly, in all material respects, the relevant aspects of the Department's controls that had been placed in operation as of May 27, 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 the Department's controls.

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 the body of the report, to obtain evidence about their effectiveness in meeting the control objectives, during the period from January 10, 2005 through May 27, 2005. The specific controls and the nature, timing, extent, and results of the tests are listed in the body of the report. This information has been provided to the Department's

user organizations and to their auditors to be taken into consideration, along with information about the internal control at user organizations, when making assessment of control risk for user organizations. In our opinion, the controls that were tested, as described in the body of the report, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in the body of the report were achieved during the period from January 10, 2005 through May 27, 2005.

The relative effectiveness and significance of specific controls at the Department and their effect on assessments of control risk at user organizations are dependent on 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 the Department is as of May 27, 2005 and information about tests of the operating effectiveness of specified controls covers the period from January 10, 2005 through May 27, 2005. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specified controls at the Department 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 Appendix C of this report is presented to provide additional information to user organizations. The information in Appendix C has not been subjected to the procedures applied in the examination of the description of controls, and accordingly, we express no opinion on it.

This report is intended for the information and use of the Auditor General, the General Assembly, the Legislative Audit Commission, the Governor, Department management, affected State agencies, and auditors of the State agencies. However, this report is a matter of public record and its distribution is not limited.

William J. Sampias, CISA
Director, Information Systems Audits

Mary Kathryn Lovejoy, CPA
Information Systems Audit Manager

May 27, 2005

THIRD PARTY REVIEW

**Department of Central Management Services
Bureau of Communication and
Computer Services**

July 2005

REPORT SUMMARY

INTRODUCTION

The Department of Central Management Services' (Department) Bureau of Communication and Computer Services (Bureau) carries out statutory responsibilities relating to data processing and telecommunication services (20 ILCS 405/405-10; 20 ILCS 405/405-20; 20 ILCS 405/405-250; 20 ILCS 405/405-255; 20 ILCS 405/405-260; and 20 ILCS 405/405-270). To fulfill its responsibilities, the Department operates the Central Computer Facility (CCF), the Communications Center, and branch facilities. A Springfield branch facility also serves as the primary backup site should a disaster prevent processing at the CCF. Through its facilities, the Department provides data processing services to approximately 96 user agencies (see Appendix B).

The CCF functions as a service organization providing computing and telecommunication resources for State agencies' use. The Department and the agencies that use the Department's computer resources share the responsibility for maintaining the integrity and security of computerized data and functions. Although the Third Party Review addressed only controls for which the Department is responsible, we identified numerous control areas that should be reviewed and addressed by user agencies and their internal and external auditors (see Appendix A).

We reviewed data processing general controls at the Department. We performed tests to determine compliance with policies and procedures, conducted interviews, performed observations, and identified specific control objectives and procedures we considered necessary in the circumstances to evaluate the controls.

We also reviewed or confirmed application controls for systems maintained by the Department for State agencies' use. The systems were:

Accounting Information System;

Central Payroll System;

Central Inventory System; and

Central Time and Attendance System.

The Department's control procedures and the degree of compliance with the procedures were sufficient to provide reasonable, but not absolute, assurance that relevant control objectives were achieved.

Control Deficiencies

We identified several control deficiencies that appear in pages 25 through 79. One of these issues warrants additional emphasis.

Disaster Contingency Planning

The Department has developed basic strategies to address the disaster contingency needs of the State's Central Computer Facility; however, the plans and operational provisions need to be enhanced to provide assurance that all of the State's critical applications and network operations can be recovered within required timeframes. Although continuity plans exist to guide recovery activities, management has not approved the plans, nor has the Department performed testing to identify any deficiencies in the plans and determine if the plans would effectively guide recovery efforts in the event of a disaster.

Department management stated the development of an effective business continuity plan is one of its primary objectives in fiscal year 2006.

The State is placing great reliance on the Department's ability to provide data processing and network services in the event of a disaster. As such, comprehensive and thoroughly tested disaster contingency plans are an essential component of recovery efforts.

The Department should ensure the necessary components (plans, equipment, and facilities) are available to provide for continuation of critical computer operations in the event of a disaster. In addition, the Department should conduct comprehensive tests of the plans on an annual basis. (See pages 35-38 for additional information)

We will review progress towards the implementation of our recommendation during the next Third Party Review.

Department Response

The Department concurs with the recommendation.

As stated in the Report Summary, CMS/BCCS leadership has designated Disaster Contingency Planning as one of the top priorities for the upcoming fiscal year. In addition to the work already in place, including an improvement of tape management processes, a regional vaulting process, expansion of continuity exercises and comprehensive testing at our vendor's recovery site, we have begun planning work on a new backup data center site located approximately 200 miles from the current primary data center. This site will initially offer the backup and recovery capabilities for Category One applications that are currently provided through a vendor contract. We will also assess and develop a plan to provide full redundancy and operational capacity not previously available to the State at a site that will allow seamless data center operation in the event of a regional disaster.

The planning function is also being expanded from focus only on recovery of systems to true business continuity, addressing not only the recovery of systems, but allowing employees to continue to work in the case of a shutdown. In addition, as part of our ongoing reorganization efforts, we plan to enhance the staffing and reporting lines in the continuity unit, reflecting our commitment to improvement in this area.

The Department response was provided on June 14, 2005, by Jay Carlson, Deputy Director/Bureau Manager, Bureau of Communication and Computer Services of the Department of Central Management Services.

SERVICE ORGANIZATION - DESCRIPTION OF CONTROLS

The following Description of Controls section (pages 7 through 21) consists of text provided by the Department of Central Management Services.

ADMINISTRATION

The Department of Central Management Services' (Department) Bureau of Communication and Computer Services (Bureau) is statutorily mandated to provide "use of electronic data processing equipment, including necessary telecommunications lines and equipment, available to local governments, elected State officials, State educational institutions, and all other governmental units of the State requesting them." (20 ILCS 405/405-250) To fulfill this responsibility, the Department operates the Central Computer Facility (CCF), the Communications Center and various branch facilities.

The Bureau currently has eight Divisions:

- Information Management Systems
- Information Services Division
- Customer and Account Management
- Administration and Planning
- Illinois Century Network
- Infrastructure Systems
- Local Area Network
- EPMO

A reorganization is underway that will reflect changes in progress within the Bureau and the State. The proposed organization chart will add the following major operating Divisions:

- Enterprise Architecture and Strategy
- Workforce Logistics

The new organization should be effective during FY 2005, and refinements and augments will continue into FY 2006.

The Department has established an IT and Telecommunications Governance model to help oversee rationalization, standardization, centralization and consolidation efforts. The Governance model is a set of political processes, driven by business and technology principles to ensure that IT investment meet the following objectives:

- Alignment of IT/Telecom with the Enterprise goals and realization of the promised benefits.
- Use of IT/Telecom to enable the enterprise by taking advantage of opportunities.
- Optimize use of IT/Telecom resources.
- Management of IT/Telecom-related risks.

An Architecture Review Board (ARB) and an Enterprise Architecture and Strategy (EA&S) group have been established with staff from various agencies to assist with the governance and standardization efforts.

The CCF Command Center operates twenty-four hours a day, seven days a week, 365 days a year. The Command Center is responsible for the monitoring of systems, responding to system messages, and logging problem calls. The monitoring of systems is divided among the operators.

The Department dedicates a great deal of resources to ensure proper training and cross training of employees. Training is provided through scheduled classes at the Capitol City Center, arranging for special classes, external training classes, and via use of purchased self-training packages. In addition, employees are continuously receiving on the job training. Through the Rationalization Project the Workforce Logistics group will manage the training function.

The Department procures computer equipment and software to be utilized by State agencies in accordance with Article 20 of the Illinois Procurement Code and the internal procurement policies and procedures established by the Bureau of Strategic Sourcing and Procurement. The Department determines need based on function and potential users. The Department has three enterprise licensing agreements related to technology. The Department monitors the agreements on a continuous basis.

The Department has developed three planning documents to aid in promoting long-range information technology planning:

- Environmental Overview-January 26, 2005,
- Information Technology Rationalization Plan-January 1, 2005, and
- Telecommunications Rationalization Plan- January 1, 2005.

In accordance with Executive Order 10, the internal audit functions for each agency, office, division, department, bureau, board and commission directly responsible to the Governor were consolidated under the jurisdiction of the Department of Central Management Services as the Illinois Office of Internal Audit (IOIA).

A statewide Information Technology (IT) audit function was developed as part of the IOIA to address those entities under the Governor's jurisdiction. IT is addressed on a statewide basis, which reduces duplication of efforts and increase efficiencies. IOIA perform various types of IT audits including system development audits, application audits, special audits, and internal audits.

The Fiscal Control and Internal Auditing Act mandates IOIA review the design of major new electronic data processing systems and major modifications to those systems. IOIA is in the process of establishing procedures for identifying major new systems and major changes to existing systems for system development audits to determine which systems development projects are major and require an audit.

The Department is required to establish charges for statistical services requested by State agencies and provided by the Department. In addition, the Department is responsible for the centralized communication services among all State agencies. The Department operates two internal service funds in regards to billing information supplied from the Statistical Services Revolving Fund (SSRF) and the Communication Revolving Fund (CRF).

The KOMAND IV system (system) is the primary system used to compile the SSRF billing. The system provides a means for charging resource utilization data back to the users of the computer systems. Users are billed for various services, such as use of the Local Area Network, on-line storage, secure cards, mainframe usage, and print jobs. In addition, users are charged for the usage of the “Common Systems”: Accounting Information System; Central Inventory System; Central Time and Attendance System; and Central Payroll System.

The Department has developed procedures for each phase of the SSRF billing process. At the end of each phase, verification is performed to ensure all totals are correct. Reports from each source are verified against each other to ensure accuracy of the information. Throughout the process, an “Edit Check” is conducted to ensure completeness and accuracy of each phase.

In order to comply with the requirements of the federal Department of Health and Human Services, the Department performs an annual analysis of the previous year’s cost, by service center, to determine the profit/loss for each service. Excess revenues are returned to the user entities.

Each month the Department receives billing information for communication services from the various vendors. The information is compiled to produce the CRF billing for users. Users are charged for usage of voice and data service, cell phones, pagers and communication equipment.

The Department is in the process of implementing a new billing system for the CRF billings. The billing system, Expense Management System 11 (EMS) is expected to be in production by the end of FY05, and refinements and augments in FY06.

The Department requires the agencies to remit the total amount on the invoice. Payment is to be made within one billing cycle of receipt. The Department’s Accounting Division is responsible for pursuing outstanding SSRF and CRF accounts. If an agency persists in not paying delinquent amounts, the Department’s Director will send a letter to the Director of the delinquent agency requesting payment.

In December 2004, the Department implemented the Billing Allocation System (BAS). BAS provides memorandum billings to agencies, documenting the Department’s spending in support of consolidated services; Internal Audit, Legal, Facilities Management, Public Information Office, and IT Consolidations.

CONTINGENCY PLANNING

The Department of Central Management Services (Department), Bureau of Communication and Computer Services (Bureau), is mandated to provide computing services to agencies of the State of Illinois. In the event a disaster, the Bureau would provide disaster recovery service in order to minimize the risk of disrupted services or loss of resources.

The Department has developed four written disaster recovery plans for the restoration of the State’s data center and critical applications:

- State of Illinois, DCMS, BCCS, ISD, Continuity Methodology-Revised January 3, 2005,
- State of Illinois, DCMS, BCCS, ISD, Recovery Activation Plan-Revised December 20, 2004,
- State of Illinois, CMS, LAN, Recovery Activation Plan-Revised August 11, 2004, and
- State of Illinois, DCMS, Division of Telecommunications, NCC, Recovery Activation Plan-Revised February 6, 2004.

The Department has appointed a Continuity Services Manager and Continuity Services Specialist to assist in updating, testing, and reviewing the disaster recovery needs of the State and the Department.

The Department has arranged for four satellite facilities in the Springfield area for providing disaster recovery services. In addition, the Department has contracted with a disaster recovery service provider for out-of-state recovery locations, in the event of a regional disaster. The Department's satellite facilities are available to any State agency for recovery purposes. It is the responsibilities of the State agency to contact the Department for usage of a satellite facility.

The Department strives to conduct testing at the out-of-state recovery locations annually. Additionally, testing is conducted at the Department's satellite locations. State agencies may conduct testing at any of the Department's satellite locations.

The Department maintains a Statewide Critical Application Listing based on information received from State agencies. State agencies are to prioritize their applications in one of five categories:

- Human Safety (Category One)-Resources that directly impact the lives and safety of Illinois citizens, including state employees;
- Welfare Human Services (Category Two)-Resources that directly impact the well being of Illinois citizens;
- Non-Welfare Human Services (Category Three)-A human service resource that directly impacts the welfare of Illinois citizens;
- Administrative State Functions & Processes (Category Four)-Resources that support the administration of state processes; and
- Support of Specific Agency Functions & Processes (Category Five)-Resources related to the maintenance of a specific agency function or a process.

In the event of a regional disaster the Department will only recovery Category One applications for those State agencies that have met the requirements. State agencies with Category One applications are required to conduct testing at one of the Department's satellite facilities on an annual basis. Additionally, the State agencies are to provide the Department with a copy of their disaster recovery plans and submit results of their annual tests.

The Department conducts nightly backups of its environment. State agencies' data residing on the Department's mainframe are backed up with the Department's nightly cycle. The Department utilizes three off-site storage facilities for storage of critical information, in addition to an out-of-state storage facility.

In order to mitigate the risk of a power failure, the Department's data center is fed by two different sources. In the event one source fails, the other source will become active. In addition, the Department has installed an uninterruptable power supply (UPS). Within an allotted time the Department's generators will kick in. The Department has in place a service contract for the UPS to provide routine preventive maintenance and remedial services as required.

The Department has developed procedures for the restart and recovery of applications and systems. Restart and recoveries may occur for various reasons other than a disaster, such as hardware failure, new maintenance levels, new software releases, and job failures. Departmental staff are continuously updating and training in regards to the procedures.

COMPUTER OPERATIONS

The mission of the Command Center is to provide continuous monitoring and operation of the Department of Central Management Services, Bureau of Communications and Computing Services (Bureau) computing resources to ensure availability, performance, and support response necessary to sustain customer business demands.

The Command Center is responsible for documenting all daily actions and events that affect the status of the computing environment and customer business functions. Additionally, the Command Center maintains availability and functionality of computing resources as scheduled in support of customer business needs and coordinates and oversees implementation of changes to the computing environment.

The Department has established a Change Control Committee to review changes to technology that affect operations. Change control procedures also exist within each business unit. Every Wednesday a videoconference meeting is held with the Change Management Members. The Change Management Members are composed of appointed individuals from the divisions and business units, as well as other areas that provide foundation support to the Department for providing its technology services. The members review the change requests that have been submitted during the past week. During the meeting the change owner or a representative is to attend the meeting to represent their submitted request. The meetings are used to clarify questions regarding the nature and scope, as well as review impact and address concerns or questions regarding pre and post testing and acceptance of the change as well as review customer notification process.

The Department currently has three separate systems which document tracking of changes to the various environments. However, the Department is in the process of implementing a consolidated enterprise change management system, which is to be in production by the end of FY05.

The Department has established procedures relating to change management. All change requests are assessed by each technical area to determine any adverse issues. We have a plan to add additional staff to assist with this function.

