THIRD PARTY REVIEW

Department of Central Management Services
Bureau of Communication and
Computer Services

July 2004

TABLE OF CONTENTS

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 14, 2004. Our review, started in the summer of 2003 and primarily performed between December 10, 2003 through May 14, 2004, 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 14, 2004. 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 December 10, 2003 through May 14, 2004. 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 December 10, 2003 through May 14, 2004.

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 14, 2004 and information about tests of the operating effectiveness of specified controls covers the period from December 10, 2003 through May 14, 2004. 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 by the Department to provide additional information to user organizations and is not a part of the Department's description of controls placed in operation. The information in Appendix C has not been subjected to the procedures applied in the examination of the description of controls related to Public Key Infrastructure, 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

May 14, 2004

THIRD PARTY REVIEW

Department of Central Management Services
Bureau of Communication and
Computer Services

July 2004

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; and 20 ILCS 405/405-260). To fulfill its responsibilities, the Department operates the Central Computer Facility (CCF), the Communications Center, and branch facilities in Springfield. 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 101 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 23 through 79. One of these issues warrants additional emphasis.

Disaster Contingency Planning

The Department has developed 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. 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 31-35 for additional information)

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

Department Response

We concur with your recommendations. We will continue to evaluate and enhance our planning and preparations for the business continuity of important assets for which we are responsible.

The Department response was provided on June 15, 2004, 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 20) 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 Department has five divisions within the Bureau:

- Security
- Information Management Services
- Administration and Planning
- Information Services
- Telecommunications

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.

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

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

- Strategic Plan & Digest-July 1, 2001-June 30, 2004,
- Information Technology Plan-Fiscal Years 2003 & 2004,
- Environmental Overview-November 2002, and
- Illinois Technology Enterprise Planning System-August 15, 2001.

The Department has established the Agency Strategic Accountability Council to aid in the development of the Strategic Plan & Digest.

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. In the past, IT audit was addressed on an individual basis at each agency only if resources were available. IT will now be addressed on a statewide basis, which will reduce duplication of efforts and increase efficiencies. IOIA plans to 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 that 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 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.

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 December 16, 2003,
- State of Illinois, DCMS, BCCS, ISD, Recovery Activation Plan-Revised December 16, 2003,
- State of Illinois, CMS, LAN, Recovery Activation Plan-Revised October 21, 2002, and
- State of Illinois, DCMS, Division of Telecommunications, NCC, Recovery Activation Plan-Revised November 8, 2002.

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 conducts testing at the out-of-state recovery locations twice a year. 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 two 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 procedures relating to change management. The Data Processing Guide includes the following sections:

- Creating a Change,
- Change/Approval Process,
- Change/Schedule Process,
- Category of Change,

- Documentation Elements, and
- Level of Testing.

In addition, the Problem/Change Management System is documented in the Info Change and Problem Management procedures.

All change requests are assessed by each technical area to determine any adverse issues that could result from a change. Prior to implementation, all change requests are approved.

The policies and procedures list the change management testing levels, scope of tests, and the extent of testing required for each level. The Problem/Change Management System documents that the program change was approved and tested before being placed into production. 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 Department has issued several security policies relating to information technology:

- CMS Policy Manual,
- CMS Information Technology Security Policy,
- Internet Security Policy,
- Information Security Policy - Local Area Network (LAN)/Office Automation (OA), and
- Statewide Information Security Policy BCCS/CCF Internal.

The Department has established a Security Task Force Committee that is responsible for updating the security policies and promoting security awareness for the Department.

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 (http://www.intra.state.il.us/).

The Department has assigned the responsibility for all aspects of computer security to the Security Coordinator. The duties of the Security Coordinator include:

- Directing the Department of Central Management Services (DCMS) Information Technology (IT) security administration program,
- Developing the IT security plan and procedures,
- Reviewing, testing and evaluating the IT security system, policies and procedures,
- Developing solutions for identified security issues,
- Developing a security awareness program,
- Serving as the security task force chairperson, and
- Working with internal and external auditors.

The Security Coordinator is responsible for security administration for all Departmental employees, contractual staff, and user agencies utilizing networks maintained by the Department. The Department's Regional Offices, the Telecommunications Building, the Administration and Planning Building, and the Central Computer Facility each have appointed Security Administrators.

The Department utilizes a cardkey system to provide control over access to its facilities. The system's readers are proximity readers that control and log the use of all cardkeys throughout the day at the Central Computer Facility, Telecommunications 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 a cardkey with appropriate access rights. Requests for cardkeys are submitted to the Security Coordinator for approval. An individual's access rights are based on their job duties. Visitors and employees who forget their cardkey 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 a cardkey 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 Central Computer Facility 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 in the Springfield area and a regional location.

APPLICATION SYSTEMS DEVELOPMENT CONTROLS

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 Project,
- Microsoft Project Manager, and
- Quality Assurance (QA) Project Tracking System.

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 movement of programs in a production library or panlib. 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.

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.

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 Network Control Center (NCC) Maintenance Section is responsible for problems relating to data, while the Statewide Maintenance Section is responsible for voice problem. Each problem requires a Trouble Ticket to be completed and entered into MONIES or the Voice Trouble System. The Department has developed the NCC Problem Management Methods and Procedures Manual to provide guidance on data and maintenance problems. In addition, the Department has developed the CMS Voice Repair Manual to provide guidance on voice problems.

The Department utilizes a Blockade token-based system for securing telecommunication software and dial-up lines from unauthorized access. Blockade users dial directly to the host computer. Users are required to provide a token number and id. If the user fails to authenticate, they are disconnected. The Department utilizes reports and monitoring tools to monitor user usage. Each month the Department sends activity reports to user agencies.

