REPORT DIGEST

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES BUREAU OF COMMUNICATION AND COMPUTER SERVICES

THIRD PARTY REVIEW
For the Year Ended:
June 30, 2001

Release Date:
July 2, 2001

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 106 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 16 to April 27, 2001. 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

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

STATISTICS	2001
Mainframes	4 Units Configured as 14 Systems
Services/Workload	73,259 Nodes Statewide (Terminals, Printers, etc.) 72 Million IMS Transactions per Month 1.6 Million Feet of Laser Printing per Month 232,828 Reel/Cartridge Tape Mounts per Month
State Agency Users	106
CCF Employees	1998 -- 125 1999 -- 131 2000 -- 136 (includes 8 vacancies) 2001 -- 138 (includes 13 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 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 2001 -- 135,758 -- 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

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 recommendation and stated that during the week of May 7, 2001, the Department conducted the annual comprehensive recovery exercise.

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 2001

TABLE OF CONTENTS

REPORT ON THIRD PARTY REVIEW
JULY 2001

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 27, 2001. Our review, started in the summer of 2000 and primarily performed between January 16 and April 27, 2001, 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 27, 2001. 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 16 to April 27, 2001. 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 16 to April 27, 2001. 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 27, 2001, and information about tests of the operating effectiveness of specified controls covers the period from January 16 to April 27, 2001. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specified controls at the Department is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

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

_____

William J. Sampias, CISA
Director, Information Systems Audits

April 27, 2001

THIRD PARTY REVIEW

Department of Central Management Services
Bureau of Communication and
Computer Services

July 2001

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 106 user agencies (see Appendix B).

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

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

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

Accounting Information System;

Central Payroll System;

Central Inventory System; and

Central Time and Attendance System.

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

Control Deficiencies

We identified several control deficiencies that appear in pages 7 through 55. One of these issues warrants additional emphasis.

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 (plans, equipment, and facilities) are available to provide for continuation of critical computer operations in the event of a disaster. In addition, the Department should review contingency plans, conduct comprehensive tests of the plans on an annual basis, and continue efforts with vendors to assess and revise contingency plans (see page 13).

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

Department Response

During the week of May 7, 2001, the Department conducted the annual comprehensive recovery exercise involving all Category One Critical agencies, CMS Network Control Center and CMS LAN. All participants were successful in achieving the desired results for each recovery task.

The exercise was conducted in four phases and involved scenarios ranging from procedural walk-through to complete recovery of the application and data.

It is CMS's intent to continue to diligently pursue providing continuity recovery services.

The Department response was provided on May 30, 2001, 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; and
- ensuring sufficient and effective Internal Audit activities;

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

- segregation of duties, job descriptions, and staffing levels;
- training requirements, records, and documentation;
- Internal Audit's participation in the development or modification of computer systems and the two-year audit plan;
- 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, procedures for processing credit requests, and accuracy of user lists; and
- the status of 2000 Department administration findings.

We reviewed administration controls and noted the following:

Software Licenses - The Department has 11 enterprise licensing agreements with software vendors at an annual cost of approximately $10 million.

Staffing shortages - The command center operates 24 hours a day, 7 days a week, 365 days a year. Each of the four shifts (two per day) were designed for four operators and one supervisor, with each operator working a 12-hour shift. The Department is using voluntary overtime to compensate for staffing shortages in the command center; however, the voluntary overtime is failing to adequately compensate for the staffing shortages. The Department should develop a strategy to alleviate the shortage of computer operators and ensure that each shift is properly staffed.

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 Audit Division is mandated to perform reviews of system developments and major modifications to existing systems, Internal Audit should reconsider their process for identifying system development projects that meet the criteria for a statutorily required review. In addition, Internal Audit should analyze current staffing and determine if the number of staff is sufficient to meet statutory requirements and the audit needs of the Department. New initiatives such as Public Key Infrastructure (PKI), Web-enablement, electronic mail, and a myriad of other technology-related projects increase the need for an independent review to ensure that all risks and security issues have been adequately addressed.

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

The Department reported that from July 1, 2000, through March 31, 2001, $46.5 million and $84.3 million were billed from the SSRF and CRF respectively. As of December 2000 the Department reported the outstanding accounts receivable total was $7.5 million and $20.5 million for the SSRF and CRF respectively.

