THIRD PARTY REVIEW

Department of Central Management Services
Bureau of Communication and
Computer Services

July 2002

TABLE OF CONTENTS

REPORT DIGEST

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES BUREAU OF COMMUNICATION AND COMPUTER SERVICES

THIRD PARTY REVIEW
For the Year Ended:
June 30, 2002

Release Date:
July 2, 2002

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

To obtain a copy of the Report contact:
Office of the Auditor General
Attn: Records Manager
Iles Park Plaza
740 E. Ash Street
Springfield, IL 62703
(217) 782-6046 or TDD (217) 524-4646

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

INTRODUCTION

The Department of Central Management Services' (Department) Bureau of Communication and Computer Services carries out statutory responsibilities relating to data processing and telecommunication services (20 ILCS 405/10; 20 ILCS 405/20; 20 ILCS 405/250; 20 ILCS 405/255; and 20 ILCS 405/260). To fulfill its responsibilities, the Department operates the Central Computer Facility (CCF), the Communications Center, and its branch facility. The 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 107 user entities.

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

We reviewed data processing general controls at the Department primarily during the period from January 22 to May 13, 2002. We performed tests to determine compliance with policies and procedures, conducted interviews, performed observations, and identified specific control objectives and procedures we considered necessary to evaluate the controls.

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

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

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

STATISTICS	2002
Mainframes	4 Units Configured as 15 Production Systems
Services/Workload	82,511 Nodes Statewide (Terminals, Printers, etc.) 78 Million IMS Transactions per Month 1.7 Million Feet of Laser Printing per Month 309,680 Reel/Cartridge Tape Mounts per Month
State Agency Users	107
CCF Employees	1999 -- 131 2000 -- 136 2001 -- 138 2002 -- 142
Historical Growth Trend*	1999 -- 1,016 -- MIPS 2000 -- 1,445 -- MIPS 2001 -- 1,557 -- MIPS 2002 -- 2,040 -- MIPS MIPS -- Million Instructions Per Second * In the month of April for each year listed

Information provided by the Department

AGENCY DIRECTOR AND BUREAU MANAGER
During Audit Period: Director: Michael Schwartz -- Bureau Manager: Frank Cavallaro Currently: Director: Michael Schwartz -- Bureau Manager: Frank Cavallaro

REPORT SUMMARY

Disaster Contingency Planning

State Government Must Be Prepared

In the past several years, the Department has made progress in addressing the disaster contingency needs of the State's Central Computer Facility; however, the plans and operational provisions still 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 continue its efforts to ensure that 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 review contingency plans and conduct comprehensive tests of the plans on an annual basis.

The Department concurred with our recommendation and stated the Department will continue to maintain, evaluate, and enhance its preparations for the business continuity of the State's critical Information Technology assets for which it is responsible.

AUDITORS' OPINION

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

WILLIAM G. HOLLAND, Auditor General

WGH:WJS:ap

SPRINGFIELD OFFICE:
ILES PARK PLAZA
740 EAST ASH • 62703-3154
PHONE: 217/782-6046
FAX: 217/785-8222 • TDD: 217/524-4646

CHICAGO OFFICE:
STATE OF ILLINOIS BUILDING • SUITE S-900
160 NORTH LASALLE • 60601-3103
PHONE: 312/814-4000
FAX: 312/814-4006

OFFICE OF THE AUDITOR GENERAL
WILLIAM G. HOLLAND

REPORT ON THIRD PARTY REVIEW
JULY 2002

The Honorable William G. Holland
Auditor General
State of Illinois

We have examined the accompanying description of 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 (3) such controls had been placed in operation as of May 13, 2002. Our review, started in the summer of 2001 and primarily performed between January 22 and May 13, 2002, was limited to controls at the Department's Central Computer Facility (CCF), the Department's Communications Center, and its branch facility. 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 13, 2002. 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.

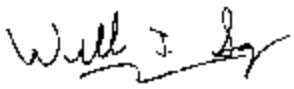
In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in the body of the report, to obtain evidence about their effectiveness in meeting the control objectives, during the period from January 22 to May 13, 2002. 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 structure, when they assess control risk at their organization. In our opinion, the controls that were tested, as described in the body of the report, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in the body of the report were achieved during the period from January 22 to May 13, 2002. However, the scope of our engagement did not

include tests to determine whether control objectives not listed in the body of the report were achieved; accordingly, we express no opinion on the achievement of control objectives not included in the body of the report.

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 13, 2002, and information about tests of the operating effectiveness of specified controls covers the period from January 22 to May 13, 2002. 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.

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 13, 2002

THIRD PARTY REVIEW

Department of Central Management Services
Bureau of Communication and
Computer Services

July 2002

REPORT SUMMARY

INTRODUCTION

The Department of Central Management Services' (Department) Bureau of Communication and Computer Services carries out statutory responsibilities relating to data processing and telecommunication services (20 ILCS 405/10; 20 ILCS 405/20; 20 ILCS 405/250; 20 ILCS 405/255; and 20 ILCS 405/260). To fulfill its responsibilities, the Department operates the Central Computer Facility (CCF), the Communications Center, and a branch facility in Springfield. The Springfield branch facility also serves as the primary backup site should a disaster prevent processing at the Central Computer Facility. Through its facilities, the Department provides data processing services to approximately 107 user agencies (see Appendix B).

The CCF functions as a data processing service center providing computing and telecommunication resources for State agencies' use. The Department and the agencies that use the Department's computer resources share the responsibility for maintaining the integrity and security of computerized data and functions. 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 7 through 53. One of these issues warrants additional emphasis.

Disaster Contingency Planning

In the past several years, the Department has made progress in addressing the disaster contingency needs of the State's Central Computer Facility; however, the plans and operational provisions still 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 continue its efforts to ensure that 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 review contingency plans and conduct comprehensive tests of the plans on an annual basis. (see page 13).