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 Governor, Lieutenant Governor, and the Department of Labor Local Area Networks (LAN). Additionally, there are 13 agencies that use the Department's LAN connections for email purposes.

The Department's Micro Group Support and Office Automation Systems Division provides support and maintenance of its internal LANs. The security infrastructure is interrelated between the Department's internal LANs and the LANs maintained for external agencies.

The Department has appointed a LAN Security Administrator. The Administrator is responsible for ensuring adherence to the Information Technology Security Policy. Additionally, the Department utilizes BindView to monitor users. The Administrator runs reports monthly to ensure compliance with Departmental policies and to identify any security weaknesses.

The Department maintains and supports the firewall and software that connects the Central Computer Facility and the Harris Facility to the internal Ameritech Data Network Services frame relay cloud, which provides the connection to the Internet. 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, and
- Information Technology Security Policy.

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 has established an Internet Security Team and appointed an Internet Security Manager. The Team and Manager are responsible for the security and control over the Internet.

Changes to the Department's Internet environment follow the NCC Problem Management Methods and Procedures. Changes require a TDR and management approval.

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 Resource Access Control Facility (RACF) security software to secure libraries 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. One individual 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 RACF ID and password. The user must authenticate to RACF 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.

The Department utilizes RACF software to control access and protect resources. The Department uses RACF as their primary tool for controlling and monitoring access to the Department's computer resources. RACF uses a user ID to identify the user and a password to verify the user's identity. RACF 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 three individuals with primary responsibility for RACF security and administration. The RACF Security Administrator and the RACF Programmer are responsible for the administration and security over RACF. The Security Coordinator is responsible for policies and procedures, security awareness and the Security Task Force.

The Department has an informal procedure in place for the monitoring of security violations. The RACF Security Administrator reviews violations every two weeks. Violation reports are distributed to users requesting explanations and are required to be returned within two weeks.

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 Resource Access Control Facility (RACF) software, in addition to internal security requirements. Users must have an authorized RACF 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.

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:

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 position descriptions, segregation of duties, staff qualifications, training programs, and staffing levels.

Results – The Department maintains a manual of position descriptions and annually reviews the position descriptions during staff evaluations. The position descriptions state the specialized knowledge, skills, abilities, and licensure or certification necessary for the successful performance of the work required for each position. We reviewed position descriptions with five employees, noting two of the individuals were performing duties outside of their position descriptions.

The Department provided for training through scheduled and special classes at the training center, various external training classes, and purchased self-training packages.

The Command Center operates 24 hours a day, 7 days a week, 365 days a year. Each of the shifts was designed for four operators and one supervisor, with each operator working a 12-hour shift. We reviewed timesheets for the Command Center for a two-month period noting:

- 842 hours of overtime were worked during those two months;
- 135 of 532 shifts (25%) worked during those two months were not fully staffed; and
- 116 of 532 shifts (22%) did not have supervisors present.

Over the last two fiscal years, the Department has experienced a decline in staffing due to various factors. Based on review of the Bureau's Organizational Chart, we noted:

- 110 of 528 positions (20%) were vacant; and
- 116 of 528 positions (22%) were filled by contractors.

Of the 110 vacant positions, 56 positions (51%) were deemed critical by management.

As part of the Department's IT Rationalization project, a study will be conducted of the State's IT workforce, which will include the Bureau's workforce. The workforce study is anticipated to be completed in FY05.

The current staff shortages may place undue reliance on staff members and the loss of additional staff members may place operations at risk.

Software Licenses

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

Tests Performed - We reviewed procurement rules and enterprise licensing agreements.

Results - The Department monitors enterprise licensing agreements with 4 vendors, with an annual cost of approximately $16 million.

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 Rationalization project.

Results - The Governor ordered the consolidation of the State's information technology services in the Department of Central Management Services (Department), tasking the Department with rationalizing and improving this system. The Department has embarked on the IT Rationalization project 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, staffing and qualifications, the Annual Report, and audits completed and in-progress.

Results - On March 31, 2003, the Governor signed Executive Order 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 46 executive agencies.

The primary activities of the IOIA have been related to consolidation activities. In addition, 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. The risk assessment project and associated two-year audit plan are expected to be completed by June 30, 2004.

On September 2003, the Department's Internal Audit (pre-consolidation) group submitted the required Annual Report to the Director. The Audit Plan section of the Annual Report stated, "Due to consolidation, an audit plan was not submitted for FY 2004. However, the plan approved on July 28, 2002 covered fiscal years 2003 and 2004."

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.

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 billing data for the month of December 2003 and identified several discrepancies. Although the discrepancies were not financially significant, they do indicate weaknesses in the billing process. The billing process is extremely complex, documentation to support the overall process is lacking, and great reliance is placed on the institutional knowledge of key staff members to reconcile data and mitigate errors. The Department has embarked on a program to improve documentation and transfer knowledge to existing staff.

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 April 2003 through December 2003 noting no duplicate credits and the credits appeared reasonable. In addition, we reviewed 48 credits (25 CAF and 23 ARCM) 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, 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 catch-up billings for the month of December 2003, 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, 2003 the accounts receivable (for State and non-state entities) for the SSRF and CRF were $12 million and $15.8 million, respectively.

It appears that some of the problems with the billing system are due to the complexity of the current process and the loss of institutional knowledge due to retirements.