The Department should be commended for its efforts to correct many of the billing issues identified in the 2000 BCCS Third Party Review. The Department has increased the automation in the billing process which has decreased the time for producing the monthly billings from 12 days to 2 days.

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

- Develop procedures to ensure that Billing staff are notified of new or deleted users of the common systems.
- Ensure that all information entered into the credit logs corresponds to the original request, or maintain appropriate documentation to support the reason for any differences.
- Consider developing an acceptable mechanism for collecting past due accounts.

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 backup procedures, backup strategy, and verification of usability of backups;
- storage of key information, programs, and documentation in a secure, off-site location;
- restart and recovery procedures; and
- the status of 2000 Department contingency planning findings.

We reviewed contingency planning controls and noted the following:

Contingency Planning - The Department is mandated to provide computing services to over 100 State agencies that depend on a continuation of computing services in order to fulfill their duties, missions, and goals. A contingency plan is essential for an organization to minimize service 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, off-site storage of backups, designation of an alternate processing facility, and availability of a backup power supply.

Contingency Plans - The Department has established three disaster recovery plans: the DCMS/BCCS/ISD Disaster Recovery Plan, the Network Control Center (NCC) Disaster Recovery Plan, and the Local Area Network (LAN) Disaster Recovery Plan. The DCMS/BCCS/ISD Disaster Recovery Plan, dated March 2000, is for the recovery of the Department's Central Computer Facility (CCF). The NCC Plan, dated February 1996, is for the recovery of the Department's Network Control Center, Internet and telecommunication services. The LAN Plan, dated June 1997, is for recovery of the Department's Local Area Network. However, we determined that the three plans have not been reviewed or certified in the past year. Management stated that all three plans are currently under review by the contracted disaster recovery services vendors.

Disaster Recovery Testing - According to the DCMS/BCCS/ISD Disaster Recovery Plan, "the plan is to be tested periodically." The complexity of the testing may be classified into four different classes:

- class A-testing of recovery file for completeness and usability
- class B-testing of documentation in recovery file and use to restore
- class C-testing the capability to recover from loss of one facility
- class D-testing of recovery file and media stored in the off-site vault at the recovery center

However, the Department has not conducted testing in the past year. Management stated that a comprehensive test will be scheduled in the near future.

The LAN and NCC disaster recovery plans have not been tested in the last three audit periods.

Staffing - The Department has assigned a Disaster Recovery manager and coordinator to assist in ensuring the plans are updated, tested and reviewed continuously. In January 2001 the coordinator retired, and as of April 2001 a replacement had not been hired. Similar staff assignments have not been made for the LAN and NCC, and as a result, the plans have not been updated for four and five years, respectively.

Contracts - In December 1999 the Department entered into a two-year contract for disaster recovery services for the NCC and LAN. 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
- Department of Public Health

The contract states the vendor is to provide the Department and participating agencies with the following:

- an assessment of the current backup procedures
- an assessment of the disaster recovery plan
- a recovery site
- 24 hours of testing per year

The assessments have not been provided, testing has not been performed, and hardware requirements are outdated. In the event the Department would declare a disaster, the vendor would provide the recovery environment; however, any hardware required, but not listed in the original contract, would cost the State additional monies. Department management stated that the vendor is currently developing testing plans and scheduling testing times for the participating agencies; however, if a contract amendment is not finalized the testing will be cancelled.

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

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

As of April 2001, the vendor had provided drafts of all outlined deliverables and scheduled testing at its facility for September 2001.

Statewide Critical Application Listing - The Department maintains a Statewide Critical Application Listing based on information received from agencies annually. Each year all agencies are requested to review and update the information contained in the Statewide Disaster Recovery file. In the event a disaster would occur, only those applications listed in the Statewide Disaster Recovery file would be considered for recovery. The applications are given a priority number within each category.

Currently applications are prioritized in one of five categories:

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

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

Off-site Storage - The Department currently utilizes two off-site storage facilities: the Capitol vaults and the Harris facility. In addition, the Department has contracted with a distant off-site storage facility, which will be used to store critical information and data starting in May 2001.

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 25 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.

A service contract agreement, effective July 1, 2000 through June 30, 2001, has been established to provide routine preventive maintenance on the UPS components located at the CCF and the Harris facility.