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

Department Response

DCMS will continue to maintain, evaluate, and enhance our preparations for the business continuity of the State's critical Information Technology assets for which we are responsible.

- We recognize that there are frequent changes in those assets as well as recovery best-practices. Consequently we will continue to review our plans periodically in order to maintain them at current, appropriate, effective, and efficient levels.
- We recognize that rehearsing for various disruptions is an effective method of evaluation. Consequently we will continue to require that recovery simulations for the most critical applications and associated infrastructure be performed at least annually. To the extent practicable, we will annually perform comprehensive simulations.
- We will continue to enhance our plan for business continuity to reflect the results of our reviews and rehearsals.
- We will also continue to train, to provide assistance to, and to cooperate with other State agencies in their preparations for business continuity.

The Department response was provided on June 6, 2002, by Frank Cavallaro, Manager, Bureau of Communication and Computer Services of the Department of Central Management Services.

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;
- Contingency Planning;
- Computer Operations;
- Security;
- Application Systems Development;
- Telecommunication;
- Systems Software; and
- Public Key Infrastructure.

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.

Control objectives for administration include:

- segregating duties to prevent information systems (IS) personnel's performance of incompatible functions;
- ensuring staffing is sufficient;
- providing training and direction;
- monitoring and controlling software licenses;
- ensuring that IS and user management participate in long-range planning;
- ensuring sufficient and effective Internal Audit activities; and
- billing user agencies for computer services.

Our review of the administration control objectives included a review of:

- segregation of duties, position descriptions, personnel qualifications, and staffing levels;
- training requirements, records, and documentation;
- computer software, computer purchases, and enterprise licensing agreements;
- long-range planning efforts and steering committee activities;
- Internal Audit's participation in the development or modification of computer systems and the two-year audit plan;

- the process of billing user agencies for computer services, accounts receivable, accuracy of rate structures, procedures for processing credit requests, and accuracy of user lists; and

- the status of 2001 Department administration findings.

We reviewed administration controls and noted the following:

Software Licenses - The Department has enterprise licensing agreements with 12 vendors, with an annual cost of approximately $19 million.

Command Center - The command center operates 24 hours a day, 7 days a week, 365 days a year. Each of the four shifts (two per day) were designed for four operators and one supervisor, with each operator working a 12-hour shift. During the audit period, the Department experienced staff and supervisor shortages on various shifts. The Department embarked on a training program to alleviate the shortage of supervisors, and should continue to address the staffing shortages to ensure that each shift is properly staffed and supervised.

Internal Audit Coverage of Information Systems - 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. Internal Audit should evaluate the allocation of audit resources to information technology activities to ensure that integrity and security issues are adequately addressed.

Long-Range Planning - The Department has a formal steering committee and has developed several information technology planning documents. The Department should continue to work with the Illinois Technology Office and other entities to ensure that technology issues are addressed in a comprehensive, consistent, and synchronized manner. In addition, the Department should make certain that risks (including security risks) are routinely addressed and formally incorporated into the long-range planning process.

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

The Department reported that from July 1, 2001 through March 31, 2002, $50.6 million and $88.7 million were billed from the SSRF and CRF respectively. As of March 15, 2002, the Department reported the outstanding accounts receivable total was $15.1 million and $20.5 million for the SSRF and CRF respectively.

The billing process has undergone major changes in the past two years; however, a formal training program has not been finalized to communicate the changes to staff. In addition, the Accounting Department does not have formal procedures for its portion of the billing process.

The Department should continue to utilize technological advances to enhance the billing process. In addition, we recommend the Department:

- Develop a training program for employees involved in the billing process.

- Coordinate the development of formal procedures for the billing process with the Accounting Department.

This Page Intentionally Left Blank

CONTINGENCY PLANNING CONTROLS

Contingency planning 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.

Control objectives for contingency planning include:

- adequate backup power sources;
- a written and tested disaster contingency plan;
- adequate alternate processing site(s);
- adequate backups of critical resources; and
- an alignment of processing needs with alternate site processing capabilities.

Our review of the contingency planning control objectives included a review of:

- the uninterruptible power supply (UPS) system at the CCF and measures taken to ensure an adequate alternate power supply exists at the alternate processing site;
- disaster contingency plan, including the systems and program products included in the plan, user agencies' critical application lists, recovery tests, test documentation, and disaster contingency information at the off-site storage location;
- system backup procedures, backup strategy, and verification of usability of backups;
- storage of key information, programs, and documentation in a secure, off-site location;
- restart and recovery procedures; and
- the status of 2001 Department contingency planning findings.

We reviewed contingency planning controls and noted the following:

Contingency Planning - 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.

Contingency Plans - The Department has established four disaster recovery plans: the DCMS/BCCS/ISD Continuity Methodology (dated April 17, 2002), DCMS/BCCS/ISD Recovery Activation Plan (dated April 18, 2002), DCMS LAN, Recovery Activation Plan (dated April 4, 2002), and the DCMS, Division of Telecommunications, NCC Recovery Activation Plan (dated April 5, 2002).

The DCMS/BCCS/ISD Continuity Methodology and Recovery Activation Plan are for the recovery of the Department's Central Computer Facility. The LAN Recovery Activation Plan is for the recovery of the Department's Local Area Network. The NCC Recovery Activation Plan is for the recovery of the Department's Network Control Center, Internet, and telecommunication services.

Disaster Recovery Testing – According to the DCMS/BCCS/ISD Continuity Methodology, "exercising the plan, in part or in whole, validates the plan." The Methodology states:

- Exercises involving DCMS/BCCS/ISD computing facilities and services are conducted at least twice a year.
- Exercises in other areas are to be conducted annually.
- Exercises may be conducted as a desk check, simulation, component, or comprehensive.

Although limited tests have been conducted, there is no assurance that the plans and supporting infrastructure provides the necessary recovery provisions. A comprehensive test to simultaneously recover all critical applications (or even a majority of applications) has not been conducted. In addition, all Category One (resources that directly impact the lives and safety of Illinois citizens and State employees) applications have not been successfully tested even on an individual basis nor has a detailed test of the NCC been performed.