Although reasonable administration controls existed, we recommend the Department:

- Review the complete billing process, ensure its accuracy, enhance staff knowledge of the billing system, and adequately document the process to provide the capability to understand and maintain the process.

- Perform a formal assessment of current staffing and technical experience levels and develop a staffing plan to address any deficiencies.

- Evaluate the allocation of 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 over 100 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 December 16, 2003;
- State of Illinois, DCMS, BCCS, ISD, Recovery Activation Plan-Effective December 16, 2003;
- State of Illinois, DCMS, LAN, Recovery Activation Plan-Revised March 14, 2003; and
- State of Illinois, DCMS, Division of Telecommunications, NCC, Recovery Activation Plan-Revised March 31, 2004.

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.

Staffing

Control Objective - Management should ensure staff are assigned to manage continuity services.

Tests Performed - We reviewed the organization chart, job descriptions, and information provided by continuity services staff.

Results - The Department has assigned a Continuity Services Manager and a Continuity Services Specialist to assist in ensuring the plans are updated, tested and reviewed continuously.

Additionally, the Department has assigned a Statewide Continuity and Recovery Services Coordinator to assist the Continuity Services Manager and Continuity Services Specialist. The Department has also assigned individuals responsibility for the LAN and Network Control Center (NCC) Recovery Activation Plans.

The duties of the Continuity Services Manager and Continuity Services Coordinator not only include assisting with plans, but assisting agencies with their disaster recovery planning and testing.

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 since November 2002.

The LAN Activation Plan states "frequent exercises (minimally on an annual basis) of the Plan should be scheduled and appropriately documented." In August 2003, the Department conducted an exercise of their LAN at the State Fairgrounds. The goal of the exercise was to implement an infrastructure necessary to provide network connectivity at the State Fairgrounds for 100 workstations at six different locations. The Department setup workstations throughout the Fairgrounds 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 NCC operations at the alternate facility.

As indicated above, a comprehensive test to simultaneously recover all critical applications (or even a majority of applications) has not been conducted. In addition, 21% of the Category One applications directly impacting the lives and safety of Illinois citizens have not been successfully tested even on an individual basis.

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 in place a contract for disaster recovery services at out-of-state locations.

On July 1, 2003 the Department had in place two contracts to provide for recovery services of the Department's environment. The contracts did not include testing time at the provider's sites.

On January 29, 2004, the Department signed a contract with a disaster recovery service provider for the Department's mainframe, LAN and NCC environments. The contract provides for consulting services and testing time.

We reviewed several inter-agency 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 local vault and 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. Agencies have not provided summaries to the Department, and the Department has not requested an updated list of applications from agencies since July 2002.

Currently applications are prioritized 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 addition, the agency must perform disaster recovery testing of their Category One applications at the Department's testing site and provide an analysis of the test performed. We reviewed

documentation pertaining to testing that was performed by agencies, noting the analysis of the testing provided to the Department varied, from brief emails to detailed analysis.

In the event the agency does not comply with all of the Category One requirements, its applications will not be included on the Statewide Critical Application List. We reviewed the eight agencies with Category One applications for compliance with requirements of a Category One application, noting one of the agencies had not submitted its application form and two did not have a disaster recovery plan on file. Additionally, 2 of the 8 agencies had not conducted annual testing of 6 of the State's 29 Category One applications; therefore, 21% of the State's applications affecting the safety of Illinois citizens had not been tested.

Additionally, the Department has not conducted a "comprehensive" exercise encompassing all Category One applications. Management stated staffing problems, early retirement, and the current rationalization study being conducted at the Department prevented agencies from participating.

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.

During our inspection of the vaults and the facility, we inventoried the Statewide Disaster Recovery File and backup tapes, noting several Recovery Files were outdated. Physical security and environmental controls were acceptable with the exception of humidity related problems at the local vault.

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. For the first 15-30 minutes, depending on the load, the 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, 2003 through June 30, 2004, 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. Some of these weaknesses include:

Testing:

- The Department had not conducted required testing since November 2002; and
- 6 of 29 Category One Applications at State agencies had not met the requirement of an annual test; therefore, 21% of applications affecting the safety of Illinois citizens had not undergone required testing.

Outdated documentation:

- Inter-agency agreements;
- Statewide disaster recovery file; and
- Statewide critical application listing.

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. In order to minimize risks associated with a loss of service, the Department should:

- 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 inter-agency agreements for the alternate sites, particularly agreements with agencies that have been absorbed.

Additionally, the Department should perform comprehensive disaster contingency testing and ensure all Category One applications are tested annually, as required, to protect the well-being of the citizens of Illinois.

This Page Intentionally Left Blank

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 the Daily Shift Report, Shift Change Checklist, Weekly Telephone Report, and the Infoman report.

Results - The CCF maintained several reports that record Command Center activities. The Daily Shift Report, Shift Change Checklist, Weekly Telephone Report, and the Syslog are reports utilized to record Command Center activities.

We reviewed the Shift Change Checklists for the time period of December 1 through December 6, 2003, noting reviews of system status were conducted, no significant problems were noted, and that supervisory sign-off was evident.

The Daily Shift Report (Report) is available electronically to all managers. The Report documents operational events and activities as they occur. We reviewed the Reports for the month of December 2003, noting no exceptions. The Report can be used to reconstruct the events surrounding Command Center operations.

Staff Training

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

Tests Performed - We reviewed the Daily Shift Report, Shift Change Checklist, Weekly Telephone Report, and the Infoman report.

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 Infoman and network change management procedures and tested changes for compliance with the procedures.

Results - The Department 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." In order for the Department to manage changes in a "rational and predictable manner," the Department has established formal change control processes.