The policies and procedures list the change management testing levels, scope of tests, and the extent of testing required for each level. Due to the various types of changes, each section

throughout the Bureau has its own policy/procedure for testing and maintaining documentation. Each section manager determines the method, extent, and retention period of testing.

The Data Processing Guide and the Problem/Change Management System procedures provide characteristics and guidelines for emergency changes as well as procedures for emergency change requests. Emergency changes do not adhere to the normal change procedures since emergency changes require immediate implementation and have unique characteristics.

The Department maintains several reports that record the Command Center activities. The following reports provide a complete record of all operator actions: SYSLOG, Shift Change Checklist, Telephone Report, Weekly Telephone Summary, and the Daily Shift Report.

In addition, the Department utilizes InfoMan, a management tool, to record and monitor the progress of problem resolutions. The Department's objective is that 90% of the problems be resolved within their designated timeframes.

The Department collects, reviews, and analyzes operating statistics to identify trends, detect problems, and project future resources through the following reports:

- Availability Report - reflects the system and application availability on a daily and weekly basis.
- Resource Management Facility Report - reflects CPU utilization by system and machine, as well as the average and maximum number of users at any one time.
- D-Collect Report - reflects space, allocated space versus space used.
- Tape Media Report - reflects the demand for tapes and cartridges.
- Command Center Telephone Calls and Print Shop Report - reflects the number of calls received and the volume of printing.

SECURITY CONTROLS

The Department of Central Management Services, Bureau of Communication and Computer Services, Central Computer Facility was built in 1980, and was designed to meet the State's data processing needs. The Central Computer Facility is monitored 24 hours a day, 7 days a week. Access is restricted at all times.

The IT rationalization process will expand the need for security administration. Additional staff are planned to cover all security functions.

The Department has issued several security policies relating to information technology:

- CMS Policy Manual,
- CMS Information Technology Security Policy, dated December 2001,
- Statewide Internet Security Policy, dated December 2001,
- Information Security Policy - Local Area Network (LAN)/Office Automation (OA), dated May 1995, and
- Statewide Information Security Policy BCCS/CCF Internal Policy, dated February 4, 2003.

Over the past year the Department has developed a website which provides links to the above security policies, security sites and provides information regarding contingency planning www.state.il.us/cms/saa/default.htm

The Department has assigned the responsibility for all aspects of computer security to the Security and Availability Division. The Security and Availability Division duties currently include:

- Working with internal and external auditors.
- Ensuring security awareness communications and training are provided and enhanced.
- Developing solutions for identified security issues.
- Reviewing, testing and evaluation the IT security systems, policies, and procedures.
- Directing the Department of Central Management Services (Department) Information Technology security administration program.
- Oversight for the State of Illinois PKI Certificate Authority.
- Oversight of the Enterprise Change Management program for the agencies involved in rationalization.
- Reviewing the Department's Disaster Recovery program.

The Security Task Force was composed of representatives from various divisions within the Department, with the responsibility of updating security policies and promoting security awareness. In May 2004 a communication was sent to the Security Task Force members informing them a review was underway to determine the effect of the Task Force objectives given the organizational changes, which are being implemented. The Security Task Force functions were determined to be addressed by other business objectives in the following manner. The Security and Availability Division has been tasked the objective of meeting HIPAA Security regulations by April of 2005. The Security and Availability Division has also had a goal to update the security policies for the Department.

The Department's Regional Offices, the Telecommunications Building, the Administration and Planning Building, Benefits Building and the Central Computer Facility each have Facility Managers.

The Department utilizes an access card system to provide control over access to many of its facilities. The system's readers are proximity readers that control and log the use of all access cards throughout the day at the Central Computer Facility, Telecommunications Building, the Benefits Building, and the Administration and Planning Building.

The Statewide Information Security Policy requires all employees, visitors, vendors/contractors, and State agency representatives to be assigned an access card with appropriate access rights. Requests for cardkeys are submitted to the Security and Availability Division for approval. An individual's access rights are based on their job duties. Visitors and employees who forget their access card are required to sign-in and register at the guard's desk.

The Department has installed a fire suppression and detection system (System) at the Central Computer Facility. The System is approved by the Underwriters Laboratory, and utilizes an environmentally friendly gaseous agent. Additionally, the Department has installed smoke detectors, which are connected to the alarm system and local fire/police. The Department's

Telecommunications Building and the Administration and Planning Building each have fire detection and suppression systems, smoke detectors and fire extinguishers.

The Department has contracted with a janitorial service to perform duties on a daily, weekly, and monthly basis. The contract outlines the duties and timing of the duties to be performed. The janitorial employees are granted access to all areas throughout the facilities. The Department conducts background checks and training for each janitorial employee.

The Tape Library is located at the Central Computer Facility. Access to the Central Computer Facility and the Tape Library requires an access card with appropriate access rights. The “Library Services Vault Transmittal Procedures” outline the procedures to be conducted during the movement of media.

The user agency is responsible for sending a request for movement of their media. The Tape Management System is utilized to track and record the location of media.

Twice a year, the Acting Security Administrator sends user agencies a Security Authorization List, an Information Management System Authorization List, and a Tape Diskette Authorization List, which are to be updated and returned within two weeks.

The Department maintains off-site storage at three locations: two in the Springfield area and the regional location.

APPLICATION SYSTEMS DEVELOPMENT

The Department of Central Management Services (Department), Bureau of Communication and Computer Services (Bureau), Application Systems Development Section (ASD) is responsible for the development of computer systems that are available for use by user agencies and by the Department.

The Department has developed the ASD Methodology, and the Standards and Documentation Requirements to guide new system developments and modifications to existing systems. The ASD Methodology provides a structured process for the design, development and implementation of new systems, enhancements, maintenance and ad hoc requests. The Standards and Documentation Requirements provide standards for new systems, enhancements, maintenance, and ad hoc requests.

The ASD Methodology outlines four phases, which are required to be completed in sequence:

- Problem Definition and System Planning,
- Design,
- Development/Implementation, and
- Post-Implementation Review.

The Department established a Standards Committee to review and approve changes to the ASD Methodology.

The Service Request (SR) Form is used to initiate a systems development project. The Service Request Registration System registers projects, assigns a unique SR number and records the status of the project. In addition to the Service Request Registration System, the Department

utilizes the following tools to assist in tracking projects, assigning resources, and scheduling time:

- Microsoft Word,
- Microsoft Project,
- Quality Assurance (QA) Project Tracking System, and
- Service Request Registration System (SRRS)

The Department's ASD Methodology documents user involvement in all four phases. Users of the new development/modification are interviewed and requirements outlined in phases one and two. The user tests and validates the new development/modification in the third phase and a user questionnaire may be used in the fourth phase.

The Department has developed a Quality Assurance Team to monitor and verify that projects adhere to the ASD Methodology. The QA Manual provides guidance to Quality Assurance staff for each phase of a development/modification. In addition to the QA Manual, Quality Assurance utilizes a checklist to identify required tasks for each project.

Library Control is responsible for all mainframe movement of programs in a production library. The Program Library Procedures provide guidance for ensuring new programs or modifications are documented and approved before production moves are performed. A Library Control Form must be completed and approved before a move is made.

TELECOMMUNICATION CONTROLS

The Department of Central Management Services is mandated to provide and control the procurement, retention, installation and maintenance of the State's telecommunication equipment and services. The Department provides local telephone services, telecommunication equipment, software, installation, maintenance and network services to all State agencies.

The Department maintains network diagrams, which document the host-to-mainframe connections, network control program connections, State agency users, and the Systems Network Architecture network interconnects to both State and private data centers. The Transmission Control Protocol/Internet Protocol network diagram documents direct connections for user agencies.

Effective July 1, 2004, the Department assumed control of the former Illinois Century Network (ICN), which managed a statewide data network primarily for the use of educational institutions. The Department is in the process of merging the State's network and the ICN network. This merger of the networks is expected to be completed during FY05.

The Department had established procedures relating to telecommunication changes: The Guide to Telecommunications Services and Procedures (Guide). The Guide outlines the telecommunication process, including changes and user agency responsibilities. The Department utilizes the Management of Network Income Expense Services System (MONIES) to track changes. A user's guide provides instructions relating to MONIES.

During FY05 the Department will be replacing MONIES with EMS.11. Production is expected at the end of FY05.

A Telecommunication Data Service Request (TDR) is completed for equipment changes; a

Terminal Generation Request (TGR) is completed for software changes; and a Telecommunication Service Request (TSR) is completed for voice equipment, LAN installations, and fiber optics. Requests are submitted by the user agencies to the Department's Distributive Support Section and the Telecommunications Voice Provisioning Section.

The Department has established a central help desk function, the Communication Solution Center (CSC) and the Communication Management Center (CMC). The CSC will provide tier 1 support during business hours. The CMC will operate 24x7 365-days per year providing tier 1 support during non business hours and tier 2 support all hours. It will provide backup to the Command Center. The Centers provide support for voice, data, cellular, IWIN, paging, and videoconferencing provisioning and support. The CMC also performs network monitoring, diagnostics and repair dispatching for the ICN Network.

The Department is in the process of implementing a Remedy-based trouble ticketing system to be used by the CSC and CMC.

The Department utilizes the following diagnostic equipment in identifying problems:

- Sniffer,
- Telecommunication Protocols,
- Timeplex Hardware,
- Error Logging, and
- Alarm Conditions.

The Telecommunication staff are alerted to problems.

The Department maintains and supports the hardware, software, communication devices, and related services for the several agencies. Additionally, there are agencies, which use the Department's LAN connections for email purposes.

The Department is in the process of consolidating the IT infrastructure operations of twelve agencies. The first phase consists of transferring administrative control through Interagency Agreements and the transfer of infrastructure employees to the Department's payroll. This phase should be completed during FY05. Physical consolidation will begin during FY06. The infrastructure services to be provided will be governed by Service Level Agreements, which are agreed to by both the user agency, and the Department. These documents are in development.

The Department maintains and supports the firewall and software that connects the Central Computer Facility and the Harris Facility to ICN, which provides the connection to the Internet. There have been several hundred circuits migrated. All circuits should be migrated by the end of the fiscal year. The Department provides Internet Service Provider-based services for State agencies.

The Department has established two Internet security policies, which are available on the Department's Intranet:

- Statewide Internet Security Policy, dated December 2001, and
- CMS Information Technology Security Policy, dated December 2001.

The policies provide for minimum-security practices when establishing a connection to the Internet. Additionally, the Statewide Internet Security Policy requires all State agencies to obtain their Internet access through the Department. The Director of the Department must authorize all exceptions. Additionally, agency configurations will be reviewed and approved before access is granted. In the event agency configurations are changed, the agency must obtain approval from the Department. The Department does not monitor Internet usage; rather that responsibility rests with the user agency.

The Department utilizes an auditing software to monitor users. The reports are run monthly to ensure compliance with Departmental policies and to identify any security weaknesses.

The Department and Illinois State Police (ISP) have coordinated efforts to provide the Illinois Wireless Information Network (IWIN), a wireless wide area data network using Cellular Digital Packet Data (CDPD). The Department administrates the IWIN network and ISP provides the connection to the Law Enforcement Agencies Data System (LEADS), National Crime Information Center (NCIC), Secretary of State, National Law Enforcement Telecommunications System (NLETS), and Criminal History Record Information (CHRI) that the network utilizes to provide information to IWIN users.

The "Illinois Statewide Policy Manual," located on the Internet, outlines the responsibilities for the Department, ISP, local agency IWIN coordinator and the IWIN user, as well as appropriate usage, necessary certifications to obtain IWIN access and Motorola client functions.

Transmissions are sent from the users' Mobile Data Computer (MDC), equipped with the client software Premier MDC, to the nearest cellular tower equipped with CDPD equipment via a dedicated channel. The Department has a contract with Verizon Wireless (Verizon) to provide cellular towers throughout the State, as well as with Motorola to provide the software utilized by the IWIN network. Once the cellular tower has received the transmission from the user's MDC, the transmission is then forwarded to a Verizon -owned and -operated messaging switch. From the messaging switch, the transmission is forwarded to one of the Department's redundant Premier MDC Servers and then to the Department's network for access to the appropriate data. Redundant routers, maintained by SBC Ameritech, connect the Department's Premier MDC Servers to the Verizon Network.

SYSTEM SOFTWARE CONTROLS

The primary operating system at the Department of Central Management Services Central Computer Facility is Zero Downtime Operating System (z/OS). Z/OS is a complex operating system used on mainframes and functions as the system software that controls the initiation and processing of work within the computer.

The Department utilizes security software to secure libraries, protect resources, and datasets in the z/OS environment. Additionally, the System Management Facility secures the necessary documentation of the activity in the installation.

System changes follow the Department's Info Change and Problem Management procedures. There are three types of changes that may occur to the z/OS environment: reported problems that can be isolated to a specific module, Program Update Tapes, and new versions or releases. Initial Program Load requests are handled in the same format.

The Department's secondary operating system utilized at the Central Computer Facility is Virtual Machine (VM). VM is time-sharing, interactive, multi-programming operating systems for IBM mainframes.

User agencies must go through the Department to submit and obtain a VM User ID. User agencies are assigned IDs with the most restrictive security rights. The VM directory, which contains information regarding user IDs, mini-disk size and location, and operating functions, is restricted.

DataBase 2 (DB2) is a relational database management system for z/OS environments that the Department makes available to user agencies. The Department has established ten+ subsystems at the Central Computer Facility and the Department's off-site location.

The Department has assigned staff to monitor the performance and problems of DB2. The DB2 staff is responsible for software installation, maintenance and security. Another is the Database Administrator, who acts as the liaison for user agencies.

All users who access DB2 are required to have a security software ID and password. The user must authenticate to through the security software first. If the user authenticates, DB2 allows access. DB2 internal security verifies access rights to specific data. The Department authorizes one user ID at each user agency to coordinate the use of DB2 within the agency. This user ID allows each agency to create its own authority.

The DB2 Software Support Group monitor specific application problems when users call. System performance is monitored on a continuous basis. The Department's Information Management System is utilized to report and document problems.

The Customer Information Control System (CICS) is a software product that enables online transaction processing. CICS allows numerous transaction types, entered from multiple terminals, to be processed concurrently by user-written application programs. CICS acts as an interface between the operating system and application programs.

The Department offers three different levels of CICS support for user agencies, described as follows:

- **Level One** – The Department supports only the CICS software. The user owning agency

is responsible for all security for their CICS regions.

- **Level Two** – The Department supports the CICS software, and maintains CICS System Definition File (CSD)/table definitions for the user agency. The user agency supplies the definitions to the Department and controls the application support. The Department and the user owning agency share security responsibilities.
- **Level Three** – The Department supports the CICS software, maintains CSD/table definitions, and supports both CICS and the application software for the agency. The Department is also responsible for security for these regions.

Production regions are segregated from test and development regions to restrict access, based upon the various needs for each type of region. Restricted access to sensitive CICS transactions is established over production regions. Test regions have fewer access restrictions. Test regions allow programmers to test and debug against non-production files.

Information Management System (IMS), which is an online database software subsystem, used as the control architecture under which online database system applications process. An IMS system is capable of running many different applications within a single definition of one or more “Message Processing Region” and one “Control Region.” Currently, there are three production IMS regions with 10+ testing regions.

