REPORT DIGEST

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES BUREAU OF COMMUNICATION AND COMPUTER SERVICES

THIRD PARTY REVIEW
For the Year Ended:
June 30, 2000

Release Date:
July 6, 2000

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 405/35.3; 20 ILCS 405/35.7; 20 ILCS 405/35.7a; 20 ILCS 405/35.7c; and 20 ILCS 405/35.8). 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 Central Computer Facility. Through its facilities, the Department provides data processing services to approximately 104 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 20 to April 14, 2000. 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	2000
Mainframes	4 Units Configured as 21 Systems
Services/Workload	82,511 Nodes Statewide (Terminals, Printers, etc.) 68.3 Million IMS Transactions per Month 3 Million Feet of Laser Printing per Month 230,000 Reel/Cartridge Tape Mounts per Month
State Agency Users	104
CCF Employees	1997 -- 126 1998 -- 125 1999 -- 131 2000 -- 136 (includes 8 vacancies)
Historical Growth Trend*	1975 -- 400 -- Base CPU Hours Billed 1980 -- 1,700 -- Base CPU Hours Billed 1990 -- 14,143 -- Base CPU Hours Billed 1995 -- 34,977 -- Base CPU Hours Billed 1996 -- 44,201 -- Base CPU Hours Billed 1997 -- 47,618 -- Base CPU Hours Billed 1998 -- 75,900 -- Base CPU Hours Billed 1999 -- 96,393 -- Base CPU Hours Billed 2000 -- 133,752 -- Base CPU Hours Billed * In the month of January 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

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 (CCF) is provided through the Statistical Services Revolving Fund (SSRF) and the Communications Revolving Fund (CRF).

The Department reported that from July 1, 1999, through February 29, 2000, $55 million and $69 million were billed from the SSRF and CRF respectively.

Billing System Issues

Overall, we found the billing process to be extremely complex and manually intensive with an over-reliance on key staff members. Some of the specific issues we identified included:

- Of the 34 sources of monthly billing data for the SSRF, 23 are provided to billing staff in hardcopy form and manually entered into billing systems. Manual processes are needed for 15 percent ($8.3 million of the total $55 million) of the gross monthly billings.
- We noted incorrect amounts recorded in the credit log and no documentation of an independent review of the credit log.
- Two months' billing for one of the four components of the Network Services were delayed for several months and estimated, due to a loss of data.
- One agency's monthly billing was understated by $160,908, due to a manual data entry error, and corrected on a subsequent billing.
- The approved rate for payroll services was not increased in the Central Payroll System, resulting in an approximate loss of revenue of $14,000.

We recommend the Department institute measures to strengthen controls in the billing process to ensure its accuracy by reducing manual intervention and its reliance on key staff members.

Change Control

Procedures Not Always Observed

Although the Department has procedures for controlling changes to software, we found that the process was manually intensive and not always observed. The procedures contain guidelines for approving changes, based on the priority category of the change, and require signatures at different points in the process. However, we identified numerous instances of noncompliance with the procedures and concluded that the current procedures do not agree with the change control practices.

The Department issued a request for proposal for fully automating the change control procedures on October 13, 1999. The Department should accelerate the selection and implementation of a comprehensive change management system.

Disaster Contingency Planning

State Government Must Be Prepared

Although the Department has made progress in addressing the disaster contingency needs of the State's Central Computer Facility, 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, a comprehensive and thoroughly tested disaster contingency plan and sufficient backup facilities are essential components of recovery efforts.

The Department should continue its efforts to ensure that the necessary components are available to provide for continuation of critical computer operations in the event of a disaster. In addition, the Department should continue to conduct comprehensive tests of the disaster recovery plan on an annual basis.

The Department concurred with our recommendations.

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

THIRD PARTY REVIEW

Department of Central Management Services
Bureau of Communication and
Computer Services

July 2000

TABLE OF CONTENTS

REPORT ON THIRD PARTY REVIEW
JULY 2000

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 April 14, 2000. Our review, started in the summer of 1999 and primarily performed between January 20 and April 14, 2000, 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 April 14, 2000. 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 20 to April 14, 2000. 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 20 to April 14, 2000. 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 April 14, 2000, and information about tests of the operating effectiveness of specified controls covers the period from January 20 to April 14, 2000. 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

William J. Sampias, CISA
Director, Information Systems Audits

April 14, 2000

THIRD PARTY REVIEW

Department of Central Management Services
Bureau of Communication and
Computer Services

July 2000

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 405/35.3; 20 ILCS 405/35.7; 20 ILCS 405/35.7a; 20 ILCS 405/35.7c; and 20 ILCS 405/35.8). 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 104 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 11 through 53. Three of these issues warrant additional emphasis.

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 (CCF) is provided through the Statistical Services Revolving Fund (SSRF) and the Communications Revolving Fund (CRF).

The Department reported that from July 1, 1999, through February 29, 2000, $55 million and $69 million were billed from the SSRF and CRF respectively. As of January 2000 the Department reported the outstanding accounts receivable total was $15 million and $24.8 million for the SSRF and CRF respectively.

Overall, we found the billing process to be extremely complex and manually intensive with an over-reliance on key staff members. Some of the specific issues we identified included:

- Of the 34 sources of monthly billing data for the SSRF, 23 are provided to billing staff in hardcopy form and manually entered into billing systems. Manual processes are needed for 15 percent ($8.3 million of the total $55 million) of the gross monthly billings.
- The credits issued to user agencies as a result of the SSRF biannual reviews are manually input into the billing system. During FY99 $10 million of SSRF credits were issued to user agencies.
- We noted incorrect amounts recorded in the credit log and no documentation of an independent review of the credit log. In addition, we noted several credit forms lacked authorized approvals.
- Two months' billing for one of the four components of the Network Services were delayed for several months and estimated, due to a loss of data. We noted a lack of reconciliation procedures in Network Services' compilation process.
- One agency's monthly billing was understated by $160,908, due to a manual data entry error, and corrected on a subsequent billing.
- The approved rate for payroll services was not increased in the Central Payroll System, resulting in an approximate loss of revenue of $14,000.

We recommend the Department institute measures to strengthen controls in the billing process to ensure its accuracy by reducing manual intervention and its reliance on key staff members (see page 13).

Department Response

The Bureau plans to recommend to management the hiring of an outside consultant to review all billing practices, policies and procedures, to assess the strength of our controls and to recommend changes. While many of the Office of the Auditor General's recommendations are currently being implemented, we feel an outside party's thorough review of our operation will assist us in achieving the necessary level of accuracy and control.

Change Control

Although the Department has procedures for controlling changes to software, we found that the process was manually intensive and not always observed. The procedures contain guidelines for approving changes, based on the priority category of the change, and require signatures at different points in the process. However, we identified numerous instances of noncompliance with the procedures and concluded that the current procedures do not agree with the change control practices.