The Department's DP Guide provides procedures for:

- Creating a Change;
- Change/Approval Process;
- Change/Schedule Process;
- Category of Change;
- Documentation Elements; and
- Levels of Testing.

At the time the change request is created, the requestor and creator determine the level of change based on impact, risk, communication, lead time, documentation, and education/training requirements. There are five primary categories of changes to select from: major impact; significant impact; minor impact; minimal impact; and emergency. The Change Procedures provide guidelines for each category.

We reviewed 25 change requests and noted all had a category indicated and found the Department generally complied with the Change Procedures.

Change Testing

Control Objective - Management should establish policies and procedures for testing change requests.

Tests Performed - We reviewed the Department's Infoman and network testing guidelines and tested changes for compliance with the guidelines.

Results - The Change Procedures provide six levels of testing. When requesting a change, one or more of the following levels of testing must be checked to indicate the scope and level of testing to be performed to assure successful implementation; however, this does not ensure that testing was performed:

- Functional Testing;
- In-House Testing;
- Software Vendor's Installation Verification Process;
- User Acceptance Test Period;
- Not Applicable; and
- Other.

The Change Procedures state documentation of the testing process and procedures must be on file. We reviewed testing documentation for ten completed change requests, noting that due to the various types of changes and various testing procedures that are customized specifically for these changes, testing documentation would vary to some extent. Although guidelines were generally followed, in some cases documentation to support testing did not exist.

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. 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 Help Desk function is housed in the Command Center for mainframe and Public Key Infrastructure (PKI) activities and in the Telecommunications Building for LAN activities.

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 September and November 2003, noting entries appeared to be adequately documented, and where appropriate, Infoman numbers were assigned to the call.

Management stated 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 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 25 Infoman incident calls from the Daily Shift Reports of September and November 2003 for analysis against the established service levels set within the system. We noted 44% of the calls were escalated due to the support/response target goal not being met. Of the 25 reviewed, 13 of the calls were assigned Severity Level 1, which indicates a critical business impact status. We determined the current Help Desk process is not adequately addressing the current level of service on incident calls, and in particular, the Severity Level 1 calls that should be at a much higher rate of compliance due to the critical nature of the impact to business operations.

The LAN Help Desk has three tiers within its group for incident call handling. Management stated a goal of 90% of all calls being resolved within four business days is the current acceptable standard.

LAN Help Desk personnel stated all calls coming into the Help Desk are assigned a severity/priority level. The severity levels are as follows:

1 - Problem affecting a large number of users;
2 - Problem affecting a high-level person;
3 - Normal problem;

4 - A low priority user request; and
5 - A user question.

We reviewed 25 calls from the time period of September and December 2003 for testing against the established service level of 90% of all incident calls being resolved within four business days. We noted all reviewed calls were resolved within the four-day timeframe.

To improve Computer Operations controls, we recommend the Department:

- Ensure all sections have formalized and documented testing guidelines that outline testing methods, documentation requirements, and retention requirements.

- Ensure incident calls are handled in a timely manner, particularly those designated as having a critical business impact.

This Page Intentionally Left Blank

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 more than 100 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 the organizational chart, position descriptions, and policies and procedures. We also 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); and
- Statewide Information Security Policy BCCS/CCF Internal (dated February 4, 2003).

Security Administration

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

Tests Performed - We reviewed the organizational chart, position descriptions, policies, and procedures.

Results - The position of Security and Availability Division Manager was created in May 2003, and reports to the Deputy Director/Bureau Manager. The Security and Availability Division

Manager is responsible for both physical and logical security. At least three other staff members also are assigned security related duties; however, the Security Manager for the CCF is in an acting capacity and devotes approximately 30% of their time to those duties.

In addition the Department has established a Security Task Force Committee (Committee). There are approximately 16 members on the Committee and 8 members on the Health Insurance Portability and Accountability Act (HIPAA) Policy and Procedure Security Task Force Subcommittee. The functional purpose of the Committee is to discuss and suggest changes and additions to security policies, procedures, and practices.

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.

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 and personal service contractors to review select policies and sign documents. Some examples include:

- Employee Acknowledgement of Policies; and
- Contractor Confidentiality and Access Authority Agreement.

Although there are no requirements for security training, the Department implemented a security-awareness training program that includes classes offered quarterly. During fiscal year 2004

classes were scheduled for September and December 2003, as well as March 2004; however, due to a lack of applicants all classes were cancelled.

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, reviewed practices regarding access to work areas by janitorial workers, and tested compliance with procedures regarding the assignment of temporary badges.

Results - The CCF is monitored 24 hours a day, 7 days a week, by security guards, surveillance cameras, proximity badge readers, and alarms. The third floor of the CCF houses the Command Center. The Department's Information Security Policy states the third floor of the CCF is intended to be under tight security at all times.

The CCF was built with pre-cast concrete, has a steel structure, and a shell that is non-combustible. The third floor, which houses the computer room, tape library, and the print shop, has both a fire detection and suppression system and a water detection system.

Janitorial services are provided by a contractual service. The contract describes the duties that are to be performed daily, weekly, monthly, and as directed by the building manager.

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.

The Telecommunications Building is staffed by three security guards on the 8am to 4pm shift, and by two guards on the remaining two eight hour shifts. A proximity badge reader is installed at the standalone door at the Building's front entrance.

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.

Physical security and environmental controls were acceptable at the off-site facilities with the exception of humidity related problems at the local vault.

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

- Perform a comprehensive review of its organization structure for security to ensure that security issues are effectively addressed.