The Department utilizes security software to control access and protect resources. The security software is the primary tool for controlling and monitoring access to the Department’s computer resources. A user ID is used to identify the user and a password to verify the user’s identity. The Department maintains a log of all access attempts, which is used to monitor unauthorized access attempts and identify areas of weakness. User agencies are responsible for protecting their own programs and data.

The Department has appointed staff with primary responsibility for the implementation and administration of the security software. The Department has an informal procedure in place for the monitoring of security violations. The Security Administrator reviews violations and select violation reports are distributed to users requesting explanations and are required to be returned with an explanation.

APPLICATION CONTROLS

The Department of Central Management Services, Bureau of Communication and Computer Services (Bureau) has developed four applications that are used by multiple State agencies. The applications known as the “Common Systems” are:

- Accounting Information System (AIS),
- Central Inventory System (CIS),
- Central Payroll System (CPS), and
- Central Time and Attendance System (CTAS).

The Common Systems run on the Department’s mainframe, processing millions of transactions each month. Each Common System is available for use during business hours and on a limited

basis on the weekends.

Each Common System is secured using security software, in addition to internal security requirements. Users must have an authorized ID and password to gain access. Assignment and authorization of access rights is the responsibility of the user agency. Once access has been gained to the operating system, users must have a separate application user ID and password to gain access.

Changes to the Common Systems are controlled through the Application Systems Development Methodology. Changes are initiated through the use of a Service Request Form. The changes are approved and tested before implementation into the production environment. The Library Control Group will then move the change into production.

The Common Systems are backed up daily, weekly and monthly using CA-Scheduler. Backups are maintained at the Central Computer Facility and the off-site storage locations.

Accounting Information System (AIS)

AIS functions as an automated expenditure control and invoice/voucher processing system. AIS, in processing invoices, allocates invoice amounts into sub accounts; groups invoices, according to the Comptroller's Statewide Accounting Management System (SAMS) procedures, for the preparation of vouchers; and allows users to track cost centers. AIS has an interface with CIS.

The Department has developed a user manual, the AIS User Manual, which is located on the State's Enterprise Web Server (Intranet). The manual provides guidance to the user when utilizing the various functions.

AIS transactions are entered online in a real-time environment, with the ability to batch transactions for processing at a later date. AIS was developed with edits that force correction of errors and completion of critical fields before a transaction is accepted. All data entry is performed by user agencies and is the responsibility of user agencies.

AIS provides various on-line and batch reports to assist in the balance of transactions. A complete listing of the various reports is maintained in the AIS Users Manual. Retention of the various reports is the responsibility of the user agency.

Central Payroll System (CPS)

CPS is an online and batch system that standardizes payroll procedures for State agencies. CPS enables State agencies to maintain automated pay records and provides a file that is submitted to the Comptroller's Office for the production of payroll warrants. CPS has an interface with CTAS.

The Department has developed a user manual, the CPS User Manual, which is available from the Department. The manual provides guidance to the user when utilizing the various functions.

Data is entered online by user agencies. CPS has online edit checks and corresponding messages

which are displayed online when an error occurs. The error must be corrected before finalization of the transaction. The Department has procedures in place to handle errors that occur during processing.

For each pay period there are six standard reports that are printed and provided to agencies. The reports are printed at the Central Computer Facility for agency pickup. Twice a year agencies are requested to update the Tape, Print and Diskette Authorization Listing. Individuals must be listed in order to pick up reports. Retention of the reports is the responsibility of the user agency.

Central Inventory System (CIS)

CIS is an online real time system; therefore, inventory data is updated immediately to reflect the transactions entered. CIS has the ability to utilize an optical scanner to read bar code labels during a physical inventory. CIS allows user agencies to maintain records of inventory and to comply with the Department's Property Control Division's rules of reporting and processing. CIS has an interface with AIS.

The Department has developed a user manual, the CIS User Manual, which is available from the Department. The manual provides guidance to the user when utilizing the various functions.

Data is entered online by user agencies. CIS has several edit checks to alert users of errors. Errors must be corrected before the transaction is accepted. The Department generates a Location Balance Report nightly to determine whether transactions processed correctly. Additional reports are available to users. The accuracy and reconciliation of data is the responsibility of the user agency.

Central Time And Attendance System (CTAS)

CTAS is an online system used to maintain current available benefit time. Additionally, CTAS allows user agencies to monitor whether usage of time is in accordance with State rules. CTAS provides for attendance information to be recorded using either the positive or exception methods. CTAS interfaces with CPS.

The Department has developed a user manual, the CTAS User Manual, which is available from the Department. The manual provides guidance to the user when utilizing the various functions.

Data is entered online by user agencies. CTAS has edit checks to alert users of errors. Transaction with errors will be rejected. CTAS provides online and batch reports that user agencies may use for reconciliation purposes. During the "close" process, CTAS generates error reports, reconciliation reports, and file maintenance activity reports. All transactions must be reconciled before the "close" process can be finalized. The accuracy and reconciliation of data is the responsibility of the user agency.

This Page Intentionally Left Blank

SERVICE AUDITOR
DESCRIPTION OF TESTS AND OPERATING EFFECTIVENESS

We reviewed or confirmed data processing general and application controls at the Department. Using the Department's Description of Controls as the foundation for our review, we performed tests to determine compliance with policies and procedures, conducted interviews, performed observations, and identified specific control objectives and procedures we considered necessary in the circumstances to evaluate the controls.

The results of our review are included in the General Controls and Application Controls sections of this report.

This Page Intentionally Left Blank

GENERAL CONTROLS

General controls are the methods, policies, and procedures adopted by an organization to ensure the protection of assets, promotion of administrative efficiency, and adherence to management's standards and intentions.

The general controls review consisted of an evaluation of the controls in seven distinct areas:

- Administration;
- Continuous Service;
- Computer Operations;
- Security;
- Application Systems Development;
- Telecommunication; and
- Systems Software.

The Third Party Review addresses each general control area in a separate control section of this report.

This Page Intentionally Left Blank

ADMINISTRATION CONTROLS

Administration controls include the procedures necessary to ensure that resources are used efficiently and in accordance with management's intentions. They encompass the overall operation of the computer facility.

Administration controls also include functions that maximize organizational efficiency and productivity. Organizational efficiency can be directed through long-range planning efforts and effective personnel policies. Productivity in the computer facility is enhanced by adherence to standards.

We reviewed administration controls and noted the following:

Communication

Control Objective - Management should ensure that it effectively communicates with staff and user agencies to ensure an awareness and understanding of its decisions and direction.

Tests Performed - We reviewed Rationalization project documentation and interviewed staff members.

Results - The Department is undergoing a significant transformation of the State's IT environment, practices, management, and staffing. During our review it became apparent that key managers and staff were unaware of significant changes that would affect their area of responsibility. Since staff are a primary control mechanism, a lack of communication could have an adverse impact on the control environment.

Personnel Policies and Procedures

Control Objective - Management should ensure that personnel policies, procedures and practices provide for clearly defined position descriptions, organizational separation of duties, adequate staffing and qualifications, and satisfactory training programs.

Tests Performed - We reviewed segregation of duties, training programs, and staffing levels.

Results - The Department maintains job class specifications and position descriptions. The position descriptions contain the position title, effective date, location, agency, division within the agency, description of responsibilities and percentage of time spent on each duty, name of the immediate supervisor and position title, and qualifications required for the position.

As part of the Department's Rationalization projects, the position descriptions are being reviewed and rewritten to reflect the new organizational structure and employees' actual duties.

As part of the Rationalization projects, 11 agencies will merge IT staff into the Department by June 30, 2005. During the merger, the Department is evaluating staffing and skill levels associated with various positions. The Department expects a complete reorganized structure by June 30, 2005.

Since the Department is in the midst of its reorganization and merger, a staffing analysis and comparison to prior years is not practicable. However, we have determined the Department is currently understaffed in some key areas and employees are taking on many more duties than delineated in their job descriptions. Projects are being reprioritized and administrative duties such as documentation are being set aside in order to ensure the day-to-day work can be completed.

As part of the Rationalization projects, the Department is reviewing its orientation program and overall training requirements and budget.

The Command Center at the CCF operates 24 hours a day, 7 days per week, 365 days per year. Operations management stated that each of the shifts (two per day) were designed for four operators and one supervisor, with each operator working a 12-hour shift, one hour being for lunch. The Command Center is responsible for the monitoring of the systems, responding to system messages, and logging of problem calls. We reviewed the timesheets for the Command Center for the period December 1, 2004 through February 15, 2005, noting:

- Of 154 shifts, only 26.5 had supervisors present;
- None of the 154 shifts had the required staffing level (4 operators and 1 supervisor); and
- 1,016 hours of overtime were worked costing approximately \$28,214.

Interagency Agreements

Control Objective - Management should establish a service level agreement process/framework/methodology, which formalizes the performance criteria against which the quantity and quality of service will be measured.

Tests Performed - We reviewed interagency agreements and documents associated with the IT Rationalization project.

Results - The Governor's Executive Order 2003-10 and Public Act 93-839 authorized the Department of Central Management Services to consolidate various functions of State government, including Information Technology (IT). In order for the Department to carry out the consolidation activities, an IT Rationalization project was initiated. The goal of the IT Rationalization project is to centralize IT functions for agencies under the Governor, thus enhancing the Department's efforts as a service bureau.

The following agencies were participating in the consolidation project:

- Department of Agriculture;
- Department of Commerce and Economic Opportunity;
- Department of Employment Security;
- Department of Financial and Professional Regulation;
- Department of Human Services;
- Department of Natural Resources;
- Department of Public Aid;
- Department of Public Health;
- Department of Revenue;

- Department of Transportation; and
- Environmental Protection Agency.

To implement the consolidation of IT functions, the Department developed three types of agreements.

Interagency Agreements

Interagency agreements outline the responsibility of the agencies in relation to the employees, assets, contracts, and appropriations affected under the IT consolidation. Until employees and assets are physically moved to the Department, they will remain at the agencies, but under the Department's control.

Federal Funding Interagency Agreements

The Department and agencies, which receive federal funding for IT services, entered into Federal Funding Interagency Agreements. These agreements outline criteria for the billing of services and require the Department to provide the agency with documentation regarding infrastructure expenditures, which the agency may submit to the federal government for reimbursement.

Service Level Agreements

These agreements outline the terms and conditions under which the Department will provide specified IT services to an agency. The objective is to provide a basis and framework for the delivery of high quality services that meets the needs of the agency.

According to the agreement, the "Standard Services" the Department will provide include:

- Mainframe Services;
- Midrange Services;
- Desktop/End User Support Services;
- Security Management Services;
- Data Communication-LAN Services;
- Data Communication-WAN Services;
- Telecom-Voice/Video Conference Services;
- Help Desk Services;
- Backup, Recovery, and IT Recovery Services; and
- Common Application Services.

The following terms and conditions are included in the agreements between the Department and each agency:

- Defining the services;
- Minimum service levels;
- Availability, reliability, and growth;
- Continuity planning;
- Security requirements;
- Change procedures for any portion of the agreement;
- Content and frequency of performance reporting; and
- Charges for services.

Software Licenses

Control Objective - Management should ensure that software licensing is controlled, monitored, and reflects the needs of the department.

Tests Performed - We reviewed enterprise licensing agreements and Rationalization project documentation.

Results - As part of the Rationalization projects, the Department established an IT and Telecommunications Governance model to help oversee rationalization, standardization, centralization, and consolidation efforts. The Governance model is a set of political processes, driven by business and technical principles to ensure IT investments meet the following objectives:

- Alignment of IT/Telecom with the Enterprise goals and realization of the promised benefits;
- Use of IT/Telecom to enable the enterprise by taking advantage of opportunities;
- Optimize use of IT/Telecom resources; and
- Management of IT/Telecom-related risks.

The Architecture Rationalization Board (ARB) is a “cross-Agency authority established to facilitate the IT and Telecom Governance of the State of Illinois. The intent of the ARB is to assure alignment of the IT portfolio, and adherence to Standards concerning the deployment of IT and Telecom. It is not intended as a review process to challenge or critique Agency direction. The goal is to assure that Agency initiatives are aligned with the State of Illinois IT Master Plan, and that the resultant products conform to established IT Standards and architecture.”

The Enterprise Architecture and Strategy (EA&S) was developed to ensure that “IT investment decisions are aligned with EA&S vision and goals and deliver outcomes that keep in step with the accelerating pace of business changes. Working with the Executive Team and the ARB, EA&S will: help create the IT Strategy and Enterprise Architecture vision, develop standards and reference architectures, create IT transition plans, and provide assistance to the central IT organization.”

The Department has enterprise licensing agreements with three vendors.

Long-Range Planning

Control Objective - Management should continually monitor and assess trends, risks, and conditions to ensure that the technological infrastructure supports, and will continue to support, the missions and objectives of the department.

Tests Performed - We reviewed documents associated with the IT and Telecommunications Rationalization projects.

Results - The Governor ordered the consolidation of the State’s IT services in the Department, tasking the Department with rationalizing and improving IT services. The Department has

embarked on Rationalization projects to comply with the Governor's directive.

Internal Audit Coverage of Information Systems

Control Objective - Management should ensure that Internal Audit routinely reviews information technology integrity and security issues. Management should also ensure that the Internal Audit division complies with the statutory mandate (30 ILCS 10/2003a (3)) to review the design of major new systems and major modifications to existing systems before their installation to ensure that the systems provide for adequate audit trails and accountability.

Tests Performed - We reviewed planning documents, the Annual Report, and a listing of audits completed and in-progress.

Results - On March 31, 2003, the Governor signed Executive Order 2003-10 to consolidate internal auditing activities under the Department of Central Management Services. On October 1, 2003 the Illinois Office of Internal Audit (IOIA) was officially established as the internal auditor for executive agencies.

A contractor has been assisting the IOIA since late November 2003 with a statewide risk assessment/management model to assess risk, determine audit frequency, and alert management to areas that require additional attention and oversight. A two-year audit plan that incorporated the statewide risk assessment was approved by the Governor's Office on June 30, 2004. Per Department staff, based on the IT risk assessment, the FCIAA risk assessment, and the database of system development projects, the two-year audit plan included audits of general controls, security, applications, and system development reviews.

Additionally, by late fiscal year 2004, IOIA began implementing a more comprehensive program to gather information regarding system development projects, which are in progress or planned at the various agencies. During fiscal year 2005 IOIA had performed general IT work in various areas of the Department.

On September 30, 2004, IOIA submitted the required Annual Report to the Director and the Governor's Office, which outlined their accomplishments for fiscal year 2004 and objectives for fiscal year 2005.

The Department oversees a vitally significant, multi-million dollar computer operation and relies heavily on information technology to provide services to other agencies and to perform its own functions. The increased use of information technology intensifies the need for independent reviews to ensure that all risks and security issues have been adequately addressed.

The Department should ensure that an effective process exists to identify and monitor information technology activities to ensure that integrity and security issues are adequately addressed.

Billing System

Control Objective - Management should ensure that a billing system exists which accurately charges users for computer services, provides for sufficient audit trails, and supplies users with sufficient information to determine the accuracy of the individual billings.

Tests Performed - We reviewed the Department's billing procedures and user agency bills. Additionally, we reviewed the process of issuing credits and the collection of outstanding balances.