Accepted information systems guidelines promote the implementation of procedures to ensure that software changes are controlled to help ensure the integrity of the computer system and user applications.

The Department issued a request for proposal for fully automating the change control procedures on October 13, 1999. The Department should accelerate the selection and implementation of a comprehensive change management system. In the interim, the Department should enhance the control over changes (see page 21).

Department Response

We have a vendor currently working on the automation of change control procedures. We anticipate these will address most, if not all, of these issues. Once these changes are implemented, we plan to review and assess our procedures and make any additional changes that ensure adequate controls.

Disaster Contingency Planning

Although the Department has made progress in addressing the disaster contingency needs of the State's Central Computer Facility, 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, a comprehensive and thoroughly tested disaster contingency plan and sufficient backup facilities are essential components of recovery efforts.

The Department should continue its efforts to ensure that the necessary components are available to provide for continuation of critical computer operations in the event of a disaster. In addition, the Department should review contingency plans, conduct comprehensive tests of the plans on an annual basis, and continue efforts with vendors to assess and revise contingency plans (see page 15).

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

Department Response

In the past year, the Department issued Requests for Proposals soliciting vendors to assist with all phases of disaster contingency planning. We are currently working with a vendor on LAN and NCC contingency, and expect to have a contract in place very soon for the mainframe operation. We intended these contracts, along with our past actions and the work of our staff, to provide the necessary recovery capability for all critical operations. We look forward to the Office of the Auditor General's assessment of our program after implementation of the contract requirements.

The Department responses were provided on June 7, 2000, 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; and
- Systems Software.

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

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;

- providing training and direction;

- ensuring that IS and user management participate in long-range planning;

- ensuring that the computer security administration function is independent of computer operations;

- providing reports and performing reviews of attempted security violations; and

- ensuring that users and employees are counseled on security considerations.

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

- segregation of duties and job descriptions;

- training requirements, records, and documentation;

- Internal Audit's participation in the development or modification of computer systems and their two-year audit plan;

- statements of current insurance coverage for computer and telecommunications equipment, and a comparison of coverage to the computer equipment inventory;

- computer software, computer purchases, and master license agreements;

- long-range planning efforts;

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

- year 2000 compliance;

- computer security administrators' responsibilities and independence;

- security policies;

- general state of security awareness; and

- the status of 1999 Department administration findings.

We reviewed administration controls and noted the following:

Insurance Coverage - The Department currently has two insurance policies: 1) insuring approximately $56 million of computer equipment; and 2) insuring approximately $13 million of telecommunications equipment.

Year 2000 - The State placed a great deal of emphasis on Year 2000 planning efforts and a coordinated effort appears to have helped prevent significant problems in the delivery of State services. The Illinois Technology Office estimated that the State spent $137 million to ensure State government computer operations were Year 2000 compliant.

Internal Audit Coverage of Information Systems - The Department oversees a $200 million computer operation and relies heavily on electronic data processing activities to provide services to other agencies and to perform its own functions. Since the Department's Internal Audits (IA) Division has a mandated requirement to perform reviews of system developments and major modifications to existing systems, IA should reconsider their process for identifying system development projects that meet the criteria for a statutorily mandated review.

Security Administration – The responsibility for all aspects of computer security is formally assigned to a Security Officer, who is also the Assistant to the Bureau Manager. The CCF Security Administrator, Local Area Network (LAN) Security Administrator, and the Internet Security Administrator, report to the Security Officer for security-related issues. A comprehensive Information Technology (IT) Security Policy (Policy) exists. All other IT security policies are subordinate to the Policy. The Department's other security policies include:

- Statewide Information Security Policy (dated March 5, 1997);
- Statewide Information Security Policy Internet (dated December 6, 1996);
- Statewide Information Security Policy Intranet (dated August 11, 1999);

- Statewide Information Security Policy for Local Area Network (LAN) and Office Automation (OA) (dated May 26, 1995); and,
- Network Software Guide (dated January 29, 1999).

Department staff are required to sign a Statement of Understanding acknowledging receipt of the Policy and agreeing that it is their responsibility to read and act in accordance with the Policy. However, we determined that new employees this fiscal year had not been asked to sign a Statement of Understanding.

As computers become more and more integrated into the delivery of State services, and contain critical and confidential information, security becomes even more essential. Additionally, new initiatives introduce security concerns that must be adequately and globally addressed. Therefore, we strongly recommend that the Security Officer hold monthly meetings to address the myriad of security issues that will impact the security and integrity of the State's data. In addition, we recommend that the Department update their security polices and require all staff to sign a Statement of Understanding, as required by the Policy Manual.

Software Licenses - The Department has 12 enterprise licensing agreements with software vendors at an annual cost of $13.6 million. The Department also has maintenance contracts with 49 individual software vendors.

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 (CCF) is provided through the Statistical Services Revolving Fund (SSRF) and the Communications Revolving Fund (CRF).

The Department reported that from July 1, 1999, through February 29, 2000, $55 million and $69 million were billed from the SSRF and CRF respectively. As of January 2000 the Department reported the outstanding accounts receivable total was $15 million and $24.8 million for the SSRF and CRF respectively.

Overall, we found the billing process to be extremely complex and manually intensive with an over-reliance on key staff members. Some of the specific issues we identified included:

- Of the 34 sources of monthly billing data for the SSRF, 23 are provided to billing staff in hardcopy form and manually entered into billing systems. Manual processes are needed for 15 percent ($8.3 million of the total $55 million) of the gross monthly billings.

- The credits issued to user agencies as a result of the SSRF's biannual reviews are manually input into the billing system. During FY99, $10 million of SSRF credits were issued to user agencies.
- We noted incorrect amounts recorded in the credit log and no documentation of an independent review of the credit log. In addition, we noted a lack of authorized approvals.
- Two months' billing for one of the four components of the Network Services were delayed for several months and estimated, due to a loss of data. We noted a lack of reconciliation procedures in the Network Services' compilation process.
- One agency's monthly billing was understated by $160,908 due to a manual data entry error, and corrected on a subsequent billing.
- The approved rate for payroll services was not increased in the Central Payroll System, resulting in an approximate loss of revenue of $14,000.

In addition, we noted:

- Agencies were not charged for the correct number of library tapes purchased. The improper billing resulted in a net over charge of $423.
- The "Summary of BCCS/SSRF Bill" did not agree to detail support.
- Multiple agency code listings are used throughout the billing process. In addition, numerous agency names are incorrect.
- Computer program and table changes to the SSRF billing system do not follow the Department's formal change control process.