- Review and update all information security policies on an annual basis to ensure policies reflect the current environment and Departmental practices. In addition, the Department should ensure that all policies are dated, all employees have access to the current versions of policies, and individuals are annually required to sign a statement of acknowledgement and understanding regarding the Department's 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.

- Develop procedures to ensure that access authorization rights (for example, cardkey badges, real property keys, and authorization listings) 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:

System 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 five systems development projects 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 cost/benefit analysis of all 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 five development projects for review. Our review indicated 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). We also examined five systems development projects to assess compliance with the Methodology.

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 20 service request forms and determined that 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 determined test plans were required for all five projects reviewed. We reviewed the test plan for completed projects, noting no exceptions.

Training Plans

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

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

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 of five projects, we determined training plans were required for four. All four projects requiring training plans were still pending.

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 five systems development projects 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. Although no significant problems were identified, our review of five systems development projects identified a few instances of non-compliance with Methodology.

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.

During our review, we examined 20 move requests, noting all were completed in compliance with the Program Library Procedures.

Although our review indicated general compliance with defined policies and procedures, we recommend Quality Assurance increase efforts to ensure complete compliance with all policies and 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.

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.

The CCF maintains network diagrams, which document 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 TCP/IP network diagram documents direct connections for State agency users, as well as connections via the frame relay network to the Department's Internet network.

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, memos are distributed periodically to user agency Telecommunications Coordinators. We reviewed copies of telecommunications-related memos and notices distributed during fiscal year 2004, and it appears memos and notices were disseminated on a regular basis.

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 submitted to the Department's Telecommunications Data Provisioning Section. The flow of the TDR process is documented in the Guide. We reviewed 10 TDR forms and determined that all 10 forms were properly completed, and all 10 requests were closed within a reasonable time frame.

Some, but not all, TDR submissions by user agencies also result in the need for software changes. When this occurs, a Terminal Generation Request (TGR) form must be completed in addition to a TDR. TGR requests are handled by the Department's Distributive Support Section of the Information Services Division and follow the Information Services Division's Change Management Procedures. In situations that require both TDR and TGR forms, the forms should be submitted by the user agency simultaneously to avoid implementation delays.

Telecommunications Service Request (TSR) forms are completed by user agencies, and submitted to the Department's Telecommunications Voice Provisioning Section. Instructions for completion of the form exist. We reviewed five TSR forms and determined that all five were properly completed. Additionally, it appears that voice requests were completed within a reasonable time frame.

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. The Network Control Center (NCC) maintenance section handles telecommunications problems pertaining to data, and problems pertaining to voice are handled by the Statewide Maintenance Section. All problems require a Trouble Ticket and must be tracked in either MONIES, or the VOice Tracking System (VOTS).

The NCC Problem Management Methods and Procedures Manual outlines the handling of data problems and maintenance, and appears to be comprehensive. Upon notice of a problem, the NCC opens a Trouble Ticket, updates the Ticket throughout the problem resolution cycle, and closes the Ticket upon resolution. All Trouble Tickets are logged in MONIES. During our review, we reviewed MONIES Trouble Tickets, and determined that all 10 were properly completed. Additionally, it appeared that data problems were being resolved timely.

The Voice Repair Manual outlines the handling of voice problems, and appears to be adequately comprehensive. As with data problems, a Trouble Ticket is opened upon notice of a problem and logged in VOTS. We reviewed 10 VOTS Trouble Tickets, and determined that all 10 were properly completed. Based on review of the Trouble Tickets, it appeared that voice problems were being resolved timely.

The Department has procedures in place to identify and resolve telecommunications problems, and they perform their duties in accordance with defined procedures.

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 that 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;
- Nextira1 and TimeView 2000 provide error logging for networking facilities to aid NCC staff in error resolution; 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.

Dial-in Security

Control Objective - Management should ensure that appropriate security measures are taken to secure dial-in access to computer resources.

Tests Performed - We reviewed the mechanisms in place that secure telecommunications software and dial-up lines. Additionally, we reviewed user agency responsibilities and activities.

Results - The Department uses a Blockade token-based system for securing telecommunications software and dial-up lines from unauthorized access. During our review, we noted 215 Blockade users at 10 user agencies.

Blockade users dial-in directly to the host computer and the user is prompted for a user ID and token number (displayed by the Blockade SecurID card). If the user's ID and Blockade token number are valid, the user is prompted for a password. If the user fails to be authenticated, they are disconnected.

Monthly, user agencies are sent a user list and are notified of users no longer using Blockade. Reporting and monitoring tools have been developed to monitor the users of the Blockade system, and agencies are also sent an activity report monthly. We reviewed the January 2004 mailing, noting 89 of 215 users had never used their Blockade SecurID card.

Internet

The Department maintains and supports the firewall hardware and software that connects the CCF and the Harris Computing Facility to the internal frame relay cloud, which provides the connection to the Internet. The Department also provides ISP (Internet Service Provider) 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.

The Department is responsible for entering rules into the firewalls and monitoring security violations. There are approximately 14 staff members who have some responsibility regarding Internet security and control. The Department has assigned an Internet Security Manager, as well as a backup, to monitor the firewalls and the Internet. Firewall incidents are reported to a four-level security group.

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.

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. The Department administers the IWIN network and the Illinois State Police provides the connection to the Law Enforcement Agencies Data System, National Crime Information Center, Secretary of State, National Law Enforcement Telecommunications System, and Criminal History Record Information that the network utilizes to provide information to IWIN users.