Staffing - The Department has assigned a Disaster Recovery Manager and Coordinator to assist in ensuring the plans are updated, tested and reviewed continuously.

Contract - In December 2000, the Department signed a two-year contract for disaster recovery services for the mainframe. The contract requires the vendor to:

- develop a backup and recovery methodology;
- assess the current disaster recovery procedures;
- assess the disaster recovery plan and cookbook;
- provide a recovery site;
- provide 240 hours of testing; and
- provide off-site media storage.

Contract deliverables have been submitted and are currently being reviewed by the Department. Additionally, the Department conducted limited testing (72 hours) at the recovery site in September 2001 and is scheduled to return in October 2002.

The Department is in the process of procuring a disaster recovery services contract for the NCC and LAN to replace an existing contract, and expects to have a contract by December 2002.

Statewide Critical Application Listing - The Department maintains a Statewide Critical Application Listing based on information received from agencies. The Plan states that all agencies will be requested to annually review and update the information contained in the Statewide Disaster Recovery file. However, the Department has not requested agency updates for the past two years. In the event a disaster would occur, only those applications listed in the Statewide Disaster Recovery file would be considered for recovery. Applications are given a priority number within each category.

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.

Satellite Facilities - The Department has arranged for three satellite facilities in the Springfield area for providing disaster recovery services. In addition, the disaster recovery contracts provide out of state recovery locations.

Off-site Storage - The Department currently utilizes two off-site storage facilities: the Capitol vaults and the Harris facility. In addition, the Department stores critical information and data at a distant off-site storage facility. We found that the Statewide Disaster Recovery file was not stored off-site during our audit tests.

Backup Power Source - 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 CCF has two 6,000-gallon fuel tanks outside and one 300-gallon fuel tank inside the building. Department staff stated that the fuel supply could support operations for approximately three days, if operations were at full load capacity. The alternate processing facility (Harris facility) is also equipped with a UPS. In addition, the facility is equipped with a 1,000-gallon fuel tank for the facility's diesel turbine generators. Department staff stated that the Harris facility's fuel supply could last approximately two days if operations were at full load capacity.

A service contract agreement, effective July 1, 2001 through June 30, 2002, has been established to provide routine preventive maintenance on the UPS components located at the CCF and the Harris facility.

Restart and Recovery - The Department's Data Processing Guide provides procedures to staff for restarts and recoveries. Restarts and recoveries may occur for various reasons other than a disaster: hardware failures, new maintenance levels, new software releases, and job failures. We noted all systems were available 98.43% of the time from April 2001 to February 2002.

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.
- Ensure that all required disaster recovery information is current and stored off-site.
- Annually evaluate the interagency agreements for the alternate sites.

COMPUTER OPERATIONS CONTROLS

The command center unit of computing services is the focal point of data processing for the Central Computer Facility (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 all actions performed by computer software.

Control objectives for computer operations include:

- ensuring that operator actions, system actions, operating problems, and operating statistics are maintained;
- standards, policies, and procedures for the administration of the systems programming function;
- standards, policies, and procedures for the measurement of system performance; and
- procedures for testing and approving changes.

Our review of the computer operations control objectives included a review of:

- various logs and shift reports;
- hardware monitoring and problem handling;
- problem management reports;
- change control procedures;
- emergency change procedures;
- procedures for reviewing, testing, and approving changes;
- controls to prevent unauthorized changes to the systems; and
- the status of 2001 Department computer operations findings.

We reviewed computer operations controls and noted the following:

Operating Problems - The Department has procedures to help ensure that computer operating problems are documented, analyzed, and subject to frequent supervisory/management review.

Activity Logs - The Department maintained and reviewed several reports that record command center activities. The reports were designed to provide a complete record of all operator actions. The Department also collects, reviews, and analyzes operating statistics to identify trends, detect problems, and project future resource needs.

Change Control - The Department is utilizing an automated Problem/Change Management System.

The Department's Data Processing Guide (DP Guide) provides procedures for:

- creating a change;
- change/approval process;
- change/schedule process;
- category assignment;
- documentation elements; and
- levels of testing.

In addition, the Problem/Change Management System procedures are also documented in a section of the DP Guide.

The Problem/Change Management System stores information regarding the creation, approval, testing, scheduling, and implementation of change requests online. The Department has the capability to run routine reports to track change management activities.

We selected a sample of 25 change requests that were completed from April through December 2001 and tested for proper approval, timely implementation, category assignment, and updates to documentation. We found that the Department generally complied with the Problem/Change Management System procedures.

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.

Control objectives for security include:

- controlling access to the facilities and within the facilities;
- utilizing alarms and prevention equipment;
- providing reports and performing reviews of security violations;
- ensuring that users and employees are counseled on security considerations;
- ensuring that the security administration function is independent of computer operations;
- establishing security policies and procedures;
- establishing janitorial contracts and housekeeping responsibilities; and
- controlling magnetic tape/cartridge usage.

Our review of the security control objectives included a review of:

- controls over access into and within the Central Computer Facility (CCF), the Telecommunications Building, the Administration and Planning Building, and the Harris Facility;
- controls over keys, badges, contractor badge procedures, admission and escorting of visitors, and policies for the return of badges from employees leaving the Department's employment;
- authorization listings and data entry logs;
- alarm devices and prevention equipment for fire, water, and environmental hazards;

- security policies, procedures, and awareness program;
- janitorial service contracts;
- security management structure, roles, and responsibilities;
- controls over tape movement in and out of the CCF and tape media stored off-site;
- tape management procedures, missing tape log, and Tape Management System reports; and
- the status of 2001 Department security findings.

We reviewed security controls and noted the following:

Security Administration - The responsibility for all aspects of computer security is formally assigned to a Security Coordinator, who reports directly to the Bureau Manager.