We recommend the Department institute measures to strengthen controls in the billing process to ensure its accuracy by reducing manual intervention and reliance on key staff members. Specifically, we recommend the Department implement the following:

- Utilize technology and automation to the fullest extent possible to reduce to a minimum the number of manual entries needed in the billing process.
- Implement additional formal reconciliation procedures.
- Implement controls to ensure all services are billed at the "approved" rate.
- Ensure proper and consistent user entity names and codes throughout the billing process.
- Comply with the Bureau's formal change control process for all program and table changes made to billing systems.

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); 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 back-up procedures, back-up strategy, and verification of usability of back-ups;
- storage of key information, programs, and documentation in a secure, off-site location;
- restart and recovery procedures; and
- the status of 1999 Department contingency planning controls.

We reviewed contingency planning controls and noted the following:

Contingency Planning - The Department provides 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 disruption 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, offsite storage of backups, designation of an alternate processing facility, and availability of a backup power supply.

The Department has developed three disaster recovery plans: the CMS/BCCS/ISD (Mainframe) Disaster Recovery Plan, the NCC (Network Control Center) Disaster Recovery Plan, and the LAN (local area network) Disaster Recovery Plan. The Mainframe Disaster Recovery Plan, dated February 1999, is for the recovery of the Department's Central Computer Facility. The NCC Disaster Recovery Plan, dated February 1996, is for the recovery of the Department's Network Control Center, Internet, and telecommunication services. The LAN Disaster Recovery Plan, dated June 1997, is for the recovery of the Department's local area network.

In December 1999, the Department entered into a consulting contract for analysis and assistance in the rewrite of the Department's NCC and LAN disaster recovery plans. We reviewed the contract and determined there were no due dates specified for the contract's deliverables. We also noted that, in addition to the Department, six other agencies are participating in the consulting services contract:

- Capital Development Board,
- Illinois Health Care Cost Containment Council,
- Illinois State Police,
- Department of Professional Regulation,
- Department of Public Aid, and
- Department of Public Health.

The contract provisions require the vendor to provide a backup strategy assessment of each agency's current backup policies and procedures, a disaster recovery test plan assessment, and a recovery site. In addition, the agencies participating will receive 24 hours of disaster recovery testing at the vendor's recovery site.

The Department is in the process of finalizing a mainframe disaster recovery consulting services contract.

Alternate Processing Location - The Department has three satellite facilities for providing disaster recovery capabilities. The Harris facility is the primary backup and disaster recovery site for the Department's mainframe operations. The Department's LAN backup and recovery site is located at the Emmerson Building on the Illinois State Fair grounds; however, the agreement with the Department of Agriculture lacks specific terms, does not identify the responsibilities of each party, and has not been renewed since 1997. In addition, the Department has a backup site for their NCC operations at the Department of Nuclear Safety.

Disaster Recovery Testing - The Department is to conduct a comprehensive disaster recovery test at least annually, as required by the Disaster Recovery Plan. However, the Department did not conduct the comprehensive test this past year. Department staff stated that the extensive Year 2000 testing that user agencies performed was a sufficient substitute for the annual comprehensive test. The Department plans a comprehensive test in October or November 2000. The Department's NCC and LAN Disaster Recovery Plans have not been tested in the last two audit periods. Department management stated that the disaster recovery consulting services contract includes 24 hours of recovery testing, within the next 18 months, for the agencies identified in the contract.

Statewide Critical Application Priority Listing - The Department maintains a Statewide Critical Application Priority Listing based on information received annually from user agencies. Department management stated that, in the event of a disaster, all Category 1 critical applications that have met the requirements as outlined in the Mainframe Disaster Recovery Plan, would be recovered. Depending on the availability of resources, additional applications would be recovered, beginning with Category 2 and working toward Category 5. The applications are prioritized based on the following five categories:

- Category 1 - Human Safety - applications that are critical to the support of human safety.
- Category 2 - Critical Human Services - applications that are critical to the welfare of humans in the State.
- Category 3 - Non-Critical Human Services - applications that are non-critical to the welfare of humans in the State.
- Category 4 - Administrative Services - applications that support the administrative process of the State.
- Category 5 - Maintenance Activities - applications that contain items related to the maintenance of the information-processing environment.

Annually, Department staff request that all agencies review and update the information they have submitted for the Department's Statewide Disaster Recovery file. We reviewed the seven agencies with applications classified as Category 1 on the Statewide Critical Application Listing and noted that one agency had not submitted the required forms for inclusion of its critical applications.

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. In addition, the turbines are solar powered. Department staff stated that the fuel supply could support operations for approximately three days, if operations were at full load capacity. Currently the CCF's processing load utilizes approximately 60-70 percent of the UPS' capability.

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.

Off-site Storage of Backups - The Department has two offsite storage facilities for tape media: the Capitol vaults and the Harris facility.

Although the Department has made great strides in assuring its recovery capabilities in the event of a disaster, we recommend the Department:

- Continue their efforts with the vendor in assessing and revising the Mainframe and LAN Disaster Recovery Plans in order for the Department to ensure that both plans meet the needs of the State in the event of a disaster. The Mainframe and the LAN plans should address the operations of the CCF and the Communications Center and include procedures for invoking the UPS at the CCF or the Harris facility.
- Ensure the three disaster recovery plans are reviewed annually.
- Ensure a comprehensive test of all the Department's plans is performed at least annually.
- Update their agreement with the Department of Agriculture for the use of the Emmerson Building. The agreement should specify terms and responsibilities of each party and be signed by the current Directors.
- Require all Category 1 applications (critical applications) be tested prior to being added to the Statewide Critical Application Priority Listing.

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 prime 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;
- care and maintenance of equipment and facilities;
- controlling job schedules;
- standards, policies, and procedures for the administration of the systems programming function;
- standards, policies, and procedures for the measurement of system performance;
- procedures for testing and approving system software changes; and
- using available error correction techniques.

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

- computer analysis logs and shift summary reports;
- hardware monitoring and problem handling;
- job scheduling procedures and Information Management Problem Summary Reports;
- systems software change control procedures;
- the Automated Library Authorization function;

- procedures for testing and approving system software changes;
- controls to prevent unauthorized changes to the systems;
- care of equipment and facilities;
- CCF janitorial contracts and housekeeping responsibilities;
- operator work schedules and overtime; and
- the status of 1999 Department computer operations findings.

We reviewed computer operations controls and noted the following:

Care of Equipment and Facilities - The CCF had policies and procedures for the care of equipment and facilities, including written policies that govern activities allowed and prohibited in the computer room. New employees are instructed to read the policies and manuals and sign a form stating that they have read and understand the rules and regulations. We reviewed the forms for eight command center employees and noted that two of the employees had not signed the forms because they had not yet received the internal security policy although one had been an employee for seven months and the other for three months.

Housekeeping - Housekeeping duties for the CCF are performed by a contractual janitorial service. The contract, outlining the duties of the contractor, is renewed on an annual basis.