IWIN coverage currently exists in 101 of 102 counties in Illinois. There are approximately 8,500 unique users of the IWIN network from approximately 12 agencies, 212 municipalities, 10 colleges and universities, 1 federal agency, and 2 railway police departments. The Department's users account for approximately 13 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 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 Governor's Office, Lieutenant Governor's Office, and the Department of Labor. In addition, the Department provides LAN connections for email purposes to 13 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.

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) - formerly known a Multiple Virtual Storage (MVS)

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 CA-Examine. CA-Examine is 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.

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 error monitoring tools, procedures for authorizing and adding new users, and security issues.

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.

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 that the Department continue the assessment of security options to address risks related to the planned access to CICS from the Internet.

Resource Access Control Facility (RACF)

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 RACF included reviewing security parameters and features; Data Security Monitor 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 the RACF security system to control and monitor access to data maintained on its mainframe computers and other resources. RACF operates as an extension of, and an enhancement to, the basic z/OS and VM operating systems. It provides a mechanism for controlling access and for monitoring secured computer resources.

RACF protects by exception; that is, the user individually defines each data set to be protected by RACF. 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. RACF limits users to the pre-defined data sets for which they have access authorization. In addition, RACF 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.

RACF 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 data sets are to be protected by RACF and for properly using the available RACF resources.

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

- Develop formal policies and procedures governing RACF administration and security.

- Review the staff allocation to RACF security, administration, and support to ensure needs are met.

- Ensure all RACF profiles clearly identify the person or device assigned to RACF 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 consisting of screens and databases. AIS functions as an automated expenditure control and invoice/voucher processing system. AIS, in processing invoices, allocates invoice amounts into subaccounts; groups invoices according to the Comptroller's Statewide Accounting Management System (SAMS) requirements, for the preparation of vouchers; and allows users to track cost centers.

AIS was implemented in March 1995. AIS is currently utilized by 52 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 - AIS transactions are entered online in a real-time environment, with the ability to batch transactions for processing at a later date. 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, AIS has several edit checks to alert the user of errors. AIS provides online and batch reports, as outlined in the AIS Users Manual, that may be used for reconciliation.

Access to AIS is controlled through RACF security software, in addition to AIS' internal security. Users must have a properly authorized RACF 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 AIS. Two levels of application security enforce AIS' functional restrictions. The first level permits initial transaction entry and maintenance functions; the second level allows auditing and final transaction approval.

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 an off-site storage location. We reviewed a listing of AIS backups that were to be located at the off-site location, noting no significant exceptions.

A Financial Applications Disaster Recovery Plan was dated February 2004 and AIS was successfully recovered as a part of disaster recovery testing conducted in November 2003.

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 RACF profiles and defined user groups with access to AIS to ensure access authorized is appropriate.

- Establish policies and procedures for the administration of RACF 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 Corrections – Correctional Industries
7. Department of Financial Institutions
8. Department of Human Rights
9. Department of Insurance
10. Department of Labor
11. Department of Military Affairs
12. Department of Natural Resources
13. Department of Professional Regulation
14. Department of Public Health
15. Department of Veterans' Affairs
16. Department on Aging
17. Emergency Management Agency
18. Environmental Protection Agency
19. General Assembly Retirement System
20. Guardianship and Advocacy Commission
21. Historic Preservation Agency
22. Human Rights Commission
23. Illinois Arts Council
24. Illinois Community College Board
25. Illinois Council on Developmental Disabilities
26. Illinois Criminal Justice Information Authority
27. Illinois Deaf and Hard of Hearing Commission
28. Illinois Educational Labor Relations Board
29. Illinois Industrial Commission
30. Illinois Law Enforcement Training and Standards Board
31. Illinois Student Assistance Commission
32. Judges Retirement System
33. Judicial Inquiry Board
34. Office of Banks and Real Estate
35. Office of Management and Budget
36. Office of the Attorney General
37. Office of the Auditor General
38. Office of the Governor
39. Office of the Inspector General
40. Office of the Lieutenant Governor
41. Office of the State Appellate Defender
42. Office of the State's Attorneys Appellate Prosecutor
43. Office of the State Fire Marshal
44. Pollution Control Board
45. Prisoner Review Board
46. Property Tax Appeal Board
47. State and Local Labor Relations Board
48. State Board of Elections
49. State Employees' Retirement System
50. State Police Merit Board
51. Supreme Court of Illinois
52. Violence Prevention Authority

See Appendix B for a complete list of user entities and consolidation activities.

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 78 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 RACF security software, in addition to CPS' internal security. Users must have a properly authorized RACF 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. We reviewed a listing of CPS backups that were to be located at the off-site location, noting no exceptions.

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 the RACF profiles and defined user groups with access to CPS to ensure access authorized is appropriate.

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

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

See Appendix B for a complete list of user entities and consolidation activities.

This Page Intentionally Left Blank

CENTRAL INVENTORY SYSTEM

The Central Inventory System (CIS) is an online and batch system that allows users to maintain a record of their physical inventory and 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 surplused, 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 31 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 - CIS transactions are entered online in a real-time environment. 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.

Access to CIS is controlled through RACF security software, in addition to CIS' internal security. Users must have a properly authorized RACF 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 granted, users must have a separate application user ID and password to gain access to CIS.

During the past year, CIS was modified to interface with the Accounting Information System (AIS).

CIS is automatically backed up daily with the backups maintained at the CCF and a backup rotated to an off-site storage location monthly. We reviewed a listing of CIS backup tapes that were to be located at the off-site location, noting 4 of 65 tapes were not located at the off-site location. The tapes were located in the Tape Library.