Results - The Department is statutorily authorized to provide data processing services for State agencies. The Department, State agencies, and users of the CCF share the costs of those services. Funding for the CCF is provided through the Statistical Services Revolving Fund (SSRF) and the Communications Revolving Fund (CRF).

We reviewed the invoices from two agencies for the month of November 2004, noting no discrepancies.

The Department has two forms to process credit requests: the Credit Adjustment Form (CAF) and the Accounts Receivable Credit Memorandum (ARCM). The CAF is used to process credits due to hardware or software failures at the Data Center that cause a program to fail. The user agency is responsible for completing the CAF and submitting supporting detail. After approval, the credit is sent to Accounting for manual entry into the billing system to adjust the user agency's next invoice.

The second form, the ARCM, is used to process credits that are the result of errors on user agencies' billing invoices. The user agencies, or Department personnel, complete the credit memo. All credit memos must be submitted with supporting detail. The form and supporting detail are reviewed by the billing staff supervisor and then forwarded to Accounting for posting.

We reviewed the credit log for the months of July 2004 through December 2004 noting no duplicate credits and the credits appeared reasonable. In addition, we reviewed 25 credits for proper approval, supporting documentation, and correspondence to the credit log, noting no exceptions.

Each month the Department receives billing information from several different vendors either in hardcopy or electronic format. This information is then reformatted and loaded into the Management Of Network Income Expense Services (MONIES) system. MONIES is the billing, order management and inventory system that the Department uses to process, track and bill telecommunications services. We reviewed the reconciliation between the vendor files and MONIES for November and December 2004, noting no exceptions.

The Accounting Department is responsible for pursuing outstanding SSRF and CRF accounts receivable. The Department has written procedures for accounts receivable for the SSRF and CRF. The Accounts Receivable Posting System is used to track accounts receivable for both the SSRF and the CRF. According to the *Illinois Administrative Code (74 Ill Adm. Code Part 1000)*,

the Department is to send out catch-up billings in the subsequent fiscal year for accounts receivable of the prior fiscal year. Catch-up billings are to be sent monthly beginning in November of the subsequent fiscal year. We reviewed 25 catch-up billings for the month of December 2004, noting no exceptions.

If any agency persists in not paying a delinquent account, the Department's Director will prepare a letter to the Director of the delinquent agency requesting attention to the matter. The letter states failure to resolve the outstanding amounts could result in curtailment of future services. In addition, if a non-state entity continues to be delinquent, the account is referred to the Debt Collection Board and/or the Comptroller's Offset System. We noted that Director Letters have not been prepared for delinquent accounts during the last two fiscal years.

As of December 31, 2004 the accounts receivable (for State and non-state entities) for the SSRF and CRF were \$17.3 million and \$17.9 million, respectively.

Although reasonable administration controls existed, we recommend the Department:

- Enhance staff knowledge of the billing system and adequately document the process to provide the capability to understand and maintain the process.
- Continue with the assessment of current staffing and technical experience levels and develop a staffing plan to address any deficiencies.
- Ensure the interagency agreements provide an effective mechanism to delineate, monitor, and evaluate IT services provided to agencies.
- Evaluate the allocation of internal audit resources to information technology activities to ensure that integrity and security issues are adequately addressed.

This Page Intentionally Left Blank

CONTINUOUS SERVICE CONTROLS

Continuous service controls include the procedures necessary to ensure that information processing resources will be available even if the primary facility is not useable. These controls encompass the entire planning and testing process associated with comprehensive contingency planning activities.

As the Department places more reliance upon computer operations, the ability to continue critical processing is of prime importance.

The Department is mandated to provide computing services to approximately 96 State agencies that depend on a continuation of computing services in order to fulfill their duties, missions, and goals. A contingency plan is essential for an organization to minimize service disruptions and fully restore operations in the event of a disaster. Continuity service protection encompasses the areas of contingency planning, backup and recovery procedures, disaster recovery testing, off-site storage of backups, designation of an alternate processing facility, and availability of a backup power supply.

We reviewed continuous service controls and noted the following:

Disaster Continuity Plans

Control Objective - Management should maintain a written plan for restoring critical applications.

Tests Performed - We reviewed the following continuity plans:

- State of Illinois, DCMS, BCCS, ISD, Continuity Methodology-Effective January 3, 2005;
- State of Illinois, DCMS, BCCS, ISD, Recovery Activation Plan-Effective December 20, 2004;
- State of Illinois, DCMS, LAN, Recovery Activation Plan-Effective August 11, 2004; and
- State of Illinois, DCMS, Division of Telecommunications, NCC, Recovery Activation Plan-Effective April 11, 2002.

Results - Although comprehensive continuity plans exist to guide recovery activities, management has not approved the plans, nor has the Department performed testing to identify any deficiencies in the plans and determine if the plans would effectively guide recovery efforts in the event of a disaster.

Testing Recovery Procedures

Control Objective - Management should ensure that plans and procedures are adequately tested.

Tests Performed - We reviewed documentation associated with tests conducted during the audit period.

Results - Department procedures state “exercises involving CMS/BCCS/ISD computing facilities and services are conducted at least twice a year.” Additionally, exercises of other areas are to be conducted at least annually. The exercises may be in the form of desk checks, simulations,

component testing, or a comprehensive test. The Department has not conducted testing in the last two years.

The LAN Activation Plan states “frequent exercises (minimally on an annual basis) of the Plan should be scheduled and appropriately documented.” In August 2004, the Department conducted an exercise of its LAN at a recovery site. The goal of the exercise was to implement an infrastructure necessary to provide network connectivity at the recovery site for 100 workstations at six different locations. The Department setup workstations throughout the recovery site utilizing wireless technology and wired services. The Department did not determine the success of the exercise nor develop a detailed analysis of test results.

The Department did not perform a test of its Network Control Center (NCC) operations at the alternate facility.

Alternate Data Processing Facilities

Control Objective - Management should arrange for alternate data processing facilities.

Tests Performed - We reviewed contracts and agreements for alternate facilities and visited the local facilities.

Results – The Department has arranged for four satellite facilities in the Springfield area for providing disaster recovery services. In addition, the Department has a contract for disaster recovery services at out-of-state locations.

On January 29, 2004 the Department signed a contract with a disaster recovery service provider to provide recovery services and continuity consulting services. The contract is valid through January 2006.

The Department has entered into several interagency agreements to assist with recovery capabilities; however, we found no evidence that the agreements had been evaluated on an annual basis. Additionally, agreements with agencies that have been absorbed by other agencies (and are, therefore, under new management) have not been re-evaluated to ensure the agreements will be honored in the event of a disaster.

Statewide Critical Application Listing

Control Objective - Management, based on criticality and sensitivity of data and operations, should determine and prioritize applications and data.

Tests Performed - We reviewed the process used to prioritize applications.

Results - The Department maintains a Statewide Critical Application Listing based on information received from agencies. In the event a disaster would occur, only those applications listed in the Statewide Recovery File and that have been tested would be considered for recovery. Agency disaster recovery information is maintained in the Statewide Disaster Recovery File,

which is stored off-site at the regional vault.

In order for an agency to be placed on the Statewide Critical Application Listing, the agency must evaluate their applications and annually provide the Department with a summary of the application's importance to the State and society. During our audit, we noted the information from the agencies was requested in January 2005. However, as of May 1, 2005 the Statewide Critical Application Listing had not been updated.

Backup and Off-site Storage

Control Objective - Management should ensure that critical resources are backed up on a regular basis and stored off-site.

Tests Performed - We visited facilities and tested for availability of backup materials and data.

Results - The Department currently utilizes three off-site storage facilities: a local vault, a local data processing facility, and a regional vault.

Physical security and environmental controls appear acceptable at the off-site storage facilities. Procedures exist to routinely backup critical data.

Backup Power Source

Control Objective - Management should ensure an uninterruptable power supply (UPS) for critical applications is available.

Tests Performed - We reviewed backup power sources, maintenance agreements, and backup power tests.

Results - The electrical power for the CCF is from two different utility-supplied power grids. If one source fails, a system will transfer to the other power source. If both power sources fail, the building's power will be supplied from the CCF's UPS. In the short term, a battery bank will supply the needed electrical power. This period of time allows the diesel-powered turbines to be started. The turbine generators can supply electrical power until utility-supplied power is restored. The local alternate processing facility is also equipped with a UPS.

A service contract agreement, effective July 1, 2004 through June 30, 2005, has been established to provide routine preventive maintenance on the UPS components located at the CCF.

As outlined above, we identified several weaknesses which may have a significant impact on the State in the event of a disaster. Department management stated the development of an effective business continuity plan (which is more comprehensive and incorporates the recovery of computer systems) is one of its primary objectives in fiscal year 2006.

Since the Department is mandated to provide computing services, it is imperative continuity services be available to minimize service disruption and fully restore critical operations in the event of a disaster. The Department's responsibility for continuity services will increase as the IT

Rationalization project progresses. The State is placing great reliance on the Department's ability to provide data processing and network services in the event of a disaster. As such, comprehensive and thoroughly tested disaster contingency plans are an essential component of recovery efforts. In order to minimize risks associated with a loss of service, the Department should:

- Prioritize the development of an effective business continuity plan that incorporates the recovery of computer services.
- Ensure that adequate plans, facilities, and equipment are available to recover all critical applications.
- Perform annual comprehensive tests of the Department's disaster recovery plans.
- Ensure that documentation supporting the goals, objectives, and results of tests is developed and maintained.
- Annually evaluate the interagency agreements for the alternate sites, particularly agreements with agencies that have been absorbed.

COMPUTER OPERATIONS CONTROLS

The command center unit of computing services is the focal point of data processing for the CCF. The control and management of computer operations are vital to overall data processing effectiveness.

Computer operations management must be aware of all facets of the operating environment and be able to control it. Department management must ensure that processing meets specifications, thereby making the review of operations a primary concern. Therefore, Department management must require the logging of all actions initiated by computer operators and help desk employees, and all actions performed by computer software.

We reviewed computer operations controls and noted the following:

Activity Logs

Control Objective - Management should ensure that sufficient information is stored in operations logs to enable reconstruction, review and examination of activities.

Tests Performed - We reviewed Daily Shift Reports, Shift Change Checklists, Vital Sign Checklists, and the InfoMan Incident Reports.

Results - The CCF maintained several reports that record Command Center activities. The Daily Shift Report, Shift Change Checklist, Vital Sign Checklist, InfoMan Incident Report, and systems logs are utilized to record Command Center activities.

We reviewed the Shift Change Checklists, Daily Shift Reports, Vital Sign Checklists, and InfoMan Incident Reports for the time periods of December 2004 and January 2005, noting reviews of system status were conducted.

Staff Training

Control Objective - Management should ensure that staff is adequately trained on start-up procedures and other operations tasks.

Tests Performed - We reviewed operational procedures and conducted interviews with Department management.

Results - Management ensures operations staff is adequately trained on start-up procedures and other operational tasks by a variety of means. Designated daily training periods are assigned to each operator. During this period the following activities were conducted:

- Ongoing review of the Data Processing Guide (DP Guide);
- Use of computer-based training tools;
- Presentation of courses at the Operations Training Facility; and
- Hands-on training conducted by supervisory staff.

Supervisory staff is responsible for the tracking of individual participation in all forms of training. Operator training reports are generated on a bi-monthly basis and forwarded to the Command Center Manager.

Change Control

Control Objective - Management should ensure policies and procedures are in place for the authorization of changes.

Tests Performed - We reviewed the Department's Change Management Policy, change management procedures and tested changes for compliance with the procedures.

Results - The Department's Change Management Policy defines a change as "any alteration to the state, configuration of, or policy concerning any production multi-user software or hardware under the Department's management, where the impact could be felt beyond the staff making the alteration."

Changes are classified into one of five categories based on potential impact, visibility, and complexity. The categories are Emergency, Major, Significant, Minor, and Transparent.

For changes, which are categorized as Major, Significant and Minor, the change management procedures should resemble those of standard project management. All changes are required to obtain approval from the Requesting Manager, all affected Systems Managers, the Change Management Board and senior management.

As of November 2004, the Department implemented a new change management process to control all significant or major changes. The Change Management Data Base is the foundation for the new change management process. All changes which have the potential to impact any Departmental services or customers are subject to the new process.

The Department is in the development stage of an Enterprise Wide Change Management Solution, which is projected to replace the existing process in fiscal year 2006.

We reviewed a sample of change requests and found:

- Guidelines did not exist to ensure all required changes complied with the change management process;
- Significant changes were not included in the Change Management Data Base;
- Some provisions in the Change Management Policy are not consistent with other existing policies;
- Testing Procedures were not included in the Change Management Policy;
- Procedures outlined in the Change Management Policy were not routinely followed; and
- An acceptable level of segregation of duties did not always exist to control the implementation of changes.

Help Desk Activities

Control Objective - Management should ensure procedures exist to register, track, and address all customer queries.

Tests Performed - We reviewed customer queries for responsiveness and completeness.

Results - The mission of the Help Desk is to provide user support for all platforms and applications, and in cases of highly technical incidents, to notify the appropriate technical support personnel for the involved user area. The Help Desk logs and tracks incident calls to ensure adequate monitoring and resolution of the incident, and measures these results against established service levels to ensure incidents are being addressed and resolved within established timeframes. The Help Desk, through the logging procedure, also provides management with data to help identify and resolve developing trends.

The Daily Shift Report consists of all incident calls received at the Command Center. The Report contains the date and time of the call. The system involved in the incident is also identified, along with a narrative providing any necessary information regarding the incident and the InfoMan number assigned to the incident call. The narrative portion of the report is also utilized to document subsequent actions taken regarding the incident call and to supply any additional pertinent information. We reviewed the Daily Shift Reports for the months of December 2004 and January 2005, noting entries appeared to be adequately documented, and where appropriate, InfoMan numbers were assigned to the call.

Calls received at the Command Center are logged into InfoMan and have an escalation time built into the system that is arrived upon by the reporting party and the Command Center personnel. The escalation process is built around two levels involving response time to the query and the resolution timeframe that is established between the user and the technician. The response time for the query is defined as:

- Premium response: First escalation is after one hour, with subsequent escalations every 30 minutes thereafter. Thus, the call must be activated within one hour.
- High response: First escalation is after two hours, with subsequent escalations every 60 minutes thereafter.
- Medium response: First escalation is after four hours, with subsequent escalations every 2 hours thereafter.
- Low response: First escalation is after one standard business day, with subsequent escalations every 12 hours thereafter.
- Premium response, next day: First escalation is after one hour on the next standard business day, with subsequent escalations every 30 minutes thereafter.

The Help Desk has the ability to select a priority level for the incident call, and this selection can vary from level 1 to level 4. The following is a breakdown of the four severity levels:

- Severity Level 1: Critical Business Impact - This level indicates the inability of the customer to use the resource, resulting in a critical impact on operations. This level requires immediate action.
- Severity Level 2: Significant Business Impact - This level indicates that the resource is usable, but is severely restricted.
- Severity Level 3: Moderate Business Impact - This level indicates that the resource is usable with less significant features (not critical to operations) unavailable.
- Severity Level 4: Minimal Business Impact - This level indicates that the resource causes little impact on operations or that a reasonable circumvention to the problem or request has been implemented.

The incident calls are automatically escalated within InfoMan whenever either the response time is not met, and/or the resolution timeframe is not met.