Computer Operators - The command center is staffed 24 hours a day, 7 days a week. Each of the command center's four shifts (two per day) were designed for four operators and one supervisor. The computer operators work 12-hour shifts for a total of 7 days every 2 weeks. The operators' responsibilities are to monitor the systems, respond to any system messages, and answer the phones for problem calls. Command center staff shortages have resulted in numerous overtime hours for the operators, shifts not staffed at desired rates, and several shifts in which no supervisor was present.

Operating Problems - The Department has developed procedures to help ensure that computer operating problems are documented, analyzed, and subjected to frequent management review. During our review, we determined that operating problems were all assigned the same priority code and that some problems were listed as "unresolved" for long periods of time.

Change Control - The Department has change control procedures which are maintained in the DP Guide (Data Processing Guide). These procedures contain guidelines for approving system changes. The Department issued a request for proposal for fully automating the change control procedures on October 13, 1999. However, we determined that the current procedures in the DP Guide were outdated, were not always followed (i.e., forms routinely did not contain all of the required information or appropriate authorization), and testing was generally not documented.

We recommend the Department:

- Ensure that all employees of the CCF receive the Employee Information Manual and sign the appropriate forms on their first day of employment.
- Develop and implement strategies aimed at attracting and retaining computer operators for the command center.
- Assign an appropriate priority code to each problem and ensure that problems are resolved and closed within a reasonable timeframe.
- Implement the new automated change control system as soon as possible. In the interim, the Department should strengthen controls over the change process by:
  - Ensuring that all change request forms are fully completed, comply with the DP Guide, and contain all the information applicable to the change.
  - Preventing command center operators from allowing any changes to be made without proper management approval.
  - Discontinuing use of “approved” as a valid entry on the status line of the hard-copy change request form.
  - Documenting the criteria for assigning a “designee”, and identifying the designee(s) of either the Computing Services Manager or Software Manager.
  - Ensuring that test results are documented on the change request form.

SECURITY CONTROLS

The presence of security controls reduces or prevents disruption of service, loss of assets, and unauthorized access to equipment. An effective physical security program is a prerequisite to effective computer security. Unless computer equipment is physically secure, attempts to protect the system and data are futile.

Security measures include controlling access to computer facilities, controlling visitors within the facility, and planning for disaster recovery.

Control objectives for security include:

- control over access to the facility;
- control over access within the facility;
- magnetic tape/cartridge usage;
- an adequate equipment servicing program; and
- alarms and prevention equipment.

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

- controls over access into and within the Central Computer Facility (CCF) and the Harris facility;
- controls over badges, contractor badge procedures, admission and escorting of visitors, and policies for the return of badges from employees leaving the CCF;
- controls over tape movement in and out of the CCF tape library and key information and tape media stored off-site;
- tape management procedures, missing tape log, and Tape Management System reports;
- alarm devices and prevention equipment for fire and water hazards;
- separation of duties; and
- the status of 1999 Department security findings.

We reviewed security controls and noted the following:

Facility Security - The Central Computing Facility (CCF) is monitored 24 hours a day, 7 days a week, by security guards, surveillance cameras, proximity badge readers, and alarms. The 3rd 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. We identified 273 individuals that had been issued badges that allow access to the third floor. The Department should review and re-evaluate the badges issued and determine if access to secured areas can be reduced.

Visitor Access - Formal procedures exist for the issuance of badges and for granting visitors and guests access to the building. Different types of temporary badges can be issued to visitors and guests, depending on their access needs.

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.

Separation of Duties - We noted some overlapping duties between the tape media, tape library, print shop, and command center staff who are housed on the third floor of the CCF. The Department should review the lack of separation of duties on the third floor.

Tape Management - The Bureau 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 off-site storage locations below the Capitol Building and electronically to the Harris facility's computer room. The following specific concerns should be corrected:

- Department management should ensure the monthly user agency tape/cartridge billing for storage reconciles with the tape library's storage records.
- Responsibility for assigning agency prefix identifiers should be assigned to only one section in the Department to eliminate both tape library and billing staff assigning the prefixes.
- Tapes/cartridges should be stored within the fire protection boundaries of the tape library.
- Procedures for the electronic vaulting should be included in the Library Guide for the Harris Facility.

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; and
- active user and management participation in defining, developing, testing, and reviewing systems and programming activities.

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

- application systems development standards and methodology and meeting minutes of the Standards Committee;
- approval of updates to the methodology;
- project management tools and techniques;
- adherence to the methodology for new projects;
- 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;
- placing authorized programs into production;

- quality assurance function; and
- status of 1999 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 Department uses the ASD Methodology (Methodology) as its guide for new systems, maintenance, enhancements, ad hoc reports, and third-party software. The Methodology is also used as a guide for development of system and user manuals, user training, testing scripts, and post-implementation reviews. The Methodology was created in October 1998 and was most recently revised in March 2000. Additionally, staff use the ASD Standards and Documentation Requirements (Standards) as a supplement to the Methodology. The Standards were created in April 1993 and were last revised in July 1999. During our review, we noted provisions in the Standards did not always agree with the Methodology.

The Methodology outlines four systems development phases: Phase I, problem definition and systems planning; Phase II, design; Phase III, development and implementation; and Phase IV, post-implementation review. However, the Methodology does not require the four phases to be completed in sequence and it does not require each phase to be signed off as it is completed.

Project Management and Quality Assurance - Several tools were available to assist in tracking computer system projects, assigning resources, and scheduling time. The Service Request Registration System (SRRS) registers projects, assigns a unique Service Request (SR) number, and records the projects' status. We selected a sample of SRs and determined that all had a corresponding entry on the SRRS and on the Quality Assurance Project Tracking System (Tracking System). However, we noted that all project information had not been updated on the Tracking System and when a project had been delayed, postponed, or its priority changed, no comment was added to either the SRRS or the Tracking System.

Testing - The Methodology states that all aspects of system development are to be thoroughly tested, reviewed, and implemented. We reviewed several test plans, and noted that they were completed in compliance with the Methodology.

Controls over the Production Library - Program Library Procedures exist to maintain program library security. Library Control staff control all movement of programs to a production library. We reviewed multiple production programs and determined Move Request forms existed for all selected and determined they were properly authorized. However, we found that neither the December 1999 nor January 2000 Library Move Authorization List was a complete list of the managers authorized to move programs to production.

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. We reviewed a new development project's documentation and determined that all documentation required for the system was completed in compliance with the Methodology. We also noted that the Project Manager's signature on the Project Sign-Off Form was the same date for all four development phases.

Post-Implementation Review - The Methodology provides guidance for performing a post-implementation review and states the review is to be conducted within six months after system testing and implementation have been completed. If a review is required, the Methodology states that a user representative, Quality Assurance staff, and Internal Audit staff must participate in the review, which is to be conducted within six months of the project's implementation. 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 system development methodology. We determined from our testing that Internal Audit staff did not participate in two required post-implementation reviews.