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 RACF profiles and defined user groups with access to CIS to ensure access authorized is appropriate.

- Establish policies and procedures for the administration of RACF 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. Board of Higher Education
2. Capital Development Board
3. Department of Agriculture
4. Department of Central Management Services
5. Department of Children and Family Services
6. Department of Employment Security
7. Department of Human Rights
8. Department of Human Services
9. Department of Military Affairs
10. Department of Natural Resources
11. Department of Professional Regulation
12. Department of Public Health
13. Department of Transportation
14. Department of Veterans' Affairs
15. Department on Aging
16. Educational Labor Relations Board
17. Emergency Management Agency
18. Environmental Protection Agency
19. Historic Preservation Agency
20. Illinois Deaf and Hard of Hearing Commission
21. Illinois Industrial Commission
22. Illinois Law Enforcement Training and Standards Board
23. Illinois Student Assistance Commission
24. Office of Management and Budget
25. Office of Banks and Real Estate
26. Office of the Attorney General
27. Office of the Governor
28. Office of the Lieutenant Governor
29. Office of the State Appellate Defender
30. Office of the State's Attorneys Appellate Prosecutor
31. Violence Protection Authority

See Appendix B for a complete list of user entities and consolidation activities.

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 31 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 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 RACF security software, in addition to CTAS' internal security. Users must have a properly authorized RACF 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. We reviewed a listing of CTAS backup tapes that were to be located at the off-site location, noting no exceptions.

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 RACF profiles and defined user groups with access to CTAS to ensure access authorized is appropriate.

- Establish policies and procedures for the administration of RACF 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. Department of Agriculture
3. Department of Central Management Services
4. Department of Commerce and Economic Opportunity
5. Department of Financial Institutions
6. Department of Human Rights
7. Department of Labor
8. Department of Natural Resources
9. Department of Professional Regulation
10. Department of Public Health
11. Department of Revenue
12. Department of Veterans' Affairs
13. Emergency Management Agency
14. Environmental Protection Agency
15. Guardianship and Advocacy Commission
16. Human Rights Commission
17. Illinois Council on Developmental Disabilities
18. Illinois Criminal Justice Information Authority
19. Illinois Deaf and Hard of Hearing Commission
20. Illinois Education Labor Relations Board
21. Illinois Industrial Commission
22. Illinois Law Enforcement Training and Standards Board
23. Office of Banks and Real Estate
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 Appellate Defender
29. Office of the State Fire Marshal
30. Property Tax Appeal Board
31. State Board of Education

See Appendix B for a complete list of user entities and consolidation activities.

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 that 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.

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.

Available security mechanism should be utilized.
User agency Resource Access Control Facility (RACF) coordinators should utilize the capabilities of RACF, and perform periodic reviews of existing RACF profiles to ensure that access rights are appropriate. In addition, user agency RACF 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.
- Determine which data sets under the agency's control have a Universal Access Authority (UACC) of "alter", and change the UACC to a more restrictive parameter.
- When users are required to have the ability to reset passwords, utilize the Department's password reset utilities; the group-SPECIAL attribute should only be assigned to users who need administrative capabilities.
- Consider utilizing the group-AUDITOR attribute to aid in security administration.

Security over Internet user should be reviewed.
To enhance Internet security throughout State government, we recommend State agencies:

- Ensure that the redundant connections to the Department are maintained.
- Regulate and monitor Internet web-based content by utilizing resources such as Internet content filtering and access logging.
- Prohibit the insecure transmission of confidential or sensitive information across the Internet.
- Comply with the Statewide IT Security Policy and obtain their Internet service exclusively (unless written approval for an exception is granted) from the Department so as not to pose a potential threat to the protected environment.
- Install and continuously update virus detection software.

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

- Ensure that the Department is notified of accounts that need to be deactivated in timely manner.
- Monitor content of data transmitted through the IWIN network.
- Develop formal policies and procedures for 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 multi-write capabilities (through granting "alter" authority) 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 that automatic time-out settings for their CICS regions provide reasonable protection of the information resources for the agency, while considering their operational needs.
- Assure their CICS regions are adequately protected by RACF including the use of recommended transaction level security.
- Assure that powerful CICS commands including the CEDA, CECI, CEMT, and CEDF 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 that user

agencies assign 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 payments 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 Guide to Telecommunications 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.
- Monitor Blockade SecurID card usage, and avoid unnecessary expenditures by only purchasing cards for individuals that use the cards.

Accounting Information Systems (AIS) use should be reviewed.
To ensure that controls are functional at the agency level, agencies should:

- Establish policies and procedures for the administration of RACF IDs.
- Regularly review the RACF profiles and defined user groups with access to AIS to ensure access authorized is appropriate.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Verify that only accurate and authorized accounting data are entered into AIS. It is the agency's responsibility to ensure that only properly authorized transactions are entered into the system.
- 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.
To ensure that controls are functional at the agency level, agencies should:

- Establish policies and procedures for the administration of RACF IDs.
- Regularly review the RACF profiles and defined user groups with access to CPS to ensure access authorized is appropriate.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- 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.
- 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).