The duties of the Security Coordinator include:

- Directing the Department's 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 Department has issued several security policies relating to information technology:

- CMS Policy Manual (dated September 1, 1998; updated during fiscal year 2002);
- CMS Information Technology Security Policy (revised December 11, 2001);
- Internet Security Policy (revised 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 March 5, 1997).

Twice a year, the Department distributes the Security Authorization List and the Tape, Print, and Diskette List to user agencies, which are to be updated and returned to the Department within two weeks. During our review, we determined that 76 of 104 (73%) agencies returned their updated Authorization Lists.

Department staff are required to sign a Statement of Understanding acknowledging receipt of Department Policies, including the IT Policy, and agreeing that it is their responsibility to read and act in accordance with the Policies.

Facility Security - 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 computer center. The Department's Information Security Policy states that the third floor of the CCF is intended to be under tight security at all times.

Visitor Access - Formal procedures exist for the issuance of badges and for granting visitors and guests access to the CCF. 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.

Alarms and Fire Prevention - 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.

Housekeeping - 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.

Tape Management - 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 its local and regional off-site storage locations.

As computers become more and more integrated into the delivery of State services, and contain critical and confidential information, security becomes even more 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. Specifically, the Department should:

- 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 and that all employees have access to the current versions of policies.

- Update all the security administrator's job descriptions to reflect current responsibilities.

- Formally promote security awareness to keep users informed and aware of security issues, and periodically assess compliance with established policies and procedures.

- Develop formal policies and procedures to ensure adequate review of security violations.

- 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.

- Develop procedures to ensure that all appropriate equipment (cardkey badges, keys) is returned and/or deactivated, and that all access authorization lists 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 designers meet 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.

Control objectives for application systems development include:

- appropriate standards, policies, and procedures to control systems and programming functions;
- properly authorized, tested, reviewed, documented, implemented, and approved activities for systems development;
- active user and management participation in defining, developing, testing, and reviewing systems and programming activities; and
- independent review of new system developments and major modifications to existing systems.

Our review of the application systems development control objectives included a review of:

- application systems development standards and methodology;
- approval of updates to the standards and methodology;
- project management tools and techniques;
- approval process for new and modified application systems;
- system, operations, program, and user documentation;
- testing requirements for new systems and major modifications to existing systems;
- post-implementation reviews;
- program library procedures;
- placing authorized programs into production;
- quality assurance function; and

- status of 2001 Department application systems development findings.

We reviewed application systems development controls and noted the following:

The Department is responsible for the development of computer systems, known as the common systems, that are available for use by State agencies, and for the Department's internal computer systems.

Standards, Methodology, and Procedures Manuals - The ASD Methodology (Methodology) (revised January 2002) and Standards and Documentation Requirements (revised March 2002) are the guides, developed in-house, for new system developments and modifications to existing systems, user manuals, the purchase of third party software, establishing user training, performing testing, and performing post-implementation reviews. During our review, we noted provisions in the Standards did not always agree with the Methodology; however, the Standards are being rewritten, with limited enforcement, until the rewrite is finalized.

The Methodology was "created to provide a structured process for the design, development and implementation of new systems, enhancements, maintenance, and ad hoc requests." The Standards and Documentation Requirements provide the 'standards' to be followed for new systems, enhancements, maintenance and ad hoc requests.

The Methodology outlines four system development phases:

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

When the Methodology was developed in 1994, the Department established a Standards Committee for reviewing current development standards, proposing new or modified standards, and implementing changes to the Methodology. We reviewed Standards Committee minutes for the first eight months of fiscal year 2002, and determined that the Committee met periodically, pertinent topics were discussed, and appropriate staff attended meetings.

The Standards Committee is responsible for approving changes to the Methodology. We compared the Methodology reviewed during the prior audit with the current Methodology to determine what changes were made during the fiscal year. All changes made to the Methodology were appropriately approved.

Project Management – The following tools were available to assist in tracking computer system projects, assigning resources, and scheduling time:

- Microsoft Project 98 for developing project plans;
- Microsoft Project Manager for managing multiple projects;
- Service Request Registration System; and
- QA Project Tracking System for verification of ASD projects

User Participation and Testing - Per the Methodology, "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 that the Project Manager request users to develop unit, system, and integration test plans.

Documentation - The Methodology states that "documentation is essential for the on-going support of the system..." and provides guidance for development and documentation of new systems, enhancements, system maintenance, and ad hoc requests.

Post-Implementation Review - The Methodology provides guidance for performing a post-implementation review. If a review is required, the Methodology states that a user representative and Quality Assurance (QA) staff must participate in the review. The purpose of a post-implementation review is to provide for a comprehensive review of the implemented project, to assure the project meets the user's needs and stated objectives, and adheres to the requirements of the Methodology.

Quality Assurance Function - The Methodology addresses the Quality Assurance function. Per the Methodology, the role of Quality Assurance is to monitor and verify that project teams adhere to the Methodology. QA uses a Checklist to identify the required tasks for projects under development. A Checklist is required for new developments and enhancement projects, but not for maintenance or ad hoc changes. QA utilizes a Quality Assurance Tracking System which contains information entered from the Checklists, such as: Service Request numbers, description, system, date of QA agreement (signing of Checklist), date of QA's last activity, current status, and phase completed.

Controls over the Production Library - Program Library Procedures exist to maintain program library security. The Program Library Procedures state that Library Control is to maintain program library security and perform special assignments, when required. The procedures are designed to ensure that new programs and modification to existing programs are thoroughly documented and approved before production moves are performed. We examined 20 move requests and determined that all were completed in compliance with the Procedures.

We selected one system development project, the Illinois Procurement Bulletin (IPB) Master Contract Database project for review. All four phases of the Methodology were completed, and all appropriate tasks were marked as required on the Checklists. The resulting documentation was adequately developed in compliance with the Methodology.