The Department has taken steps to strengthen its system development process and controls. Although significant weaknesses were not identified, we recommend the Department:

- Ensure the Methodology, Standards, Service Request Registration System, Quality Assurance Procedures Manual, and Quality Assurance Project Tracking System be synchronized, use consistent naming conventions, and reflect the current environment.
- Require that system development phases be completed in sequence. Each phase should be approved before the next phase is begun.
- Identify projects that are significantly behind their desired completion date and ensure the tracking systems record project delays.
- Ensure the accuracy of the data in the tracking systems.
- Ensure post-implementation reviews are performed in accordance with the Methodology.

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 changes;
- securing dial-up lines' access to computer resources;
- analyzing response time, detecting problems, and documenting problem resolutions; and
- selecting available telecommunication security options.

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

- security controls which prevent unauthorized access to the telecommunication software and dial-up lines;
- procedures for logging telecommunication problems and authorizing telecommunication changes;
- documentation of the telecommunication network and attached networks;
- procedures for securing the Department's Internet connection;
- Telecommunication Data Service Request Forms; and
- the status of 1999 Department telecommunication findings.

We reviewed telecommunication controls and noted the following:

Dial-up - The Department has two systems for securing access to telecommunications software and protecting dial-up lines from unauthorized access: the ACE direct dial system, and the Blockade token- based system.

Network Documentation - The Department maintains four communication network diagrams: the Central Computer Facility, the transmission control protocol/internet protocol (TCP/IP) network, the Department's Internet network, and the Department's local and wide-area networks.

Local Area Network Security - The Department maintains and supports local area networks (LANs) for the Department as well as the Governor's and Lieutenant Governor's Offices. In addition, the Bureau provides LAN connections for e-mail purposes to 11 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 on September 8, 1996. In December 1996 the Department issued the DCMS Statewide Internet Information Security Policy (Internet Security Policy) that must be followed when there is a flow of information between the Internet and the Department's protected environment, the mainframe. In June 1998 the Department approved a comprehensive Information Technology (IT) Security Policy which governs all the Department's computer resources, including Internet resources.

The Department has implemented two firewalls to protect the State's Internet connection.

With the continued reliance State agencies place on the Department's Internet service, we recommend the Department give immediate attention to correcting known web server vulnerabilities and to strengthening Internet security. In addition, the administrators for Internet Security, Internet Services, and the Internet Web Server should work together to periodically review and evaluate Internet security and coordinate and implement changes needed to prevent vulnerabilities.

We recommend the Department assess the security of its Internet environment and enforce its Security Policy. In addition, the Department should:

- Strengthen the review and approval process for dedicated Internet connections.
- Review the security requirements for agencies with or requesting dedicated connections and require agencies to employ a firewall or equivalent defense.
- Store firewall backup tapes in an environment with limited and controlled access.
- Evaluate the amount and types of resources dedicated toward the administration, testing, and security of the Department's firewall environment.
- Develop and maintain firewall administration documentation, procedures, and policies.
- Monitor State agency Internet addresses to identify those agencies that have not obtained their Internet service from the Department and thus pose a potential threat to the protected environment, the mainframe.
- 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.
- Obtain the services of an expert to assess the Department's Internet security.

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, CICS; and
- using the security features of RACF effectively.

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 features of RACF, CICS, and DB2;
- policies pertaining to protection of data and resources, restriction of access to production data, and review and timely revocation of access;
- procedures to monitor the use of high risk utilities and access privileges of NetView Ids; and
- the status of 1999 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 Central Computer Facility (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 for MVS.

Although security over MVS was reasonably well instituted, the Department should review the authorities assigned to consoles located outside the CCF to ensure they are appropriate. In addition, management should ensure consoles are located in physically secure areas.

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.

In the VM system, the emphasis is on flexibility and user-friendliness. Users with varying degrees of expertise use VM's two main applications: the electronic mail application, which allows messages to be distributed among several State agencies, and NOMAD, which is a data base management system.

Our review of the VM operating system's control objectives included formally confirming the status of VM controls, 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.

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 consider implementing the File Resource Security and Program Resource Security features.

Security Over Utility Programs - High-risk utilities are generally considered to be software utilities or programs that can be used to circumvent system security. System programming and operations staff primarily use utilities that are available within the current operating systems. The Department should periodically review user Ids and groups with access to high-risk utilities and NetView, ensure they are properly assigned, and allow access based on a user's need.

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 MVS and VM 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 1999 BCCS Third Party Review.

The Ids used by the computer operators provide access to functional areas and are shared by all of the operators. Although a specific user Id and password are used to gain access to each functional area, the Ids being shared by all the operators provide no individual accountability for actions taken. We also found that powerful system programmer Ids were occasionally shared if problems occurred during the night or on weekends.

Although RACF was reasonably well instituted, the Department should:

- Store MVS passwords using the federal government standard for encryption rather than scrambled text.
- Ensure that all Ids are immediately revoked or re-assigned and the password changed upon an employee's termination of employment.
- 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.
- Limit the sharing of powerful user Ids and passwords to extenuating circumstances to preserve the security environment. A policy or procedure should be developed to require system programmers to change their password as soon as possible after sharing it with an operator. If situations are severe enough to require that computer operators perform system software functions, this information should be forwarded to the CCF Security Administrator.
- Increase the minimum password length and require the use of special characters in passwords.

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.

ACCOUNTING INFORMATION SYSTEM

The Accounting Information System (AIS), implemented in 1995, is an online and batch system used to process expenditures, obligations, transfers, and vendor invoices and it includes the production of vouchers and schedules. AIS tracks expenditures from the initial receipt of the invoice through vouchering and posting. AIS also interfaces with other applications maintained by the Department, in addition to the Illinois Office of the State Comptroller's Statewide Accounting Management System (SAMS). AIS is currently utilized by 56 entities (see user list on page 41) .

During our review, we noted that the list of users identified by the Department's AIS staff did not reconcile with the list of users being billed through the Department's Billing System. The Department should ensure AIS staff regularly reconcile their system user list with the billing list and notify billing staff of any discrepancies.

Transactions entered into AIS are primarily entered online in a real-time environment. However, the system does offer the ability to batch transactions for processing at a later time. All data entered into the system is entered by the user agency and is the responsibility of the agency. To assist in ensuring the data entered has integrity and is accurate, AIS has edit checks designed into the system which alert a user to input errors. The errors must be corrected online before the user can continue entering data into the system. AIS provides supervisor override capability on some functions. Access to this feature is controlled by the AIS Security Module, in which user agencies define security parameters and identify the staff authorized to override specific functions. AIS also provides several online and batch reports, as indicated in the AIS Reports Manual, that can be used for reconciliation purposes. AIS reports are generated after transactions are processed and are distributed based on printer identification. Users, via the AIS Security Record database, control security over printed reports. During our review we selected one agency's AIS data and tested for proper input, edits, and century issues; no significant issues were identified.