We reviewed 30 InfoMan incident calls from the Daily Shift Reports of December 2004 and January 2005 for analysis against the established service levels set within the system, noting 17% of the calls (5 of 30) were escalated due to the support/response target goal not being met. Of the five incident calls escalated, one was escalated twice.

As part of the IT Rationalization project, the Department is moving toward an Enterprise-Wide Help Desk. Over the next fiscal year the Department will be providing the Enterprise-Wide Help Desk to select agencies. Additionally, the Department is in the process of implementing new software to log and track calls.

To improve Computer Operations controls, we recommend the Department:

- Expedite the development and implementation of the Enterprise-Wide Change Management Solution.
- Ensure the Change Management Policy and associated procedures are followed on all applicable changes.
- Review the current Change Management Policy and associated procedures to ensure they meet the needs of the Department.
- Ensure the appropriate and timely response to service incidents supports the business demands of State agency customers.
- Ensure appropriate policies and procedures for the Enterprise-Wide Help Desk are developed timely.

SECURITY CONTROLS

The presence of security controls reduces or prevents disruption of service, loss of assets, and unauthorized access to equipment. An effective security program is a prerequisite to effective computer security.

Security measures include controlling access to computer facilities, controlling visitors within the facility, and establishing appropriate security policies and procedures.

As computers become increasingly integrated into the delivery of State services, and contain critical and confidential information, security becomes increasingly essential. New initiatives introduce security concerns that must be continually, adequately, and globally addressed. In addition, since the Department functions as a computer service bureau used by approximately 96 State agencies, there is an inherent leadership role regarding technology and security issues. Therefore, we strongly believe that an effective security administration function is critical to the overall security and integrity of the State's computing environment.

We reviewed security controls and noted the following:

Security Policies

Control Objective - Management should have a written plan that clearly describes the department's security program, policies, and procedures.

Tests Performed - We reviewed policies and procedures and interviewed staff regarding security-related functions.

Results - The Department has issued several security policies relating to information technology:

- CMS Policy Manual (each section is dated);
 - CMS Information Technology Security Policy (dated April 26, 2002) included as Chapter 4, Section 3 of the CMS Policy Manual;
- Statewide Internet Security Policy (dated December 11, 2001);
- Information Security Policy - Local Area Network (LAN)/Office Automation (OA) (dated May 26, 1995);
- Statewide Information Security Policy BCCS/CCF Internal (dated February 4, 2003);
- Office Automation Coordinators Manual (dated February 2003); and
- CMS LAN Office Systems Procedures Guide (dated February 2003).

Security Administration

Control Objective - Management should coordinate a security management structure and clearly assign responsibilities.

Tests Performed - We reviewed the organizational chart and interviewed staff to obtain an understanding of the current security organizational structure.

Results - The Department is reviewing its organizational structure for security and plans to have a new structure implemented by July 2005.

The Department currently has a Security and Availability Manager who is responsible for both logical and physical security. At least three other staff members also are assigned security-related duties.

In addition to the security structure, the Department established a Security Task Force Committee which was responsible for updating the security policies and promoting security awareness. However, per management, the Security Task Force is no longer active as it was determined that topics addressed by the Security Task Force were being addressed in other business functions.

Personnel Policies

Control Objective - Management should have a written personnel policy that includes procedures relating to hiring, transferring and terminating employees.

Tests Performed - We reviewed personnel policies and practices for hiring, transferring, and terminating employees, including guidelines to update or remove access privileges.

Results - All new personnel are required to undergo a security screening investigation by the Department's Office of Investigative Services, and must sign the appropriate release forms to allow the security staff to obtain any necessary documentation. Our testing indicated not all required security screening investigations were conducted prior to the start of employment.

According to the CMS Policy Manual, "the Bureau is responsible for notifying the Office of Internal Personnel of an employee leaving the agency. Supervisors are responsible for collecting a separated employee's telephone credit card, door and desk keys, parking lot stickers, Data Center admittance cards, identification cards, vehicles and special equipment. The supervisor is also responsible for contacting the Data Processing Manager if the employee had terminal or operator access to data bases."

We found that guidelines did not exist to notify all appropriate security staff of personnel changes to update or eliminate physical and logical access rights.

Security Awareness

Control Objective - Management should ensure that staff are aware of their roles and responsibilities.

Tests Performed - We reviewed policies and procedures, assessed security awareness, reviewed practices to communicate policies to staff, and reviewed security training programs.

Results - The Department requires employees to review select policies and sign statements of understanding.

Our testing indicated not all required statements of understanding were signed at the start of employment. In addition, policies and procedures do not exist requiring statements of understanding be reviewed and re-signed on an annual basis.

There are no requirements for employees to routinely attend security-awareness training and limited training was conducted during the audit period.

Physical Security

Control Objective - Management should ensure that physical access to computer resources is restricted.

Tests Performed - We reviewed policies and procedures, assessed physical security, and tested compliance with procedures regarding the assignment of temporary badges.

Results – Controls existed to restrict physical access to computer resources.

The CCF was constructed in 1980, and designed to meet the State's data processing needs. The CCF was built with pre-cast concrete, has a steel structure, and a shell that is non-combustible. The CCF is monitored 24 hours a day, 7 days a week, by security guards, surveillance cameras, proximity badge readers, and alarms. The Command Center is protected by both a fire detection and suppression system and a water detection system. The Department's Information Security Policy states the area housing the Command Center of the CCF is intended to be under tight security at all times.

The Telecommunications Building is monitored 24 hours a day, 7 days a week, by security guards, surveillance cameras, proximity badge readers, and alarms.

Procedures exist for the issuance of badges and for granting visitor and guest access to the CCF and Telecommunications Building. Different types of temporary badges can be issued to visitors and guests, depending on their access needs. Visitors, or employees who forget their badge, are required to sign-in and register with security guards to gain access to the facility.

Physical security and environmental controls were acceptable at the off-site facilities.

Tape Management

Control Objective - Management should develop procedures relating to data storage to ensure the accuracy of inventory counts of physical movement and storage of media.

Tests Performed - We reviewed tape management procedures and practices, rotation of tapes to off-site storage locations, physical security of the off-site locations, and environmental conditions at the off-site locations.

Results - The Department has formal tape procedures in place to control the movement of

magnetic tapes to and from the CCF. In addition to agency tapes being rotated to the off-site storage location, CCF staff physically rotate operating system backups to the local and regional off-site storage locations. Agencies also have been provided with the capability to electronically transmit backup data to an alternate location.

Although security controls were addressed at the Department, to enhance security the Department should:

- Continue with the comprehensive review of its organizational structure for security, ensure security issues are effectively addressed, and meet implementation deadlines. Additionally, the Department should ensure the security organization reports to the highest level of management to promote independence and accountability.
- Review and update all information security policies on an annual basis to ensure policies reflect the current environment and Departmental practices and intentions. In addition, the Department should ensure all policies are dated and all employees and contractors have access to the current versions of policies.
- Formally promote security awareness and require training to keep users informed and aware of security issues, and periodically assess compliance with established policies and procedures.
- Ensure required security screening investigations are conducted prior to the start of employment.
- Require individuals to sign a statement of understanding regarding the Department's policies at the start of employment, and annually thereafter.
- Develop procedures to ensure that access authorization rights are periodically reviewed and updated to ensure access rights align with job requirements and are updated upon the termination of employment or contracts.

APPLICATION SYSTEMS DEVELOPMENT CONTROLS

Application systems development is a critical part of the data processing function. A structured systems development process helps to ensure system reliability, quality, predictability, and user satisfaction.

The acceptance of a structured systems development methodology ensures that system design meets the requirements of system users. A structured approach includes the use of standards for systems design, documentation, testing, and post-implementation review. It also ensures that all new and enhanced computer systems meet organizational requirements.

The Department is responsible for the development of computer systems (common systems) that are available for use by the user agencies as well as those systems used by the Department.

We reviewed application systems development controls and noted the following:

Systems Development Methodology

Control Objective - Management should have a documented systems development methodology that details the procedures that are to be followed when applications are being designed and developed, as well as subsequently modified.

Tests Performed - We reviewed the Application System Development Methodology (Methodology) and the Standards and Documentation Requirements (Standards). We also examined an enhancement project to assess compliance with the Methodology.

Results - The Methodology (revised July 2003) is the guide, developed in-house, for new system developments, modifications to existing systems, user manuals, the purchase of third party software, user training, testing, and post-implementation reviews.

The Methodology outlines four system development phases:

- Phase I - Problem Definition and Systems Planning;
- Phase II – Design;
- Phase III - Development and Implementation; and
- Phase IV - Post-Implementation Review.

Phase I (problem definition and systems planning) is the initial phase and examines the feasibility and benefit of a project. Requirements for a cost/benefit analysis of new applications or major system enhancements are included in the Methodology.

Phase II (design) is intended to document, propose, and obtain approval of the design. A security statement, database layouts, sample input documents, sample output, system narratives, diagrams, backup requirements, and conversion plans are developed. The Methodology states a user committee will be formed to assist with system analysis and design.

In **Phase III** (development and implementation), the project will be developed based on the system specifications documented in Phase II. The Methodology states all aspects of the system must be thoroughly tested and reviewed prior to implementation.

According to the Methodology, **Phase IV** (post-implementation review), if required, will be conducted within 30 to 180 days after the system is in production. The purpose of a post-implementation review is to review the production system and evaluate its actual benefits, performance, and cost.

The service request form is used to initiate system development projects. The Service Request Registration System (SRRS) registers projects and records the status of the project. There are four categories of system development projects: a new development, enhancement, maintenance, or ad hoc request. A new development is the development of new applications or systems when no system is in production, or a rewrite of an entire existing system. An enhancement is a routine change or the addition of a new feature to an existing system. Maintenance requests are emergency changes or required changes to an existing system which do not change system functionality. An ad hoc request is a one-time request for reports or programs.

We selected an enhancement project for review and found general compliance with the Methodology.

Development Process Oversight

Control Objective - Management should establish roles and responsibilities for planning, developing, reviewing, implementing and auditing the development process.

Tests Performed - We reviewed the Application System Development Methodology (Methodology) and the Standards and Documentation Requirements (Standards).

Results - The Methodology addresses the roles and responsibilities of the development group, technical support, Quality Assurance, and Internal Audit. The development group is responsible for mainframe and LAN systems design, coding, program walk-through, testing, documentation, implementation, database administration and ongoing production application support. Technical support provides resources for database technical reviews and security software. Quality Assurance monitors and verifies project teams adhere to the Methodology. Users are to participate in each phase of systems development, assist with defining business rules and designing the system, and executing systems tests. Internal Audit determines its own level of involvement in projects.

Project Management

Control Objective - Management should have management tools for the tracking of projects.

Tests Performed – We interviewed management and reviewed pertinent documents to determine what project management tools were utilized. Additionally, we reviewed service request forms to determine if they were properly completed, approved, and categorized.

Results - The Department utilizes several tools to aid in tracking of system projects, assignments and scheduling of time.

One tool is the SRRS which is used to track projects involving application system enhancement, development, or change. A service request form is used to record the request and input information into the SRRS.

We reviewed 40 service request forms, and determined all were properly completed.

Test Plans

Control Objective - Management should require that a test plan be created for developments, implementations, and modifications.

Tests Performed - We reviewed test plans to determine if they were completed in compliance with the Methodology.

Results - The Department requires the project teams to work closely with user groups when developing a new application. The Methodology states user involvement is vital for system development to be successful. Users are to participate in each phase of system development and assist with defining the business rules and designing the system. Users are responsible for developing and executing system tests according to the business rules.

The Methodology requires the Project Manager to request users to develop unit, system, and integration test plans.

During our review, we reviewed a project and determined test plans were required. We reviewed the test plans, noting no exceptions.

Training Plans

Control Objective - Management should require that training plans be created for projects.

Tests Performed - We reviewed the Application System Development Methodology (Methodology) and the Standards and Documentation Requirements (Standards).

Results – According to the Methodology, a training schedule is to be developed and training sessions are to be conducted during Phase III (development and implementation). During our review, the Department did not have a project, which required training plans.

Quality Assurance

Control Objective - Management should ensure that the responsibilities of the Quality Assurance personnel include a review of general adherence to the systems development methodology and objectives of the project.

Tests Performed - We reviewed documentation to determine if Quality Assurance was performing its duties in accordance with applicable policies and procedures.

Results - The Methodology includes the Quality Assurance Review Procedural Manual which addresses the quality assurance function. It is Quality Assurance's responsibility to monitor and verify that project teams adhere to the Methodology during each phase of a systems development project.

Our review of projects indicated that Quality Assurance is performing its duties in accordance with applicable policies and procedures.

Program Movement

Control Objective - Management should ensure that access to production libraries is limited and movement of programs is controlled.

Tests Performed - We reviewed a sample of move requests to determine if moves to production were completed in compliance with the Program Library Procedures.

Results – The Program Library Procedures state “Library Control is to maintain program library security and perform special assignments, when required.” Library Control staff control all movement of programs in a production library. The procedures are to ensure that new programs and modifications to existing programs are thoroughly documented and signed off by a manager before production moves are performed. The process of requesting a change be moved to production is automated.

We reviewed 20 move requests, noting all were completed in compliance with the Program Library Procedures.

TELECOMMUNICATION CONTROLS

Telecommunication systems control the transmission of messages between users and the computer. Through the telecommunication network, users at remote sites can access computer programs at the computer facility. The majority of devices interface with the computer facility by a telecommunication device. Control over the telecommunication network is necessary to ensure that only authorized users have access to the computer facility.

Telecommunication network controls should encompass the network's operating performance and security.

The Department has a statutory obligation to “provide for and control the procurement, retention, installation, and maintenance of telecommunications equipment or services used by State agencies in the interest of efficiency and economy.” (20 ILCS 405/405-270)

The Department operates in a manner similar to a telephone company and utilizes a combination of State and vendor services. The Department provides local telephone service, telecommunications equipment, software, installation, maintenance, and networking services to State agencies. The statewide telecommunications network is comprised of thousands of miles of voice and data lines serving the State.

The Management of Network Income Expense Services (MONIES) system is the billing, order management, and inventory system the Department uses to process, track, and bill all telecommunications products and services.

During the fiscal year, the Department added a significant network with the absorption of the Illinois Century Network (ICN). Additionally, the inventory, change and problem management, and billing functionality of the MONIES system were being migrated into two new systems.

The Department also implemented the Customer Solution Center (CSC) and Customer Management Center (CMC). The CSC was responsible for maintenance and provisioning of voice, video, data, and wireless systems and services. The CMC is responsible for all trouble resolution, network surveillance and ongoing technical support.

We reviewed telecommunication controls and noted the following:

Network Documentation

Control Objective - Management should ensure that the telecommunications networks are adequately documented.

Tests Performed - We reviewed network diagrams representing the Department's telecommunications environment. Additionally, we reviewed the telecommunications Intranet site and memorandums distributed to user agency Telecommunications Coordinators.

Results - The Department maintains communications network diagrams for the CCF, including

Transmission Control Protocol/Internet Protocol (TCP/IP) and Systems Network Architecture (SNA) networks. The Department also maintains Local and Wide Area Network (LAN/WAN) diagrams.

In addition, the Department maintains diagrams documenting the host-to-mainframe connections, network control program connections, State agency users, and the SNA network interconnects to both State and private sector data centers.