Though our review indicated compliance with defined policies and procedures, we identified some recommendations to improve their systems development process. The Department should:

- Continue and accelerate the rewrite of the Standards and Documentation Requirements.
- Ensure that Methodology and Standards Committee meetings are held on a regular basis.
- Ensure that project documentation maintained online is kept up-to-date.

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.

Control objectives for telecommunication include:

- testing and approving telecommunication software and equipment changes;
- securing dial-in access to computer resources;
- analyzing response time, detecting problems, and documenting problem resolutions;
- analyzing security and controls of telecommunications, Internet, and Local Area Network (LAN) environments; and
- utilizing available security options.

Our review of the telecommunication control objectives included a review of:

- security controls which prevent unauthorized access to telecommunication software;
- security controls over dial-in access to computer resources;
- procedures for diagnosing, logging, and resolving telecommunication problems;
- procedures controlling changes to the telecommunications network;
- documentation of the telecommunications network and attached networks;
- procedures for securing the Department’s Internet and LAN connections;
- policies and procedures for the use of the Internet and LAN;
- telecommunications service and change requests;

- LAN security settings and security assessment reports;
- Internet security and monitoring;
- firewall and router configurations;
- virus protection; and
- the status of 2001 Department telecommunication findings.

We reviewed telecommunication controls and noted the following:

Dial-in - The Department uses the Blockade token-based system for securing access to telecommunications software and protecting dial-in lines from unauthorized access.

Network Documentation - The Department maintains communications network diagrams for the Central Computer Facility (CCF), including Transmission Control Protocol/Internet Protocol (TCP/IP) and Systems Network Architecture (SNA) networks. The Department also maintains Local and Wide Area Network diagrams.

The network diagrams 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.

Change Requests - Network changes are associated with telecommunications software, data communications equipment or facilities (circuits), and voice equipment. Each type of change requires a different request form. Data communications facilities and equipment changes require a user to submit a TDR (Telecommunications Data Service Request). A TGR (Terminal Generation Request) is used to request software changes. A TSR (Telecommunications Service Request) form is used to request voice equipment, LAN installations, and fiber optics. Each user agency has a designated person that is responsible for approving these forms. We examined 10 TDR and 5 TSR forms and determined that all were properly completed, and all requests were closed within a reasonable time frame.

Telecommunication Problems - The Department has established procedures for the handling of telecommunication problems. The Network Control Center (NCC) Maintenance Section handles telecommunication problems pertaining to data. Problems pertaining to voice are handled by the Statewide Maintenance Section. All problems require a Trouble Ticket and are tracked in a computer system. We examined a sample of 20 Trouble Tickets and determined that all were properly completed, and the problems appeared to be resolved timely.

Local Area Network Security - 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 e-mail purposes to 13 agencies. The Department should ensure that security requirements are adequately addressed on all LANs it supports.

Internet Security - The Department's Internet connection was created in September 1996 and is protected by firewalls.

The Department issued a Statewide Internet Security Policy (Policy), dated December 2001, to "establish minimum security practices that must be followed while connecting to, using, and administering all current and future State Internet facilities". The Department has also issued a comprehensive Information Technology (IT) Security Policy, dated December 2001, which "governs the security of IT resources". These policies are available on the Department's Intranet.

The Policy states that State agencies must acquire Internet access from the Department and all exceptions must be approved by the Department's Director. In addition, "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 directly access the Internet.

The Policy also requires the Department to approve changes to an agency's environment before implementation. During our review we noted that a State agency's configuration is only reviewed upon the initial request, with no follow-up reviews conducted. With the continual advances in technology and staffing changes at agencies, the Department should review, update, and enforce its Policy, and routinely review agency configurations to ensure the integrity of the Department's environment.

With the continued reliance State agencies place on the Department's Internet service, 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 technology. The Department should also increase the allocation of resources toward administering, testing, monitoring, and securing the firewalls and Internet connection.

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.

Control objectives for systems software include:

- setting appropriate system parameters and security options for MVS, VM, DB2, and CICS;
- using the security features of RACF effectively; and
- ensuring access by agency users is adequately controlled.

Our review of the systems software control objectives included a review of:

- MVS and VM system parameters and security options;
- performance and error monitoring reports from the MVS and VM operating systems;
- security parameters for CICS and DB2;
- RACF security features;
- 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; and
- the status of 2001 Department systems software findings.

We reviewed systems software controls and noted the following:

Multiple Virtual Storage (MVS) – MVS is the primary operating system used at the CCF. MVS 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. MVS' continuing integrity is critical to maintain confidence in the accuracy and security of programs and data under its control.

Our general objective was to review the MVS operating system to assess the level of security and the integrity of controls in place within the operating system environment. The review of MVS was conducted by auditor observation, inquiry, and testing as well as through the use of CA-Examine. CA-Examine is an online product that provides detailed information on the hardware and software environment of the MVS system and provides information about security parameters and control mechanisms. No significant weaknesses were identified in our review of MVS. However, we recommend the Department evaluate the security over the use of universal access authority and exits.

Virtual Machine (VM) - The VM operating system is the secondary 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, such as MVS, can be run on a virtual machine under the control of VM.

VM differs from the MVS 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 MVS 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.

Our review of the VM operating system's control objectives included reviewing controls over the VM directory, performance and error monitoring tools, procedures for authorizing and adding new users, and security issues.

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) - DB2 is a relational database management system for the MVS environment that the Department makes available to user agencies. No significant weaknesses were identified in our review of DB2.

Customer Information Control System (CICS) – 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 evaluate the current time-out setting to determine if the setting meets the control objectives for the Department, and continue the assessment of security options to address risks related to the planned access to CICS from the Internet.

Resource Access Control Facility (RACF) - 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 MVS 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.

During our review of RACF security, we reviewed DSMON reports, RACF parameters and security options selected on both the MVS and VM operating systems, and the status of the RACF issues identified in the 2001 BCCS Third Party Review.