Access to AIS is controlled using Resource Access Control Facility (RACF), in addition to AIS' internal security. Users must have a RACF user Id and password to gain access to the operating environment. Once access to the operating environment has been allowed, users must have a separate application user Id and password to gain access to AIS. AIS application security is used to enforce two approval levels, bureau and accounting, and to determine which level the user is assigned. Bureau level users are the primary staff responsible for entering accounting transactions into the system; accounting level users are responsible for approving accounting transactions. We reviewed the RACF groups with access authorities to the AIS production libraries, noting 286 Ids have access. AIS is automatically backed up daily, weekly, and monthly. The daily and weekly backups are stored in the CCF tape library; the monthly backups are rotated to the CCF's off-site storage location. We reviewed a listing of AIS backups that were to be located at the off-site location; however, we determined that 79 of 350 (23%) backups were not at the location reported by the Tape Management System. We selected a sample of 15 of the 79 tapes and determined they were located in the tape carousels at the CCF. The Department should ensure that the appropriate backup tapes are stored off-site.

No significant changes have been made to AIS since June 30, 1999. However, additional interfaces and the development of history and help screens are in progress. During the prior year, the system was modified to enable it to process Year 2000 dates, tested on the Department’s Year 2000 compliant system, and certified Year 2000 compatible.

To ensure controls are fully implemented and functional, internal and external auditors performing compliance audits of agencies using the AIS should:

- Ensure that agency personnel are using the available security mechanisms to control access to their data.

- Regularly review the RACF user profiles and user groups with access to AIS to ensure access authorized is appropriate.

- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.

- Verify that only accurate and authorized accounting data are entered into AIS. It is the agencies’ responsibility to ensure that only properly authorized transactions are entered into the system.

- Ensure the correct agency name is used.

- Review the billing statement to ensure the charges are proper.

Department records listed the following user entities that were billed for use of the Accounting Information System.

1. Administrative Offices of the Illinois Courts
2. Board of Higher Education
3. Bureau of the Budget
4. Capital Development Board
5. Department of Agriculture
6. Department of Central Management Services
7. Department of Commerce and Community Affairs
8. Department of Corrections
9. Department of Corrections – Correctional Industries
10. Department of Financial Institutions
11. Department of Human Rights
12. Department of Human Services
13. Department of Insurance
14. Department of Labor
15. Department of Lottery
16. Department of Military Affairs
17. Department of Natural Resources
18. Department of Professional Regulation
19. Department of Public Health
20. Department of Veteran's Affairs
21. Department on Aging
22. Emergency Management Agency
23. Environmental Protection Agency
24. General Assembly Retirement System
25. Guardianship and Advocacy Commission
26. Historic Preservation Agency
27. Human Rights Commission
28. Illinois Arts Council
29. Illinois Community College Board
30. Illinois Criminal Justice Information Authority
31. Illinois Deaf and Hard of Hearing Commission
32. Illinois Educational Labor Relations Board
33. Illinois Health Care Cost Containment Council
34. Illinois Industrial Commission
35. Illinois Law Enforcement Training and Standards Board
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. Pollution Control Board
47. Prairie State 2000 Authority
48. Prisoner Review Board
49. Property Tax Appeal Board
50. State and Local Labor Relations Board
51. State Board of Elections
52. State Employees' Retirement System
53. State Fire Marshal
54. State Geological Survey
55. State Police Merit Board
56. State's Attorneys Appellate Prosecutor

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 State Comptroller for the production of the agencies' payroll warrants.

There have been no significant changes made to the CPS since June 30, 1999. The system was modified to enable it to process Year 2000 dates, tested on the Department's Year 2000 compliant system, and certified Year 2000 compatible.

The CPS is currently utilized by 85 entities (see user list on page 45). The CPS users can enter data online or they can request their data be entered by DCMS personnel. It is the goal of the Department to have all agencies enter their data online and currently 80 user agencies do enter their data online.

During our review, we noted that the list of users identified by the Department's CPS staff did not reconcile with the list of users being billed through the Department's Billing System. The Department should ensure CPS staff regularly reconcile their system user list with the billing list and notify billing staff of any discrepancies.

State agencies using the CPS are charged monthly for the number of warrants issued in the agency's regular payroll plus a supplemental charge for warrants processed outside the regular payroll. During our review of the billing cycle we determined the approved rate increase, effective July 1999, had not been charged. Billing management stated it was an oversight that the rate increase had not been input into the CPS. The CPS generates the amount to bill user entities. The Department should ensure that approved changes to billing rates are updated in CPS.

To gain access to the operating environment, CPS users must have a RACF user Id and password. Users must also have a different application user Id and password to access the system. We reviewed the Department's RACF groups with access authorities to the CPS production libraries, noting 26 Ids have access. The Department should review programmer access rights.

The CPS has online edit checks, which prevent a user from entering a transaction with incomplete 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 for proper input, edits, and compliance with Year 2000; no significant weakness were identified. We determined that the data was entered properly and complied with Year 2000 standards.

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

To ensure that controls are fully implemented and functional, internal and external auditors performing compliance audits at agencies using the Central Payroll System should:

- Review critical manual controls. Auditors should verify that agency personnel review voucher schedules prepared by the system to ensure the schedules are correct.

- Verify the accuracy of gross pay and trace all deductions to properly signed authorizations.

- Ensure that agency personnel are using the available security mechanisms to control access to their data.

- Verify that only accurate and authorized data are entered into the CPS. It is the agencies' responsibility to ensure that only properly authorized transactions are entered into the system. The input of inaccurate or unauthorized data may result in the production of incorrect or unearned payroll warrants.

- Review the appropriateness of user access rights to production files to ensure access is limited to those with a need to know and that the access level is appropriate.

- Regularly review the RACF user profiles and user groups with access to CPS to ensure access authorized is appropriate.

- Review the billing statement to ensure the charges are proper.

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, City of *
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 Math and Science Academy
47. Illinois Planning Council on Developmental Disabilities
48. Illinois Racing Board
49. Illinois Rural Bond Bank
50. Illinois State Board of Investment *
51. Illinois State Police
52. Illinois Student Assistance Commission
53. Joint Committee on Administrative Rules
54. Judges' Retirement System
55. Judicial Inquiry Board *
56. Legislative Audit Commission
57. Legislative Information System
58. Legislative Printing Unit *
59. Legislative Reference Bureau
60. Legislative Research Unit
61. Legislative Space Needs Commission
62. Illinois Liquor Control 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 State Appellate Defender
70. Office of the State Fire Marshal
71. Office of the Treasurer
72. Pension Laws Commission
73. Pollution Control Board
74. Prairie State 2000 Authority
75. Prisoner Review Board
73. Property Tax Appeal Board
77. State's Attorneys Appellate Prosecutor
78. Secretary of State
79 State and Local Labor Relations Board
80. State Board of Education
81. State Board of Elections
82. State Employees’ Retirement System
83. State Police Merit Board
84. State Universities' Civil Service System
85. Teachers’ Retirement System of the State of Illinois

* Entity’s data is entered by DCMS.