The Department has established an Intranet site to communicate training and other information to user agency Telecommunications Coordinators, audio-conferencing users, and video-conferencing users. Additionally, memorandums are distributed periodically to user agency Telecommunications Coordinators. We reviewed telecommunications-related memos and notices distributed during fiscal year 2005, and it appears memos and notices were disseminated on a regular basis.

The Department is migrating their telecommunications services off of vendor-supplied networks, and on to the Illinois Century Network.

Change Procedures

Control Objective - Management should establish policies and procedures over telecommunication changes.

Tests Performed - We reviewed the Department's telecommunications change control procedures, and examined the change control process. Additionally, we tested various telecommunications change request forms for proper completion and timely resolution.

Results - The Department has established procedures controlling telecommunications changes. The Guide to Telecommunications Services and Procedures (Guide) outlines the Department's telecommunications process, including changes and user agency responsibilities. The Guide was last revised in November 2003 and appears comprehensive.

The primary types of telecommunications change requests in the Department's environment are data requests and voice requests. Every change request requires a completed change request form.

Telecommunications Data/Intercity Service Request (TDR) forms are completed by user agencies, and are used to submit data requests. We reviewed the instructions for completing the TDR form documented in the Guide, noting that the instructions are accurate. We examined five TDR forms and found some minor documentation and timeliness issues.

Telecommunications Service Request (TSR) forms are completed by user agencies, and are used to submit voice requests. We examined five TSR forms and determined all five were properly completed; however one of the five was not completed on time.

Problem Handling

Control Objective - Management should establish policies and procedures over telecommunication problems.

Tests Performed - We reviewed the Department's telecommunications problem management procedures. Additionally, we tested various telecommunications problems for proper handling and timely resolution.

Results - The Department has established procedures for the handling of telecommunications problems. Significant problems are logged on a Major Event Log. An enterprise-wide system for problem management is being developed.

The NCC Problem Management Methods and Procedures Manual outlines the handling of data problems and maintenance. The Manual was last updated in February 2003; however, significant changes, including the absorbing of the Illinois Century Network (ICN), and the pending migration to the enterprise-wide system for problem management has prompted a rewrite of the Manual. We reviewed five trouble tickets, and determined all five were properly completed and resolved timely.

The Voice Repair Manual outlines the handling of voice problems, and appears to be adequately comprehensive. We reviewed five trouble tickets, and determined all five were properly completed and resolved timely.

The Department has procedures in place to identify and resolve telecommunications problems.

Security Options

Control Objective - Management should ensure that available security options are utilized.

Tests Performed - We interviewed management and reviewed pertinent documentation to determine the security options used by the Department.

Results - Management stated the Department utilized the following telecommunications security mechanisms:

- Encryption converts data to a form that appears to bear no relation to the original data;
- Digital Signatures guarantee the authenticity of a set of input data by using encryption to achieve a unique electronic signature for each user. Digital signatures are associated with the Department's Public Key Infrastructure system;
- Access Control ensures that a person or system has the permission to use a particular computer resource;
- Authentication Exchange is a dialogue between a claimant and a verifier, to assure the verifier of the claimant's identity;
- Routing Control enables messages to flow through different routes over a network, making the complete message difficult to trace and identify; and
- Notarization is the use of a third party that is trusted by the communication entities. The notary can arbitrate between the communicating entities.

We found the Department had implemented reasonable security options.

Diagnostic Equipment

Control Objective - Management should ensure that available diagnostic equipment is utilized.

Tests Performed - We interviewed management to determine the diagnostic equipment used by the Department. Additionally, we reviewed the control over sensitive diagnostic equipment.

Results - Management stated the Department uses the following types of diagnostic equipment to aid in identifying telecommunications problems:

- Sniffers – Sniffers are portable computers that plug into a port, data circuit, or telephone line and can view data being transmitted across a network, including sensitive information such as passwords;
- Telecommunications Protocols – Positive acknowledgement of data receipt is built into most communications protocols;
- Error Logging – The Network Problem Determination Aid and the Network Performance Monitor log errors on the host system at the CCF; and
- Alarm Conditions – The majority of lines terminating at the State node sites are monitored for alarm conditions.

We determined the Department utilized diagnostic equipment.

Internet

The Department utilizes the Illinois Century Network (ICN) and a vendor as its primary and secondary Internet Service Providers (ISP). The Department maintains and supports the firewall hardware and software that connects the CCF and the local computing facility to the internal frame relay network that provides the connection to the Internet. The Department also provides ISP based services for Illinois State agencies.

Control Objective - Management should ensure the integrity and security of Internet connections.

Tests Performed - We reviewed policies, procedures, and network topology maps related to the design and security of the Department's Internet environment. Additionally, we reviewed firewall and router implementation and configuration, as well as software in place to provide protection against viruses. We also reviewed the process in place for monitoring security violations, as well as for the continual assessment of Internet security.

Results - The Statewide Internet Security Policy requires State agencies to acquire Internet access from the Department and all exceptions must be approved by the Department's Director. Additionally, connections to the State's Internet or the protected information environment will not be permitted until the agency's configuration has been reviewed and approved by the Department. The Department should ensure that an agency's configurations have been reviewed and approved before allowing the agency to access the Internet, either directly or through the Department's firewall.

The Statewide Internet Security Policy states, for any changes to the agency's Internet configuration "the agency must notify and obtain approval from CMS." With the continual advances in technology and staffing changes at agencies, configurations need to be constantly reviewed to ensure the integrity of the Department's environment. Additionally, according to the Statewide Internet Security Policy, "It is each agency's responsibility to determine employee Internet access and block sites they do not wish their employees to visit."

The Department is responsible for entering rules into the firewalls and monitoring security violations. There are approximately ten staff members who have some responsibility regarding Internet security and control (firewall and router configuration).

Virus protection is not employed on the firewalls; however, anti-virus software actively protects both servers and desktops. Additionally, incoming and outgoing emails are scanned for viruses.

We reviewed the Internet topology maps and determined that the routers and firewalls are placed in suitable logical positions, with an emphasis on redundancy and service continuity. The routers and firewalls are physically located in secure locations.

As part of the IT Rationalization project the Department is reviewing its organizational structure, including security. As a part of the reorganization, the Department is implementing a Risk Management section. Management stated one of the functionalities of the Risk Management section would be the oversight of Internet security.

Internet Privacy Policy

Control Objective - Management should deploy a privacy policy on the Department's web site informing users of tracking technologies that are utilized and contain provisions that disclose practices regarding Notice, Choice, Access and Security.

Tests Performed - We reviewed the Department's web site for the existence of an Internet privacy policy. Additionally, we reviewed the privacy policy to determine if it adequately addressed the issues of Notice, Choice, Access, and Security.

Results - The Department's web site contains a privacy policy (policy), dated January 2003. The policy informs users that personal information is not collected unless voluntarily provided by the user via email, online forms, survey response, or registration for a specific service. Users who choose not to participate in the above listed activities will still have the ability to utilize all other features of the web site. The policy then includes a provision notifying users of their right to review any personal information that has been collected by the Department and recommend changes to any inaccuracies.

The policy also states "the Department of Central Management Services, as developer and manager of this web site, has taken several steps to safeguard the integrity of its communications and computing infrastructure, including but not limited to authentication, monitoring, auditing, and encryption."

We noted the policy contained provisions that disclosed practices regarding Notice, Choice, Access, and Security.

Wireless

Control Objective - Management should ensure the integrity and security of wireless networks.

Tests Performed - We reviewed the control and security over wireless networks. Additionally, we reviewed wireless network coverage and users.

Results - The Department and the Illinois State Police have coordinated efforts to provide the Illinois Wireless Information Network (IWIN), a wireless wide area data network using cellular digital packet data (CDPD), and recently implemented code division multiple access (CDMA) technologies. The Department is currently in the process of phasing out CDPD and intends to have all users converted to CDMA by July 2006. The Department administers the IWIN network, and the Illinois State Police provides the connection to the Law Enforcement Agencies Data System (LEADS), National Crime Information Center, Secretary of State, National Law Enforcement Telecommunications System, and Criminal History Record Information (CHRI) that the network utilizes to provide information to IWIN users.

IWIN coverage currently exists in 101 of 102 counties in Illinois. There are almost 9,000 unique users of the IWIN network from approximately 12 agencies, 271 municipalities, 12 colleges and universities, 3 federal agencies, and 2 railway police departments. The Department's users account for approximately 5 of the unique users utilizing the IWIN network.

We found that reasonable controls existed.

Local Area Network (LAN) Security

Control Objective - Management should ensure the integrity and security of LANs.

Tests Performed - We reviewed or confirmed the physical and logical security over the Department's LANs. Additionally, we reviewed policies and procedures related to LAN security.

Results - The Department maintains and supports LANs for the Department as well as the Civil Service Commission, Department of Human Rights, Department of Labor, Human Rights Commission, Illinois Educational Labor Relations Board, Illinois Rural Bond Bank (part of the Illinois Finance Authority), Judicial Inquiry Board, Office of Executive Inspector General, Office of the Governor, Office of the Lieutenant Governor, Prisoner Review Board, and the State Police Merit Board. In addition, the Department provides LAN connections for email purposes to 7 agencies. We also determined the Department has policies relating to LAN security; however, in some instances the policies are inaccurate and outdated.

The Department's LAN servers were located in the CCF and NCC. As such, they were housed in physically secured and environmentally controlled settings. Based on our review and confirmation of the implementation of LAN security requirements, it appears that LAN settings were reasonable and complied with Department requirements.

Although reasonable telecommunications controls existed, we recommend the Department:

- Implement controls to ensure the protected environment is adequately safeguarded from unauthorized access from sources external to State agencies, especially as the Department is moving forward with incorporating new Internet-based technology.
- Formally review the telecommunications environment and ensure that an appropriate network security structure is established to ensure that information assets and resources are adequately protected from unauthorized or accidental disclosure, modification, or destruction.
- Ensure compliance with provisions of the Statewide Internet Security Policy.
- Continue to review IWIN and ensure that an appropriate wireless information network security structure is established to ensure that information assets and resources are adequately protected from unauthorized or accidental disclosure, modification, or destruction.
- Ensure all policies and procedures are accurate and up-to-date. Specifically, we recommend the Department thoroughly review, update, and, where appropriate, consolidate telecommunications procedures.
- Ensure procedures are followed and problems are resolved on a timely basis.

This Page Intentionally Left Blank

SYSTEMS SOFTWARE CONTROLS

Systems software consists of computer programs and related routines that control computer processing. The operating system is the prime component of system software; it controls the execution of user application programs.

Each system software product can be tailored to meet user needs. System tailoring is accomplished by setting optional system parameters and, therefore, has an impact on system performance and security.

We reviewed systems software controls and noted the following:

Zero Downtime Operating System (z/OS)

Control Objective - Management should ensure that operating systems are configured and controlled to promote security and integrity.

Tests Performed - We reviewed operating system parameters, security profiles and access to sensitive libraries, and staffing allocations. We performed auditor observations, conducted interviews, and performed testing including the use of an online product that provides detailed information on the hardware and software environment of the system and provides information about security parameters and control mechanisms.

Results - z/OS is the primary mainframe operating system used at the CCF. It is a complex operating system used on mainframe computers and functions as the system software that controls the initiation and processing of all work within the computer. The continuing integrity of z/OS is critical to maintain confidence in the accuracy and security of programs and data under its control.

Our general objective was to review the z/OS operating system to assess the level of security and the integrity of controls in place within the operating system environment. No significant weaknesses were identified in our review. However, we recommend the Department continue to assess security over its systems, datasets, and libraries.

Virtual Machine (VM)

Control Objective - Management should ensure that operating systems are configured and controlled to promote security and integrity.

Tests Performed - Our review of VM included assessing controls over the VM directory, security parameters, performance and monitoring tools, and procedures for authorizing and adding new users.

Results - The VM operating system is the secondary mainframe operating system used at the CCF. VM creates a virtual environment for each system user. As far as users are concerned, they are in total control of the computer, a virtual storage device, a virtual printer, and possibly such devices as telecommunication lines. The illusion is so complete that other operating systems can be run on a

virtual machine under the control of VM.

VM differs from the z/OS system in the security available to users, the way users are defined, and the types of applications available on the system. VM is similar to z/OS in that VM controls the initiation and processing of work in the computer. The integrity of VM is critical to maintaining confidence in the accuracy and security of programs and data under its control.

Although security over the VM operating system was reasonably well instituted, the Department should continue to discourage user agencies from permitting multiple users to write to a disk simultaneously, and periodically review IDs that can bypass password change requirements.

DataBase 2 (DB2)

Control Objective - Management should ensure that operating systems are configured and controlled to promote security and integrity.

Tests Performed - Our review of DB2 included a review of any significant modifications to the DB2 environment, including: the identification of established subsystems; identification of Department and user agencies' roles and responsibilities; assessing established security parameters; review of access to sensitive administrative IDs and other resources; and a review of established backup procedures and performance monitoring.

Results - DB2 is a relational database management system that the Department makes available to user agencies. No significant weaknesses were identified in our review of DB2. However, we recommend the Department ensure access to DB2 resources is restricted to those who require access based on job duties.

Customer Information Control System (CICS)

Control Objective - Management should ensure that operating systems are configured and controlled to promote security and integrity.

Tests Performed - Our review of CICS included review of any significant modifications to the CICS environment; assessing security parameters to determine if security was adequate and implemented at the transaction level; a review of access to sensitive transactions and other CICS-related resources; and identification of established CICS levels of support for user agencies.

Results - CICS is a program product that enables transactions entered into remote terminals to be processed concurrently by user-written application programs. The Department supports CICS and makes it available to user agencies. No significant weaknesses were identified in our review of CICS. However, we recommend the Department continue to assess and strengthen security controls.

Security Software

Control Objective - Management should ensure that an appropriate security software structure is

established to ensure that information assets and resources are adequately protected from unauthorized or accidental disclosure, modification, or destruction.

Tests Performed - Our review of security software included reviewing security parameters and features; security reports; policies pertaining to protection of data and resources, restriction of access to production data, and review and timely revocation of access; procedures to maintain a current and accurate listing of agency users; procedures to log, review, and monitor security violations; administrative authority, and access to sensitive resources; and staffing allocations.

Results - The Department uses security software to control and monitor access to data maintained on its mainframe computers and other resources. The security software operates as an extension of, and an enhancement to operating systems. It provides a mechanism for controlling access and for monitoring secured computer resources.

The security software protects by exception; that is, the user individually defines each dataset to be protected. It provides security and integrity capabilities that allow authorized users access to a defined set of protected resources, deny access to all other protected resources, and permit regular access to unprotected resources. The product limits users to the pre-defined datasets for which they have access authorization. In addition, the product maintains a log of all access attempts, which is used to monitor unauthorized access attempts and identify areas where security may need to be strengthened.

The security software protects access and enforces user accountability over data and system resources by positively verifying the user's authority to utilize that data or system resource and by logging the user's actions. Under the current environment, user agencies are responsible for specifying which datasets are to be protected and for properly using the available security resources.

Although reasonable systems software controls existed, we recommend the Department:

- Ensure all security profiles clearly identify the person or device assigned to IDs. As individual accountability is a primary security objective, the Department should, wherever possible, avoid the use of generically assigned IDs, unassigned IDs, and shared IDs. While there are cases where the use of such IDs is necessary, it should generally be prohibited unless absolutely necessary.