Central Inventory System (CIS) use should be reviewed.
To ensure that controls are functional at the agency level, agencies should:

- Establish policies and procedures for the administration of RACF IDs.
- Regularly review the RACF profiles and defined user groups with access to CIS to ensure access authorized is appropriate.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- 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.
- 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.
To ensure that controls are functional at the agency level, agencies should:

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

APPENDIX B

LIST OF USER AGENCIES

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

49. Illinois Farm Development Authority
50. Illinois Housing Development Authority
51. Illinois Industrial Commission
52. Illinois Law Enforcement Training and Standards Board
53. Illinois Math and Science Academy
54. Illinois Rural Bond Bank
55. Illinois State Board of Investment
56. Illinois State Police
57. Illinois State Toll Highway Authority
58. Illinois State University
59. Illinois Student Assistance Commission
60. Joint Committee on Administrative Rules
61. Judges Retirement System
62. Judicial Inquiry Board
63. Legislative Audit Commission
64. Legislative Information System
65. Legislative Printing Unit
66. Legislative Reference Bureau
67. Legislative Research Unit
68. Legislative Space Needs Commission
69. Medical District Commission
70. Northeastern Illinois University
71. Northern Illinois University
72. Office of Banks and Real Estate
73. Office of Management and Budget
74. Office of Secretary of State
75. Office of the Attorney General
76. Office of the Auditor General
77. Office of the Comptroller
78. Office of the Governor
79. Office of the Inspector General
80. Office of the Lieutenant Governor
81. Office of the State Appellate Defender
82. Office of the State Fire Marshal
83. Office of the State's Attorneys Appellate Prosecutor
84. Office of the Treasurer
85. Pension Laws Commission
86. Pollution Control Board
87. Prisoner Review Board
88. Property Tax Appeal Board
89. Southern Illinois University
90. State and Local Labor Relations Board
91. State Board of Education
92. State Board of Elections
93. State Employees' Retirement System
94. State Police Merit Board
95. State Universities Civil Service System
96. State Universities Retirement System
97. Supreme Court of Illinois
98. Teachers' Retirement System of the State of Illinois
99. University of Illinois
100. Violence Prevention Authority
101. Western Illinois University

The list of user agencies includes all entities that were users during the period of July 1, 2003 to May 14, 2004. The information below reflects merger and consolidation activities that had an impact on the historical and current year list.

Effective June 1, 2003, per Executive Order 2003-9:

- The Department of Lottery was merged into the Department of Revenue;
- The Illinois Liquor Control Commission was merged into the Department of Revenue; and
- The Illinois Racing Board was merged into the Department of Revenue.

Effective July 1, 2003, per Executive Order 2003-11, the Prairie State 2000 Authority was merged into the Department of Commerce and Economic Opportunity.

Effective July 1, 2003, per Executive Order 2003-12, the Department of Nuclear Safety was merged into the Emergency Management Agency.

Effective December 31, 2003, per Public Act 93-205, the Illinois Rural Bond Bank was merged into the Illinois Finance Authority.

Effective February 1, 2004, per Public Act 93-632:

- The Illinois Commission on Intergovernmental Cooperation was merged into the Legislative Research Unit;
- The Pension Laws Commission was merged into the Economic and Fiscal Commission; and
- The Legislative Space Needs Commission was succeeded by the Architect of the Capitol.

This Page Intentionally Left Blank

APPENDIX C

PUBLIC KEY INFRASTRUCTURE (PKI)
UNAUDITED

The Electronic Commerce Security Act (5 ILCS 175) allows the State "to facilitate and promote electronic commerce, by eliminating barriers resulting from uncertainties over writing and signature requirements, and promoting the development of the legal and business infrastructure necessary to implement secure electronic commerce."

The State of Illinois has created a Public Key Infrastructure (PKI) to facilitate development of electronic applications that could replace many of the paper processes currently employed by the State's agencies. The PKI provides tools that can identify users to an electronic application, which can help enforce or apply confidentiality and privacy requirements.

The purpose of a PKI is to manage keys and certificates, which are used for identification, entitlements, verification, and privacy. By managing keys and certificates through a PKI, an organization establishes and maintains a secure and trustworthy networking environment. A PKI enables the use of encryption and digital signature services across a wide variety of applications.

In January 2001, the State's PKI system was officially established.

The Certificate Policy for Digital Signature and Encryption Applications has been established and defines all certificate policies of the PKI system. The Certificate Policy is available on the State's web site at http://www.illinois.gov/pki.

A Policy Authority comprised of individuals representing constitutional offices, State agencies, universities, and local governments has been established. The Policy Authority is responsible for ensuring that both the security policy and the practices that are employed in issuing certificates are consistent with the policies described in the Certificate Policy.

Additional information is available on the State's web site at http://www.illinois.gov/pki.

This Page Intentionally Left Blank

APPENDIX D

ACRONYM GLOSSARY

AIS - Accounting Information System

ARCM - Accounts Receivable Credit Memorandum

ASD - Application Systems Development

BCCS - Bureau of Communication and Computer Services

Bureau - Bureau of Communication and Computer Services

CAF - Credit Adjustment Form

CCF - Central Computer Facility

CDPD - Cellular Digital Packet Data

CHRI - Criminal History Record Information

CICS - Customer Information Control System

CIS - Central Inventory System

CMS - Central Management Services

CPS - Central Payroll System

CRF - Communication Revolving Fund

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

HIPAA – Health Insurance Portability and Accountability Act

ILCS – Illinois Compiled Statutes

IOIA – Illinois Office of Internal Audit

ISD – Information Services Division

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

MVS - Multiple Virtual Storage

NCC - Network Control Center

NCIC - National Crime Information Center

NLETS - National Law Enforcement Telecommunications System

OA - Office Automation

PKI - Public Key Infrastructure

RACF - Resource Access Control Facility

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

UACC - Universal Access Authority

UPS - uninterruptable power supply

VM - Virtual Machine

VOTS - VOice Tracking System

WAN - Wide Area Network

z/OS - Zero Downtime Operating System