CENTRAL INVENTORY SYSTEM

The Central Inventory System (CIS), implemented in October 1985, 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 officials stated the system provides the ability to process batched transaction files; however, this capability is restricted to the Department's CIS staff for use in assisting agencies in rare instances when an agency has a special project and must enter an enormous number of transactions.

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. Although users must request these reports online, the request is batched for processing at a later time. The CIS is currently utilized by 31 entities (see user list on page 49).

In 1998, the Department developed a new Central Inventory System (CIS) and all users were migrated to the new system by August 1999. The new system was tested on the Department's Year 2000 compliant system and certified Year 2000 compatible. The new CIS provides the same processing capabilities as the old system with the addition of four new screens (Voucher Maintenance, Voucher List, Responsibility Maintenance, and Responsibility List). Department officials stated they are currently restricting the use of the Depreciation Process to CMS' Accounting Division; however, it is expected that this feature will be provided later to agency users.

During our review, we noted that the list of users identified by the Department's CIS staff did not reconcile with the list of users being billed through the Department's Billing System. The Department should ensure CIS staff regularly reconcile their system user list with the billing list and notify billing staff of any discrepancies.

CIS users must have a RACF user Id and password to gain access to the system. In addition, the CIS requires a separate application user Id and password to provide additional security over accessing the CIS. We reviewed the RACF groups with access authorities to the CIS production libraries, noting 73 Ids have access.

CIS is automatically backed up nightly, for use in recovering from a system failure; the backups are to be rotated to the off-site storage location. However, we reviewed a listing of CIS backups the Tape Management System reported were to be located at the off-site location and observed that none of the 133 backup tapes were there. We selected a sample of 15 of 133 tapes and determined they were located in the tape carousels at the CCF. In addition to the nightly backups, the Department maintains transaction history files for six months prior to archiving the data. Once archived, the transaction history files are maintained for another two and a half years. During our review, we determined that written backup and recovery procedures did not exist; CIS management stated that backups are created automatically, and rollback is used for recovery. The Department should develop recovery procedures and ensure that the appropriate backup tapes are stored off-site.

During our review, we selected two agencies' CIS data and tested for proper input, edits, and compliance with Year 2000. We did not identify any duplicate property tags or incorrect billing; however, we identified some date-related issues with optional fields such as depreciation, inventory date, and addition date.

Although the CIS provides reasonable assurance of accuracy and security, many controls are the responsibility of system users. Internal and external auditors should:

- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.

- Ensure that agency personnel are using the available security mechanisms to control access authority to their data.

- Regularly review the RACF user profiles and user groups with access to CIS to ensure access authorized is appropriate.

- Review their BCCS Utilization Billing Reports to determine if they are appropriately billed for CIS. If the agency determines they are being billed for old CIS data and no longer need access to the CIS, they should notify the Department to request the old data and access to the system be removed.

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 Commerce and Community Affairs
7. Department of Employment Security
8. Department of Human Rights
9. Department of Human Services
10. Department of Lottery
11. Department of Military Affairs
12. Department of Natural Resources
13. Department of Nuclear Safety
14. Department of Professional Regulation
15. Department of Public Health
16. Department of Transportation
17. Department of Veterans' Affairs
18. Department on Aging
19. Emergency Management Agency
20. Environmental Protection Agency
21. Historic Preservation Agency
22. Illinois Deaf and Hard of Hearing Commission
23. Illinois Industrial Commission
24. Illinois Law Enforcement Training and Standards Board
25. Illinois Racing Board
26. Illinois Student Assistance Commission
27. Office of Banks and Real Estate
28. Office of the Attorney General
29. Office of the Governor
30. Office of the Lieutenant Governor
31. State's Attorneys Appellate Prosecutor

CENTRAL TIME AND ATTENDANCE SYSTEM

The Central Time and Attendance System (CTAS) was developed by the Department and is currently utilized by 29 entities to provide a comprehensive system for recording and managing employee benefit time (see user list on page 53). During our review, we noted that the list of users identified by the Department's CTAS staff did not reconcile with the list of users being billed through the Department's Billing System.

CTAS users must have a RACF user Id and password to gain access to the system. In addition, a separate CTAS user Id and password are required to access the system. We reviewed the Department's RACF groups with access to the CTAS production libraries, noting 82 Ids have access.

CTAS data is automatically backed up daily and weekly. Daily backups are maintained at the Central Computer Facility (CCF). Five generations of backup are kept, four in the vault and one at the CCF. Backups are rotated to off-site storage weekly. We observed that CTAS backup tapes are rotated and maintained off-site. In addition, backup and recovery procedures are available. However, we determined that step-by-step procedures for the restoration of the system did not exist.

No significant changes were made to CTAS during FY 2000. However, additional screens and minor modifications to the system were implemented. During the prior year, the system was modified to enable it to process Year 2000 dates, tested on the Department's Year 2000 compliant system, and certified Year 2000 compatible.

During our review, we selected two agency's CTAS data and tested date fields, vacation balances, and the employee identification field for proper input, existence of edits, and compliance with Year 2000 date fields. No significant weaknesses were identified and we determined data was entered properly and complied with Year 2000 standards.

To ensure controls are fully implemented and functional, internal and external auditors performing compliance audits of agencies using the CTAS should:

- Ensure that agency personnel are using the available security mechanisms to control access to their data.

- Verify that only accurate and authorized timekeeping data are entered into CTAS. It is the agencies' responsibility to ensure that only properly authorized time and attendance records 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. Auditors should verify that agency personnel review timekeeping reports prepared by the system to ensure the reports are correct.

- Regularly review the RACF profiles and user groups with access to ensure access authorized is appropriate.

- Review billing statements to ensure the charges are accurate.