This Page Intentionally Left Blank

APPLICATION CONTROLS

Application controls are the methods, policies, and procedures adopted by an organization to ensure that all transactions are entered, processed, and reported correctly. Application controls ensure that data being entered, processed, and stored are complete and accurate. They ensure that the output from the computer application is timely and accurate.

Application controls can be grouped into three areas: input; processing; and output. Input controls ensure that the data entered into the system are authorized and accurate. These controls include both manual and computerized techniques. Processing controls are those that are coded into the software program. Manual procedures often supplement the programmed controls to verify that all processing has taken place as intended. Output controls govern the printing and distribution of reports.

The Department has developed several applications for use by State agencies. As part of the Third Party Review we reviewed four of the applications used by multiple State agencies.

The applications reviewed were:

- Accounting Information System;
- Central Payroll System;
- Central Inventory System; and
- Central Time and Attendance System.

This Page Intentionally Left Blank

ACCOUNTING INFORMATION SYSTEM

The Accounting Information System (AIS) is an online, menu-driven, mainframe application that provides an automated expenditure control and invoice/voucher processing system. AIS, in processing invoices, allocates invoice amounts into sub accounts; groups invoices, according to the Comptroller's Statewide Accounting Management System (SAMS) procedures, for the preparation of vouchers; and allows users to track cost centers.

AIS was implemented in March 1995. AIS is currently utilized by 50 entities (see page 67 for the list of user agencies).

Control Objective - Management should ensure that the application has policies, procedures and methods to ensure that all transactions are entered, processed and reported correctly. Management should ensure that application systems are configured and controlled to promote security, integrity, and availability.

Tests Performed - Our review of AIS included reviewing input controls, logical access and security controls, security of output documents, retention practices, backup and recovery procedures, change management procedures, and modifications to AIS during the fiscal year. In addition, we performed data integrity testing on two agencies' AIS data.

Results – Data entered into the system is the responsibility of user agencies. AIS has numerous edit checks built into the system to notify the users of any exceptions. Errors must be corrected before the transaction is accepted. AIS provides various online and batch reports to assist in the balance of transactions.

Access to AIS is controlled through security software, in addition to AIS' internal security. Users must have a properly authorized user ID and password to gain access to the operating environment. Once access to the operating environment has been allowed, users must have a separate application user ID and password to gain access to AIS. Assignment and authorization of access rights is the responsibility of each agency's security administrator.

There have been no major changes to AIS in the past year.

AIS is automatically backed up daily, weekly, and monthly. The daily and weekly backups are maintained at the CCF, with the monthly backups rotated to the off-site location.

During our testing of AIS data, we did not identify any significant weaknesses. In addition, no significant weaknesses were identified in our overall review of AIS.

To ensure that controls are fully implemented and functional at the agency level, staff, internal auditors, and external auditors of agencies using AIS should:

- Verify that only accurate and authorized data are entered into AIS. It is the agency's responsibility to ensure that only properly authorized transactions are entered into the system.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the user profiles and defined user groups with access to AIS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up AIS reports, and inform appropriate AIS personnel of changes timely.

Department records listed the following entities as users of the Accounting Information System.

1. Board of Higher Education
2. Capital Development Board
3. Department of Agriculture
4. Department of Central Management Services
5. Department of Corrections
6. Department of Financial and Professional Regulation*
7. Department of Human Rights
8. Department of Labor
9. Department of Military Affairs
10. Department of Natural Resources
11. Department of Public Health
12. Department of Revenue
13. Department of Veterans' Affairs
14. Department on Aging
15. Emergency Management Agency
16. Environmental Protection Agency
17. General Assembly Retirement System
18. Guardianship and Advocacy Commission
19. Historic Preservation Agency
20. Human Rights Commission
21. Illinois Arts Council
22. Illinois Community College Board
23. Illinois Commerce Commission
24. Illinois Criminal Justice Information Authority
25. Illinois Deaf and Hard of Hearing Commission
26. Illinois Educational Labor Relations Board
27. Illinois Law Enforcement Training and Standards Board
28. Illinois Planning Council on Developmental Disabilities
29. Illinois Student Assistance Commission
30. Illinois Violence Prevention Authority
31. Illinois Workers' Compensation Commission^
32. Judges Retirement System
33. Judicial Inquiry Board
34. Office of the Attorney General
35. Office of the Auditor General
36. Office of the Governor
37. Office of the Inspector General
38. Office of the Lieutenant Governor
39. Office of Management and Budget
40. Office of the State Appellate Defender
41. Office of the State Fire Marshal
42. Prisoner Review Board
43. Procurement Policy Board
44. Property Tax Appeal Board
45. State and Local Labor Relations Board
46. State Board of Elections
47. State Employees' Retirement System
48. State Police Merit Board
49. State's Attorneys Appellate Prosecutor
50. Supreme Court of Illinois

* The Department of Financial Institutions, the Department of Insurance, the Department of Professional Regulation, and the Office of Banks and Real Estate were consolidated on July 1, 2004.

^ Illinois Industrial Commission renamed on January 1, 2005

This Page Intentionally Left Blank

CENTRAL PAYROLL SYSTEM

The Central Payroll System (CPS) is an online and batch system that standardizes payroll procedures and processing for State agencies. The CPS enables State agencies to maintain automated employee pay records and provides them with payroll documents and a computer file that are submitted to the Office of the Illinois Comptroller for the production of the agencies' payroll warrants.

CPS was implemented in July 1972. CPS is currently utilized by 74 entities (see page 71 for the list of user agencies).

Control Objective - Management should ensure that the application has policies, procedures and methods to ensure that all transactions are entered, processed and reported correctly. Management should ensure that application systems are configured and controlled to promote security, integrity, and availability.

Tests Performed - Our review of CPS included reviewing input controls, logical access and security controls, security of output documents, retention practices, backup and recovery procedures, change management procedures, and modifications to CPS during the fiscal year. In addition, we performed data integrity testing on two agencies' CPS data.

Results – CPS transactions are entered online in a real-time environment, with the ability to batch transactions for processing at a later date. Most CPS user agencies enter their data online; however, Department personnel perform data entry for three agencies.

Data entered into the system is the responsibility of the user agency. The CPS has online edit checks to help prevent a user from entering a transaction with invalid data. If an error occurs during data entry, users are not allowed to continue until the error has been corrected.

Access to CPS is controlled through security software, in addition to CPS' internal security. Users must have a properly authorized user ID and password to gain access to the operating environment. Assignment and authorization of access rights is the responsibility of agency security administrators. Once access to the operating environment has been allowed, users must have a separate application user ID and password to gain access to CPS.

There have been no major changes to CPS in the past year.

CPS is automatically backed up daily and weekly. The daily backups are stored in the CCF and weekly backups are rotated to an off-site storage location.

During our testing of CPS data, we did not identify any significant weaknesses. In addition, no significant weaknesses were identified in our overall review of CPS.

To ensure that controls are fully implemented and functional at the agency level, staff, internal auditors, and external auditors of agencies using CPS should:

- Verify that only accurate and authorized data are entered into CPS. It is the agency's responsibility to ensure that only properly authorized transactions are entered into the system.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review security software profiles and defined user groups with access to CPS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up payroll reports, and inform appropriate CPS personnel of changes timely.
- Retain hardcopy payroll vouchers for at least the 3 most current pay periods, as specified by the CPS User Manual.
- Perform their own CPS data entry (applicable only to agencies that depend on the Department to perform their data entry).

Department records listed the following entities as users of the Central Payroll System.

- | | |
|---|--|
| 1. Board of Higher Education | 38. Illinois State Board of Investment * |
| 2. Capital Development Board | 39. Illinois State Police |
| 3. Civil Service Commission | 40. Illinois Student Assistance Commission |
| 4. Commission on Government Forecasting and Accountability | 41. Illinois Violence Prevention |
| 5. Comprehensive Health Insurance Plan | 42. Illinois Workers' Compensation Commission^ |
| 6. Court of Claims | 43. Joint Committee on Administrative Rules |
| 7. Department of Agriculture | 44. Judges' Retirement System |
| 8. Department of Central Management Services | 45. Judicial Inquiry Board |
| 9. Department of Children and Family Services | 46. Legislative Audit Commission |
| 10. Department of Commerce and Economic Opportunity | 47. Legislative Information System |
| 11. Department of Corrections | 48. Legislative Inspector General |
| 12. Department of Financial and Professional Regulation** | 49. Legislative Printing Unit |
| 13. Department of Human Rights | 50. Legislative Reference Bureau |
| 14. Department of Labor | 51. Legislative Research Unit |
| 15. Department of Military Affairs | 52. Medical District Commission * |
| 16. Department of Natural Resources | 53. Office of the Architect of the Capitol |
| 17. Department of Public Health | 54. Office of the Attorney General |
| 18. Department of Revenue | 55. Office of the Auditor General |
| 19. Department of Veterans' Affairs | 56. Office of the Governor |
| 20. Department on Aging | 57. Office of the Inspector General |
| 21. East St. Louis Financial Advisory Authority * | 58. Office of the Lieutenant Governor |
| 22. Emergency Management Agency | 59. Office of Management and Budget |
| 23. Environmental Protection Agency | 60. Office of the Secretary of State |
| 24. Executive Ethics Commission | 61. Office of the State Appellate Defender |
| 25. Guardianship and Advocacy Commission | 62. Office of the State Fire Marshal |
| 26. Historic Preservation Agency | 63. Office of the Treasurer |
| 27. House of Representatives | 64. Prisoner Review Board |
| 28. Human Rights Commission | 65. Procurement Policy Board |
| 29. Illinois Arts Council | 66. Property Tax Appeal Board |
| 30. Illinois Commerce Commission | 67. State and Local Labor Relations Board |
| 31. Illinois Community College Board | 68. State Board of Education |
| 32. Illinois Criminal Justice Information Authority | 69. State Board of Elections |
| 33. Illinois Deaf and Hard of Hearing Commission | 70. State Employees' Retirement System |
| 34. Illinois Educational Labor Relations Board | 71. State Police Merit Board |
| 35. Illinois Law Enforcement Training and Standards Board | 72. State Universities Civil Service System |
| 36. Illinois Math and Science Academy | 73. State's Attorneys Appellate Prosecutor |
| 37. Illinois Planning Council on Developmental Disabilities | 74. Teachers' Retirement System of the State of Illinois |

* Agency payroll information is entered into the system by CPS staff.

** The Department of Financial Institutions, the Department of Insurance, the Department of Professional Regulation, and the Office of Banks and Real Estate were consolidated on July 1, 2004.

^ Illinois Industrial Commission renamed January 1, 2005.

This Page Intentionally Left Blank

CENTRAL INVENTORY SYSTEM

The Central Inventory System (CIS) is an online and batch system that allows agencies to maintain records of inventory to comply with the Department's Property Control Division's rules of reporting and processing. Transactions (additions of new inventory items, deletions of inventory items being surplus, and updates of existing inventory items) are primarily entered into the CIS online real-time, meaning users' inventory data is updated immediately to reflect the transactions entered.

CIS was implemented in 1998. CIS is currently utilized by 27 entities (see page 75 for the list of user agencies).

Control Objective - Management should ensure that the application has policies, procedures and methods to ensure that all transactions are entered, processed and reported correctly. Management should ensure that application systems are configured and controlled to promote security, integrity, and availability.

Tests Performed - Our review of CIS included reviewing input controls, logical access and security controls, security of output documents, retention practices, backup and recovery procedures, change management procedures, and modifications to CIS during the fiscal year. In addition, we performed data integrity testing on two agencies' CIS data.

Results - Data entered into the system is entered by the user agency and is the responsibility of the agency. To help ensure the accuracy of the data, CIS is equipped with online edit checks which provide the user with immediate notification if errors are encountered during data entry, and processing edit checks which report processing errors online.

Error reports are available to CIS staff and to user agencies. The Department generates a Location Balance Report nightly to determine whether transactions were processed correctly. Additional reports are also available to users for reconciliation purposes. The accuracy and reconciliation of data is the responsibility of the user agency.

Access to CIS is controlled through security software, in addition to CIS' internal security. Users must have a properly authorized user ID and password to gain access to the operating environment. Once access to the operating environment has been allowed, users must have a separate application user ID and password to gain access to CIS. Assignment and authorization of access rights is the responsibility of agency security administrators.

There have been no major changes to CIS in the past year.

CIS is automatically backed up daily. The daily backups are stored in the CCF and monthly backups are rotated to an off-site storage location.

During our testing of CIS data, we did not identify any significant weaknesses. In addition, no significant weaknesses were identified in our overall review of CIS.

To ensure that controls are fully implemented and functional at the agency level, staff, internal auditors, and external auditors of agencies using CIS should:

- Verify that only accurate and authorized data are entered into CIS. It is the agency's responsibility to ensure that only properly authorized transactions are entered into the system.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the user profiles and defined user groups with access to CIS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up inventory reports, and inform appropriate CIS personnel of changes timely.

Department records listed the following entities as users of the Central Inventory System.

1. Capital Development Board
2. Department of Agriculture
3. Department of Central Management Services
4. Department of Children and Family Services
5. Department of Employment Security
6. Department of Financial and Professional Regulation*
7. Department of Human Rights
8. Department of Military Affairs
9. Department of Natural Resources
10. Department of Public Health
11. Department of Transportation
12. Department of Veterans' Affairs
13. Department on Aging
14. Educational Labor Relations Board
15. Emergency Management Agency
16. Environmental Protection Agency
17. Historic Preservation Agency
18. Illinois Deaf and Hard of Hearing Commission
19. Illinois Law Enforcement Training and Standards Board
20. Illinois Student Assistance Commission
21. Illinois Violence Protection Authority
22. Illinois Workers' Compensation Commission^
23. Office of the Attorney General
24. Office of the Governor
25. Office of the Lieutenant Governor
26. Office of Management and Budget
27. State's Attorneys Appellate Prosecutor

* The Department of Financial Institutions, the Department of Insurance, the Department of Professional Regulation, and the Office of Banks and Real Estate were consolidated on July 1, 2004.

^ Illinois Industrial Commission renamed January 1, 2005.

This Page Intentionally Left Blank

CENTRAL TIME AND ATTENDANCE SYSTEM

The Central Time and Attendance System (CTAS) is an online system that provides a comprehensive system for recording and managing employee benefit time.

CTAS was implemented in 1992. CTAS is utilized by 32 entities (see page 79 for the list of user agencies).

Control Objective - Management should ensure that the application has policies, procedures and methods to ensure that all transactions are entered, processed and reported correctly. Management should ensure that application systems are configured and controlled to promote security, integrity, and availability.

Tests Performed - Our review of CTAS included reviewing input controls, logical access and security controls, security of output documents, retention practices, backup and recovery procedures, change management procedures, and modifications to CTAS during the fiscal year. In addition, we performed data integrity testing on two agencies' CTAS data.

Results – CTAS transactions are entered online in a real-time environment. CTAS provides for attendance information to be recorded using either the positive or exception method. The positive method of recording daily attendance requires the timekeeper to enter or confirm an employee's general attendance information. The exception method assumes that an employee's scheduled work time is the correct attendance unless the timekeeper enters something different.

Data entered into the system is the responsibility of the user agency. CTAS has hundreds of edit checks built into the system to notify the user of any exceptions.