The Department implemented several security enhancements during the audit period and we encourage them to continue addressing security issues. Although RACF was reasonably well instituted, the Department should:

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

- Ensure all RACF profiles clearly identify the person or device assigned to the RACF ID. 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.

- Increase efforts to review and monitor security issues, security parameters, and unauthorized access attempts.

- Ensure adequate responses to security violations are obtained, and that sufficient action is taken when unjustified security violations occur.

This Page Intentionally Left Blank

PUBLIC KEY INFRASTRUCTURE (PKI) CONTROLS

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, that can help enforce or apply confidentiality and privacy requirements, and that provide electronic signatures that comply with both the federal E-Sign Act and the State of Illinois' Electronic Commerce Security Act.

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.

Control objectives for PKI include:

- ensuring that appropriate policies and procedures exist;
- ensuring that an appropriate security structure is established;
- ensuring that the system protects the integrity of transactions, keys, parties, and has sufficient audit trails;
- protecting resources from unauthorized or accidental disclosure, modification, or destruction; and
- ensuring certificates are issued and maintained in order to guarantee integrity.

The following framework has been established to control PKI.

In January 2001, the Department conducted the root key generation. In February 2001, the Department completed the production environment rebuild and key transfer to establish the system. The root key generation was reviewed, audited, and approved by an external audit firm.

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://www100.state.il.us/tech/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.

The Department contracted with an external audit firm to perform an examination of the internal control structure of the PKI system. The final report is expected to be delivered to the Department prior to June 30, 2002.

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), for the preparation of vouchers; and allows users to track cost centers.

AIS was implemented in March 1995. AIS is currently utilized by 58 entities (see page 41 for the list of user agencies).

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. During our review we selected two agencies' AIS data and tested for proper input, edits, and compliance with date standards. No significant weaknesses were identified.

Access to AIS is controlled through Resource Access Control Facility (RACF) 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.

Management stated that there have been no major changes to AIS in the past year. However, over the next year several changes to AIS are anticipated. These include changes to comply with Government Accounting Standard Board number 34 (GASB 34) requirements, and interfaces with other application systems.

AIS is automatically backed up daily, weekly, and monthly. The daily and weekly backups are maintained at the Central Computer Facility, with the monthly backups rotated to an off-site storage location. A Financial Applications Disaster Recovery Plan was finalized in December 2001 and AIS was successfully recovered as a part of disaster recovery testing conducted at the alternate site in December 2001.

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 user entities that were billed for use of the Accounting Information System.

1. Board of Higher Education
2. Bureau of the Budget
3. Capital Development Board
4. Department of Agriculture
5. Department of Central Management Services
6. Department of Commerce and Community Affairs
7. Department of Corrections
8. Department of Corrections – Correctional Industries
9. Department of Financial Institutions
10. Department of Human Rights
11. Department of Insurance
12. Department of Labor
13. Department of Lottery
14. Department of Military Affairs
15. Department of Natural Resources
16. Department of Professional Regulation
17. Department of Public Health
18. Department of Veteran's Affairs
19. Department on Aging
20. Emergency Management Agency
21. Environmental Protection Agency
22. General Assembly Retirement System
23. Guardianship and Advocacy Commission
24. Historic Preservation Agency
25. Human Rights Commission
26. Illinois Arts Council
27. Illinois Community College Board
28. Illinois Criminal Justice Information Authority
29. Illinois Deaf and Hard of Hearing Commission
30. Illinois Educational Labor Relations Board
31. Illinois Health Care Cost Containment Council
32. Illinois Industrial Commission
33. Illinois Law Enforcement Training and Standards Board
34. Illinois Liquor Control Commission
35. Illinois Planning Council on Developmental Disabilities
36. Illinois Racing Board
37. Illinois Student Assistance Commission
38. Judges Retirement System
39. Judicial Inquiry Board
40. Office of Banks and Real Estate
41. Office of the Attorney General
42. Office of the Auditor General
43. Office of the Governor
44. Office of the Lieutenant Governor
45. Office of the State Appellate Defender
46. Off ice of the State Fire Marshal
47. Pollution Control Board
48. Prairie State 2000 Authority
49. Prisoner Review Board
50. Property Tax Appeal Board
51. State and Local Labor Relations Board
52. State Board of Elections
53. State Employees' Retirement System
54. State Geological Survey
55. State Police Merit Board
56. State's Attorneys Appellate Prosecutor
57. Supreme Court of Illinois
58. Violence Prevention Authority

This Page Intentionally Left Blank

CENTRAL PAYROLL SYSTEM

The Central Payroll System (CPS), implemented in July 1972, is an online and batch system that standardizes payroll procedures and processing from both code and non-code 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.

The CPS is currently utilized by 85 entities (see page 45 for the list of user agencies). The CPS users can enter data online or they can request their data be entered by Department personnel. It is the goal of the Department to have all agencies enter their data online and currently 81 user agencies do enter their data online.

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. During our review, we selected two agencies' CPS data and tested social security numbers, voucher numbers, warrant amounts and date fields for proper input, edits, and compliance with date standards. No significant weaknesses were identified.

Access to CPS is controlled through Resource Access Control Facility (RACF) 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.

Management stated that there have been no major changes to CPS in the past year; however, management also stated that a rewrite of CPS is in progress.

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

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.