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 Public Health
12. Department of Revenue
13. Department of Veterans' Affairs
14. Emergency Management Agency
15. Environmental Protection Agency
16. Guardianship and Advocacy Commission
17. Human Rights Commission
18. Illinois Criminal Justice Information Authority
19. Illinois Deaf and Hard of Hearing Commission
20. Illinois Education Labor Relations Board
21. Illinois Health Care Cost Containment Council
22 Illinois Industrial Commission
23. Illinois Law Enforcement Training and Standards Board
24. Illinois Planning Council on Developmental Disabilities
25 Office of Banks and Real Estate
26. Office of the Attorney General
27. Office of the Governor
28. Property Tax Appeal Board
29. State Fire Marshal

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:

- Participate in the Department's annual disaster recovery test if they have a Category 1 application;
- Conduct disaster recovery tests of all critical applications;
- Continue to develop and update their disaster contingency plans to ensure the plans meet their current disaster recovery needs and submit their plans to the Department;
- Review and prioritize their critical applications and forward the updated list, with supplementary explanations and telecommunication restoration requirements, to the Department;
- Comply with the Department's recovery requirements, including forwarding critical recovery information to the Department (i.e., updated list of critical applications, thoroughly completed disaster recovery testing forms, and summary memos of testing performed);
- Ensure that critical data is backed up and stored off site.

2. Available security mechanisms should be used.

We recommend that **all** users use the security software package Resource Access Control Facility (RACF) to protect their data and prohibit the sharing of user Ids and passwords. We recommend that user agencies:

- Utilize the capabilities of RACF;
- Formally designate a security coordinator who is segregated from computer operations;
- Review the RACF violation file weekly to monitor attempted accesses to their data;
- Fully utilize the security services, policies, and guidelines offered by the Department;
- Perform periodic reviews of existing RACF profiles to ensure that access rights are appropriate and limited to those with a need to access the information, including ensuring that the universal access authority assigned to catalogs is appropriate.

3. **Security over Internet use should be reviewed**.

   User agencies are responsible for protecting the computer information resident at their location; therefore, each agency should evaluate the security over their Internet connection. Agencies should comply with the Department's Security Policy and ensure that their Internet use is not placing their internal data, or other agencies' data residing on the mainframe's protected environment, at risk. Therefore, agencies should ensure their connection configurations have been reviewed and approved by the Department.

   - Agencies should install virus detection software and assess their environment to determine whether additional security measures, such as virus detection and encryption, should be installed.
   - For agencies that are using Windows NT as their server, they should ensure that the Remote Access Server (RAS) is set to "disabled".

4. **Security of VM systems should be reviewed.**

   User agencies should review VM inactive user reports, determine Id status, and notify VM support staff of necessary changes. User agencies should review the use of multi-write capabilities (through granting "alter" authority) and have it eliminated from all minidisks where it is not absolutely essential.

5. **Control over submitting for telecommunication equipment should be reviewed.**

   User agencies should submit TGRs (terminal generation requests) and TDRs (telecommunication data service requests) to the Department at the same time to reduce the likelihood of equipment failures, billing discrepancies, and implementation delays.

6. **Bills for computer services should be reviewed.**

   User agencies should become familiar with the details of the SSRF (Statistical Services Revolving Fund) and CRF (Communications Revolving Fund) billings to ensure that they are being billed accurately for services utilized. User agencies should also review the name and address on all billing and accounts receivable documents to ensure they are accurate and consistent.

7. **Common Systems use should be reviewed.**

   Management and auditors of agencies that use the Central Payroll, Central Inventory, Central Time and Attendance, or Accounting Information Systems should review the application control memorandums on pages 37 through 53 of this document. Although no significant deficiencies were noted, management, and internal and external auditors should perform the tasks outlined in the application memorandums.

8. **The accuracy of agency security lists should be reviewed.**

   Upon receipt of the security lists, user agencies should verify the lists, make any necessary changes, and return them in a timely manner. Prompt notification ensures the security authorization lists remain accurate, complete, and timely.

9. **Subsystem security should be reviewed.**

   User agencies that have MVS consoles in their facilities should ensure the consoles are physically secure. In addition, agencies using CICS should ensure they appropriately RACF protect their load libraries within their CICS region and distinguish between test and production CICS regions; exercise caution in granting individuals both system administrator and developer permissions; invoke the automatic sign-off feature; and ensure the CICS master terminals are in a secure location.

APPENDIX B
LIST OF USER AGENCIES

1. Administrative Office of the Illinois Courts
2. Board of Higher Education
3. Bureau of the Budget
4. Capital Development Board
5. Chicago State University
6. Civil Service Commission
7. Comprehensive Health Insurance Plan
8. Court of Claims
9. Department of Agriculture
10. Department of Central Management Services
11. Department of Children and Family Services
12. Department of Commerce and Community Affairs
13. Department of Corrections
14. Department of Employment Security
15. Department of Financial Institutions
16. Department of Human Rights
17. Department of Human Services
18. Department of Insurance
19. Department of Labor
20. Department of Lottery
21. Department of Military Affairs
22. Department of Natural Resources
23. Department of Nuclear Safety
24. Department of Professional Regulation
25. Department of Public Aid
26. Department of Public Health
27. Department of Revenue
28. Department of Transportation
29. Department of Veterans' Affairs
30. Department on Aging
31. East St. Louis Financial Advisory Authority
32. Eastern Illinois University
33. Economic and Fiscal Commission
34. Emergency Management Agency
35. Environmental Protection Agency
36. General Assembly (Senate Operations)
37. General Assembly Retirement System
38. Governors State University
39. Guardianship and Advocacy Commission
40. Historic Preservation Agency
41. House of Representatives
42. House Republican Staff
43. Human Rights Commission
44. Illinois Arts Council
45. Illinois Commerce Commission
46. Illinois Commission on Intergovernmental Cooperation
47. Illinois Community College Board
48. Illinois Criminal Justice Information Authority
49. Illinois Deaf and Hard of Hearing Commission
50. Illinois Development Finance Authority
51. Illinois Educational Labor Relations Board
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 State Board of Investment
62. Illinois State Police
63. Illinois State Toll Highway Authority
64. Illinois State University
65. Illinois Student Assistance Commission
66. Joint Committee on Administrative Rules
67. Judges Retirement System
68. Judicial Inquiry Board
69. Legislative Audit Commission
70. Legislative Information System
71. Legislative Printing Unit
72. Legislative Reference Bureau
73. Legislative Research Unit
74. Legislative Space Needs Commission
75. Medical District Commission
76. Northeastern Illinois University
77. Northern Illinois University
78. Office of Banks and Real Estate
79. Office of the Attorney General
80. Office of the Auditor General
81. Office of the Comptroller
82. Office of the Governor
83. Office of the Lieutenant Governor
84. Office of the State Appellate Defender
85. Office of the Treasurer
86. Pension Laws Commission
87. Pollution Control Board
88. Prairie State 2000 Authority
89. Prisoner Review Board
90. Property Tax Appeal Board
91. Secretary of State
92. Southern Illinois University
93. State and Local Labor Relations Board
94. State Board of Education
95. State Board of Elections
96. State Employees’ Retirement System
97. State Fire Marshal
98. State Police Merit Board
99. State Universities Civil Service System
100. State Universities Retirement System
101. State’s Attorneys Appellate Prosecutor
102. Teachers’ Retirement System of the State of Illinois
103. University of Illinois
104. Western Illinois University