Access to CTAS is controlled through security software, in addition to CTAS' internal security. Users must have a properly authorized user ID and password to gain access to the operating environment. Assignment and authorization of access rights is the responsibility of each agency's security administrator. Once access to the operating environment has been allowed, users must have a separate application user ID and password to gain access to CTAS.

There have been no major changes to CTAS in the past year.

CTAS is automatically backed up daily and weekly. The daily backups are maintained at the CCF, with the weekly backups rotated to an off-site storage location.

During our testing of CTAS data, we did not identify any significant weaknesses. In addition, no significant weaknesses were identified in our overall review of CTAS.

To ensure that controls are fully implemented and functional at the agency level, staff, internal auditors, and external auditors of agencies using CTAS should:

- Verify that only accurate and authorized data are entered into CTAS. It is the agency's responsibility to ensure that only properly authorized transactions are entered into the system.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the user profiles and defined user groups with access to CTAS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up timekeeping reports, and inform appropriate CTAS personnel of changes timely.

Department records listed the following entities as users of the Central Time and Attendance System.

1. Capital Development Board
2. Civil Service Commission
3. Department of Agriculture
4. Department of Central Management Services
5. Department of Commerce and Economic Opportunity
6. Department of Financial and Professional Regulation*
7. Department of Human Rights
8. Department of Labor
9. Department of Natural Resources
10. Department of Public Health
11. Department of Revenue
12. Department of Veterans' Affairs
13. Department on Aging
14. Emergency Management Agency
15. Environmental Protection Agency
16. Guardianship and Advocacy Commission
17. Human Rights Commission
18. Illinois Criminal Justice Information Authority
19. Illinois Deaf and Hard of Hearing Commission
20. Illinois Education Labor Relations Board
21. Illinois Law Enforcement Training and Standards Board
22. Illinois Planning Council on Developmental Disabilities
23. Illinois Workers' Compensation Commission^
24. Office of Management and Budget
25. Office of the Attorney General
26. Office of the Governor
27. Office of the Inspector General
28. Office of the State Fire Marshal
29. Procurement Planning Board
30. Property Tax Appeal Board
31. State Appellate Defender
32. State Board of Elections

* The Department of Financial Institutions, the Department of Insurance, the Department of Professional Regulation, and the Office of Banks and Real Estate were consolidated on July 1, 2004.

^ Illinois Industrial Commission renamed January 1, 2005.

This Page Intentionally Left Blank

APPENDIX A

COMPLEMENTARY USER ORGANIZATION CONTROLS

Users of the State's Central Computer Facility are responsible for complying with prescribed requirements and for using available security mechanisms to protect the security and integrity of their data. During the course of our review we identified several areas of user agency responsibility that should be reviewed by user agencies and their internal and external auditors.

Disaster contingency plans are needed.

Due to the fact agencies rely on the Department for computing services, they should take steps to reduce the risks associated with disruption or loss. Agencies should:

- Submit to the Department a listing of critical applications at least annually, with all pertinent information.
- Submit to the Department formal disaster recovery plans.
- Ensure all data is backed up and stored off-site.
- Ensure all critical applications are tested at least annually. Additionally, agencies should submit to the Department detailed goals and results of the test.

Available security mechanism should be utilized.

User agency security coordinators should effectively utilize security software features and perform periodic reviews of existing profiles to ensure access rights are appropriate. In addition, user agency security coordinators should:

- Formally encourage users to include both alphabetic and non-alphabetic characters in their passwords, to protect the security of their account.
- Examine revoked IDs and consider:
 - Reassigning revoked IDs when possible, instead of creating new IDs.
 - Deleting IDs that are no longer necessary.
- When users are required to have the ability to reset passwords, utilize the Department's password reset utilities; powerful attributes should only be assigned to users who need administrative capabilities.

Security over Local Area Network (LAN) resources should be reviewed.

To enhance LAN security, agencies should:

- Develop and implement a Security Awareness Program to keep employees aware of security issues.
- Perform a risk assessment to evaluate the strength of their internal LAN security.
- Update all servers to the current vendor recommended patch level.
- Install and continuously update virus detection software.

Security over Internet user should be reviewed.

To enhance Internet security throughout State government, we recommend State agencies:

- Regulate and monitor Internet web-based content by utilizing resources such as Internet content filtering and access logging.

- Prohibit unsecured transmission of confidential or sensitive information across the Internet.
- Install and continuously update virus detection software.

Security over the Illinois Wireless Information Network (IWIN) should be reviewed.

To enhance IWIN security, we recommend State agencies:

- Ensure the Department is notified of accounts that need to be deactivated in timely manner.
- Monitor content transmitted through the IWIN network.
- Develop policies and procedures for IWIN Internet access.
- Install and continuously update virus detection software.

Security of Virtual Machine (VM) systems should be reviewed.

User agencies should review VM inactive user reports, determine ID status, and notify VM support staff of necessary changes. Inactive IDs are an unnecessary expense for both the Department and the user agency and should be deleted. In addition, user agencies should review the use of security permissions that permit multi-write capabilities (which may cause data to be corrupted or lost) and have it eliminated from all minidisks where it is not absolutely essential.

Security of Customer Information Control System (CICS) should be reviewed.

User agencies should:

- Coordinate with the Department to assure the automatic time-out settings for their CICS regions provide reasonable protection of the information resources for the agency, while considering their operational needs.
- Ensure their CICS regions are adequately protected using security software, including the use of recommended transaction-level security.
- Ensure powerful CICS commands are adequately restricted.

User agencies considering Web-based CICS connectivity should evaluate current CICS security features and coordinate with the Department in the developmental stages to assure their CICS applications and data resources are adequately protected.

Security of DataBase 2 (DB2) should be reviewed.

User agencies should provide timely notification to the Department's DB2 Application Support Administrator if the agency DB2 Coordinator changes. In addition, we recommend user agencies assign the usage of the "DB2 Coordinator ID" to a specific person to promote accountability for the use of the ID.

Bills for computer services should be reviewed.

User agencies should monitor the monthly billing to ensure charges are correct. Additionally, all user agencies should submit payment in a timely manner.

Control over requesting telecommunication equipment and changes should be reviewed.

User agencies should:

- Appoint a Telecommunications Coordinator as a single point of contact to aid in expediting projects, in compliance with the Department's Telecommunications Guide to Services and Procedures.
- Develop practices to ensure all service request forms are accurate, and document all necessary information to complete the request, prior to submitting the forms to the Department. Inaccurate or insufficient information may result in delays in, or a repeat of, the service request process.

Accounting Information Systems (AIS) use should be reviewed.

We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, staff, internal auditors, and external auditors of agencies using AIS should:

- Verify only accurate and authorized data are entered into AIS.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the user profiles and defined user groups with access to AIS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up AIS reports, and inform appropriate AIS personnel of changes timely.

Central Payroll System (CPS) use should be reviewed.

We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure controls are functional at the agency level, agencies should:

- Verify only accurate and authorized data are entered into CPS.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the users and user groups with access to CPS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up payroll reports, and inform appropriate CPS personnel of changes timely.
- Retain hardcopy payroll vouchers for at least the three most current pay periods, as specified by the CPS User Manual.
- Perform their own CPS data entry (applicable only to agencies that depend on the Department to perform their data entry).

Central Inventory System (CIS) use should be reviewed.

We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, staff, internal auditors, and external auditors of agencies using CIS should:

- Verify only accurate and authorized data are entered into CIS.

- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the user profiles and defined user groups with access to CIS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up inventory reports, and inform appropriate CIS personnel of changes timely.

Central Time and Attendance System (CTAS) use should be reviewed.

We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure controls are functional at the agency level, agencies should:

- Verify only accurate and authorized data are entered into CTAS.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the user profiles and defined user groups with access to CTAS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up timekeeping reports, and inform appropriate CTAS personnel of changes timely.

Note: Additional information is available to assist user agencies and their internal and external auditors in the review of these complementary controls. Please feel free to contact the Office at 217-782-6046 or auditor@mail.state.il.us.

APPENDIX B

LIST OF USER AGENCIES

1. Board of Higher Education
2. Capital Development Board
3. Chicago State University
4. Civil Service Commission
5. Commission on Government Forecasting and Accountability
6. Comprehensive Health Insurance Board
7. Court of Claims
8. Department of Agriculture
9. Department of Central Management Services
10. Department of Children and Family Services
11. Department of Commerce and Economic Opportunity
12. Department of Corrections
13. Department of Employment Security
14. Department of Financial and Professional Regulation
15. Department of Human Rights
16. Department of Human Services
17. Department of Labor
18. Department of Military Affairs
19. Department of Natural Resources
20. Department of Public Aid
21. Department of Public Health
22. Department of Revenue
23. Department of Transportation
24. Department of Veterans' Affairs
25. Department on Aging
26. East St. Louis Financial Advisory Authority
27. Eastern Illinois University
28. Emergency Management Agency
29. Environmental Protection Agency
30. Executive Ethics Commission
31. General Assembly (Senate Operations)
32. General Assembly Retirement System
33. Governors State University
34. Guardianship and Advocacy Commission
35. Historic Preservation Agency
36. House of Representatives
37. House Republican Staff
38. Human Rights Commission
39. Illinois Arts Council
40. Illinois Commerce Commission
41. Illinois Community College Board
42. Illinois Criminal Justice Information Authority
43. Illinois Deaf and Hard of Hearing Commission
44. Illinois Development Finance Authority
45. Illinois Educational Labor Relations Board
46. Illinois Housing Development Authority
47. Illinois Industrial Commission
48. Illinois Law Enforcement Training and Standards Board

49. Illinois Math and Science Academy
50. Illinois Planning Council on Developmental Disabilities
51. Illinois State Board of Investment
52. Illinois State Police
53. Illinois State Toll Highway Authority
54. Illinois State University
55. Illinois Student Assistance Commission
56. Illinois Violence Prevention Authority
57. Illinois Workers' Compensation Commission
58. Joint Committee on Administrative Rules
59. Judges Retirement System
60. Judicial Inquiry Board
61. Legislative Audit Commission
62. Legislative Information System
63. Legislative Inspector General
64. Legislative Printing Unit
65. Legislative Reference Bureau
66. Legislative Research Unit
67. Medical District Commission
68. Northeastern Illinois University
69. Northern Illinois University
70. Office of Management and Budget
71. Office of Secretary of State
72. Office of the Architect of the Capitol
73. Office of the Attorney General
74. Office of the Auditor General
75. Office of the Comptroller
76. Office of the Governor
77. Office of the Lieutenant Governor
78. Office of the State Appellate Defender
79. Office of the State Fire Marshal
80. Office of the State's Attorneys Appellate Prosecutor
81. Office of the Treasurer
82. Prisoner Review Board
83. Procurement Policy Board
84. Property Tax Appeal Board
85. Southern Illinois University
86. State and Local Labor Relations Board
87. State Board of Education
88. State Board of Elections
89. State Employees' Retirement System
90. State Police Merit Board
91. State Universities Civil Service System
92. State Universities Retirement System
93. Supreme Court of Illinois
94. Teachers' Retirement System of the State of Illinois
95. University of Illinois
96. Western Illinois University

The list of user agencies includes all entities that were users during the period of July 1, 2004 to May 27, 2005. The following information reflects merger and consolidation activities that had an impact on the historical and current year list.

Effective July 1, 2004, per Executive Order 2004-06, the Department of Financial Institutions, the Department of Insurance, the Department of Professional Regulation, and the Office of Banks and Real Estate were consolidated into the newly created Department of Financial and Professional Regulation.

Effective January 1, 2005, the Illinois Industrial Commission was renamed as the Illinois Workers' Compensation Commission.

This Page Intentionally Left Blank

APPENDIX C

BILLING ALLOCATION SYSTEM (BAS) UNAUDITED

The following information was obtained from the Billing Allocation System User Guide, dated March 7, 2005 and is provided for informational purposes.

Governor's Executive Order 2003-10 and Public Act 93-839 authorized the Department to consolidate various functions of state government; Facility Management, Legal, Internal Audit, Communications and IT. As a part of the process, the Department is authorized to transfer appropriation authority and cash from those funds that have been identified to be part of the services that are consolidated.

The Billing Allocation System (BAS) is a web-based system the Department utilizes to bill agencies for recently consolidated services: Facilities Management, Internal Audit (IOIA), communication managers, Legal, and IT. BAS is a paperless system that uses web technology to both present billing to agencies, and to capture allocation of the billing by the agencies for submission to the Department.

BAS has been developed to act as a multi-purpose tool to support various aspects of the consolidation process. While various funds and amounts have been identified by agency and consolidation effort in advance, there remains a need to track the actual funds, which benefits from the services provided by the Department each month. BAS fills that need by capturing billing detail from the various service areas and summarizing that detail into allocation billing statements. The billing statements supported by the detail records provides a foundation for agencies to indicate to the Department which funds benefited from the services provided.

Additionally, the statements along with detail records provide documentation for agencies to use for Federal Fund Participation purposes.

This Page Intentionally Left Blank

APPENDIX D

ACRONYM GLOSSARY

AIS - Accounting Information System

ARB – Architecture Rationalization Board

ARCM - Accounts Receivable Credit Memorandum

ASD - Application Systems Development

BAS – Billing Allocation System

BCCS - Bureau of Communication and Computer Services

Bureau - Bureau of Communication and Computer Services

CAF - Credit Adjustment Form

CCF - Central Computer Facility

CDMA - Code Division Multiple Access

CDPD - Cellular Digital Packet Data

CHRI - Criminal History Record Information

CICS - Customer Information Control System

CIS - Central Inventory System

CMC – Communication Management Center

CMS - Central Management Services

CPU – Central Processing Unit

CPS - Central Payroll System

CRF - Communication Revolving Fund

CSC – Customer Solution Center

CSD - CICS System Definition File

CTAS - Central Time and Attendance System

DB2 - DataBase 2

DCMS - Department of Central Management Services

Department - Department of Central Management Services

DP Guide – Data Processing Guide

EA&S – Enterprise Architecture and Strategy

EMS – Expense Management System

EPMO – Enterprise Program Office

FCIAA – Fiscal Control and Internal Auditing Act

FY – Fiscal Year

HIPAA – Health Insurance Portability and Accountability Act

ICN – Illinois Century Network

ILCS – Illinois Compiled Statutes

IMS – Information Management System

IOIA – Illinois Office of Internal Audit

ISD – Information Services Division

ISP – Internet Service Provider

IT - Information Technology

IWIN - Illinois Wireless Information Network

LAN - Local Area Network

LEADS - Law Enforcement Agencies Data System

MDC - Mobile Data Computer

MONIES - Management of Network Income Expense Services System

NCC - Network Control Center

NCIC - National Crime Information Center

NLETS - National Law Enforcement Telecommunications System

OA - Office Automation

QA – Quality Assurance

PKI - Public Key Infrastructure

SAMS - Statewide Accounting Management System

SNA - Systems Network Architecture

SR- Service Request

SRRS - Service Request Registration System

SSRF - Statistical Services Revolving Fund

TCP/IP - Transmission Control Protocol/Internet Protocol

TDR - Telecommunications Data/Intercity Service Request

TGR - Terminal Generation Request

TSR - Telecommunications Service Request

UPS - Uninterruptable Power Supply

VM - Virtual Machine

WAN - Wide Area Network

z/OS - Zero Downtime Operating System