Department records listed the following user entities that were billed for use of the Central Payroll System:

1. Board of Higher Education
2. Bureau of the Budget
3. Capital Development Board
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 Community Affairs
11. Department of Corrections
12. Department of Financial Institutions
13. Department of Human Rights
14. Department of Insurance
15. Department of Labor
16. Department of Lottery
17. Department of Military Affairs
18. Department of Natural Resources
19. Department of Nuclear Safety
20. Department of Professional Regulation
21. Department of Public Health
22. Department of Revenue
23. Department of Veterans' Affairs
24. Department on Aging
25. East St. Louis Financial Advisory Authority*
26. Economic and Fiscal Commission
27. Emergency Management Agency
28. Environmental Protection Agency
29. General Assembly (Senate Operations)
30. Guardianship and Advocacy Commission
31. Historic Preservation Agency
32. House of Representatives – Local Offices
33. House of Representatives – Majority
34. House of Representatives – Minority
35. Human Rights Commission
36. Illinois Arts Council
37. Illinois Commerce Commission
38. Illinois Commission on Intergovernmental Cooperation
39. Illinois Community College Board
40. Illinois Criminal Justice Information Authority
41. Illinois Deaf and Hard of Hearing Commission
42. Illinois Educational Labor Relations Board
43. Illinois Health Care Cost Containment Council
44. Illinois Industrial Commission
45. Illinois Law Enforcement Training and Standards Board
46. Illinois Liquor Control Commission
47. Illinois Math and Science Academy
48. Illinois Planning Council on Developmental Disabilities
49. Illinois Racing Board
50. Illinois Rural Bond Bank
51. Illinois State Board of Investment *
52. Illinois State Police
53. Illinois Student Assistance Commission
54. Joint Committee on Administrative Rules
55. Judges' Retirement System
56. Judicial Inquiry Board *
57. Legislative Audit Commission
58. Legislative Information System
59. Legislative Printing Unit
60. Legislative Reference Bureau
61. Legislative Research Unit
62. Legislative Space Needs Commission
63. Medical District Commission *
64. Office of Banks and Real Estate
65. Office of the Attorney General
66. Office of the Auditor General
67. Office of the Governor
68. Office of the Lieutenant Governor
69. Office of the Secretary of State
70. Office of the State Appellate Defender
71. Office of the State Fire Marshal
72. Office of the Treasurer
73. Pension Laws Commission
74. Pollution Control Board
75. Prairie State 2000 Authority
76. Prisoner Review Board
77. Property Tax Appeal Board
78. State and Local Labor Relations Board
79. State Board of Education
80. State Board of Elections
81. State Employees' Retirement System
82. State Police Merit Board
83. State Universities' Civil Service System
84. State's Attorneys Appellate Prosecutor
85. Teachers' Retirement System of the State of Illinois

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

This Page Intentionally Left Blank

CENTRAL INVENTORY SYSTEM

The current Central Inventory System (CIS), implemented in 1998, is an online and batch system that allows users to maintain a record of their physical inventory and comply with the Department of Central Management Services' 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. Department management stated they are currently restricting the use of the Depreciation Process to DCMS' Accounting Division; however, it is expected that this feature will be provided later to agency users. The CIS is currently utilized by 33 entities (see page 49 for the list of user agencies).

The system 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.

During our review, we selected three months of data for two agencies and tested inventory tag numbers, changes in the price of each item from month to month, composition of data fields, and for reasonable relationships between data fields. Although no significant problems were identified, we identified some problems with select date fields and transaction codes.

Access to CIS is controlled through Resource Access Control Facility (RACF) 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.

Management stated that there have been no major changes to CIS in the past year. However, over the next year several changes to CIS are anticipated. These include changes to comply with Government Accounting Standard Board number 34 (GASB 34) requirements.

CIS is automatically backed up daily with the backups maintained at the Central Computer Facility and a backup rotated to an off-site storage location monthly.

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 user entities that were billed for use of the Central Inventory System.

1. Bureau of the Budget
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 Lottery
10. Department of Military Affairs
11. Department of Natural Resources
12. Department of Nuclear Safety
13. Department of Professional Regulation
14. Department of Public Health
15. Department of Transportation
16. Department of Veterans' Affairs
17. Department on Aging
18. Emergency Management Agency
19. Environmental Protection Agency
20. Historic Preservation Agency
21. Illinois Deaf and Hard of Hearing Commission
22. Illinois Educational Labor Relations Board
23. Illinois Health Care Cost Containment Council
24. Illinois Industrial Commission
25. Illinois Law Enforcement Training and Standards Board
26. Illinois Racing Board
27. Illinois Student Assistance Commission
28. Office of Banks and Real Estate
29. Office of the Attorney General
30. Office of the Governor
31. Office of the Lieutenant Governor
32. State's Attorneys Appellate Prosecutor
33. Violence Protection Authority

This Page Intentionally Left Blank

CENTRAL TIME AND ATTENDANCE SYSTEM

The Central Time and Attendance System (CTAS) was developed in 1992 by the Department and is currently utilized by 31 entities to provide a comprehensive system for recording and managing employee benefit time (see page 53 for the list of user agencies).

CTAS provides for attendance information to be recorded using 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.

Users are responsible for ensuring that the data entered into CTAS is valid. The CTAS application has hundreds of edit checks built into the system to notify the user of any exceptions. During our review, we selected two agencies' CTAS data and tested date fields, vacation balances, and the employee identification field for proper input, existence of edits, and compliance with date standards. No significant weaknesses were identified.

Access to CTAS is controlled through Resource Access Control Facility (RACF) 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.

Management stated that there have been no major changes to CTAS in the past year; however, management also stated that an interface with the Central Payroll System is being developed.

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

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 user entities that were billed for use of the Central Time and Attendance System.

1. Bureau of the Budget
2. Capital Development Board
3. Department of Agriculture
4. Department of Central Management Services
5. Department of Commerce and Community Affairs
6. Department of Financial Institutions
7. Department of Human Rights
8. Department of Labor
9. Department of Lottery
10. Department of Natural Resources
11. Department of Professional Regulations
12. Department of Public Health
13. Department of Revenue
14. Department of Veterans' Affairs
15. Emergency Management Agency
16. Environmental Protection Agency
17. Guardianship and Advocacy Commission
18. Human Rights Commission
19. Illinois Criminal Justice Information Authority
20. Illinois Deaf and Hard of Hearing Commission
21. Illinois Education Labor Relations Board
22. Illinois Health Care Cost Containment Council
23. Illinois Industrial Commission
24. Illinois Law Enforcement Training and Standards Board
25. Illinois Planning Council on Developmental Disabilities
26. Illinois Racing Board
27. Office of Banks and Real Estate
28. Office of the Attorney General
29. Office of the Governor
30. Office of the State Fire Marshal
31. Property Tax Appeal Board

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.

1. Disaster contingency plans are needed.

User agencies should:

- Submit to the Department a listing of critical applications, with all pertinent information.
- Develop and update disaster contingency plans to ensure the plans meet current disaster recovery needs, and submit their plans to the Department.
- Ensure that all critical data is backed up and stored off-site.
- Ensure all critical applications are tested at least annually. Additionally, agencies should submit the test goals and results to the Department

2. 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.
- Install virus detection software to protect computing resources.

3. 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.
- Review revoked IDs, and delete unneeded IDs.
- 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.
- Utilize the Department's password reset utilities rather than the group-SPECIAL attribute for routine password resets.
- Consider utilizing the group-AUDITOR attribute to aid in security administration.

4. Security over Internet user should be reviewed.

Determine whether the agency's Internet connection is secure by determining:

- Whether the agency's Internet connection is through DCMS.
    - If not, determine if the agency has an exemption approved by the Director of DCMS.
    - If so, determine if the agency's Internet configurations was reviewed and approved by DCMS before the direct connection was allowed.
- Whether the agency regulates and monitors Internet web-based content by utilizing resources

such as Internet content filtering and access logging.

- Whether the agency prohibits the insecure transmission of confidential or sensitive information across the Internet.
- Whether the agency complies with the Statewide IT Security Policy.
- Whether the agency installs and continuously updates virus detection software.

5. Web-Site Privacy Policies should be reviewed.

Determine whether the agency has posted an acceptable privacy policy by determining:

- Whether privacy policies are readily accessible on an agency's web-site (such as being located on the homepage and other places where personal information is collected).
- Whether the privacy policies clearly identify the use of any technology used to collect information on or track individual users.
- Whether the privacy policies contain provisions that effectively disclose practices regarding the following:
    - Notice - provide users clear and conspicuous notice of the agency's information practices, including what information is collected, how it is collected (e.g., directly or through non-obvious means, such as cookies) and how it is used.
    - Choice - offer users choices as to how personal identifying information is used beyond the use for which the information was provided.
    - Access - offer users reasonable access to the information the web-site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.
    - Security - take reasonable steps to protect the security of the information collected.

6. 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.
- Delete inactive IDs, as they are an unnecessary expense for both the Department and the user agency.
- Review the use of multi-write capabilities (through granting ALTER authority) and have it eliminated from all minidisks where it is not absolutely essential.

7. Security of CICS should be reviewed.

User agencies should coordinate with the Department to ensure that automatic time-out settings for their CICS regions provide reasonable protection of the information resources for the agency, while considering their operational needs.

8. Security of DB2 should be reviewed.

User agencies should:

- Provide timely notification to the DB2 Software Support Group of agency DB2 coordinator changes and verify or update DB2 coordinator on the security-related lists as requested by the CCF Security Administrator.

9. The accuracy of agency security lists should be reviewed.

User agencies should update and return their Security Authorization List and Tape, Print, and Diskette Lists to the CCF Security Administrator within two weeks.

10. Bills for computer services should be reviewed.

User agencies should:

- Monitor monthly billing to ensure charges are correct.
- Submit payment in a timely manner.

11. Control over requesting telecommunication equipment and changes should be reviewed.

User agencies should:

- Submit their Telecommunication Generation Request (TGR) forms and Telecommunications Data/Intercity Request (TDR) forms simultaneously, when both are required, to avoid implementation delays.
- 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.

12. Accounting Information Systems (AIS) use should be reviewed.

To ensure that controls are functional at the agency level, agencies that utilize 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.

13. Central Payroll System (CPS) use should be reviewed.

To ensure that controls are functional at the agency level, agencies that utilize 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.

14. Central Inventory System (CIS) use should be reviewed.

To ensure that controls are functional at the agency level, agencies that utilize 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.

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

To ensure that controls are functional at the agency level, agencies that utilize 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.

APPENDIX B
LIST OF USER AGENCIES

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

54. Illinois Industrial Commission
55. Illinois Law Enforcement Training and Standards Board
56. Illinois Liquor Control Commission
57. Illinois Math and Science Academy
58. Illinois Planning Council on Developmental Disabilities
59. Illinois Racing Board
60. Illinois Rural Bond Bank
61. Illinois Sports Facilities Authorities
62. Illinois State Board of Investment
63. Illinois State Police
64. Illinois State Toll Highway Authority
65. Illinois State University
66. Illinois Student Assistance Commission
67. Joint Committee on Administrative Rules
68. Judges Retirement System
69. Judicial Inquiry Board
70. Legislative Audit Commission
71. Legislative Information System
72. Legislative Printing Unit
73. Legislative Reference Bureau
74. Legislative Research Unit
75. Legislative Space Needs Commission
76. Medical District Commission
77. Northeastern Illinois University
78. Northern Illinois University
79. Office of Banks and Real Estate
80. Office of the Attorney General
81. Office of the Auditor General
82. Office of the Comptroller
83. Office of the Governor
84. Office of the Lieutenant Governor
85. Office of Secretary of State
86. Office of the State Appellate Defender
87. Office of the State Fire Marshal
88. Office of the Treasurer
89. Pension Laws Commission
90. Pollution Control Board
91. Prairie State 2000 Authority
92. Prisoner Review Board
93. Property Tax Appeal Board
94. Southern Illinois University
95. State and Local Labor Relations Board
96. State Board of Education
97. State Board of Elections
98. State Employees' Retirement System
99. State Police Merit Board
100. State Universities Civil Service System
101. State Universities Retirement System
102. State's Attorneys Appellate Prosecutor
103. Supreme Court of Illinois
104. Teachers' Retirement System of the State of Illinois
105. University of Illinois
106. Violence Prevention Authority
107. Western Illinois University