Restart and Recovery - The Department's DP Guide provides procedures to staff for restarts and recoveries. Restart and recoveries may occur for various reasons other than a disaster: hardware failures, new maintenance levels, new software releases, and job failures. We noted all systems were available 99.71% of the time from July 2000 to March 2001.

Since the Department is mandated to provide computing services, it is imperative continuity services be available to minimize service disruption and fully restore operations in the event of a disaster. In order to minimize risks associated with a loss of service, the Department should:

- Ensure that adequate plans, facilities, and equipment are available to recover critical applications.
- Perform annual comprehensive tests of the Department's three disaster recovery plans.
- Continue to work with the disaster recovery vendors to update/rewrite the Department's three disaster recovery plans.
- Ensure the Department's disaster recovery plans reflect the current environment.
- Assign additional qualified individuals for the administration of disaster recovery services for the mainframe, LAN, and NCC.
- Annually evaluate the interagency agreements for the alternate sites.

COMPUTER OPERATIONS CONTROLS

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

Computer operations management must be aware of all facets of the operating environment and be able to control it. Department management must ensure that processing meets specifications, thereby making the review of operations a 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;
- 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:

- various logs and shift reports;
- hardware monitoring and problem handling;
- problem management reports;
- systems software change control procedures;
- procedures for testing and approving system software changes;

- emergency change procedures;
- controls to prevent unauthorized changes to the systems; and
- the status of 2000 Department computer operations findings.

We reviewed computer operations controls and noted the following:

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

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

Change Control - The Department has recently implemented a new Problem/Change Management System. The new System has completely automated the process for change management and improved the controls over change management.

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

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

In addition, the Problem/Change Management System procedures are documented in the "CMS Information Management System" manual.

The Problem/Change Management System stores information regarding the creation, approval, testing, scheduling, and implementation of change requests online. The Department has the capability to run routine and special reports to track change management activities. The Department plans to maintain two years of documentation online, and after two years the information will be archived to tape.

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

The Department does not have formal procedures relating to emergency change requests. However, management stated that emergency change procedures are in draft form and are expected to be finalized in the near future. We recommend the Department finalize and implement the emergency change procedures as soon as possible.

SECURITY CONTROLS

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

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

Control objectives for security include:

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

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

- controls over access into and within the Central Computer Facility (CCF), Communications center, 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;

- janitorial services contract;

- alarm devices and prevention equipment for fire and water hazards;

- security policies and procedures and awareness program;

- security management structure, roles, and responsibilities; and

- the status of 2000 Department security findings.

We reviewed security controls and noted the following:

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 Central Computer Facility (CCF) Security Administrator, the Local Area Network (LAN) Administrator, and the Internet Security Administrator report to the Security Officer for security-related issues. The Security Officer reports directly to the Bureau Manager.

We were unable to identify any significant activity regarding the development or modification of security policies, or promotion of security awareness in the past year.

A comprehensive Information Technology Policy (IT Policy) (dated June 1, 1998) exists, and all other IT security policies are subordinate to the IT Policy. Other Department 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)
- Network Software Guide (dated January 29, 1999)

The Department should review and update the security policies on an annual basis, and consider consolidating the policies into one comprehensive policy.

Twice every year, the Department distributes the Security Authorization List and the Tape, Print, and Diskette List to user agencies, which are to be updated and returned to the Department within two weeks. During our review, we determined that 26 of 86 agencies did not return their Security Authorization Lists, and 19 of 68 agencies did not return their Tape, Print, and Diskette Lists. In addition, 2 agencies had staff included on the lists, but did not appear on the distribution list. The Department should update the distribution list and ensure that responses are received from all agencies.

Department staff are required to sign a Statement of Understanding acknowledging receipt of Department Policies, including the IT Policy, and agreeing that it is their responsibility to read and act in accordance with the Policies. However, we determined that 4 of 6 new employees tested did not have a signed Statement of Understanding in their file.

As computers become more and more integrated into the delivery of State services, and contain critical and confidential information, security becomes even more essential. New initiatives such as Web-enablement and Public Key Infrastructure (PKI) introduce security concerns that must be continually, adequately, and globally addressed. In addition, since the Department functions as a computer service bureau used by more than 100 State agencies, there is an inherent leadership role regarding technology and security issues. Therefore, we strongly believe that an effective security administration function is critical to the overall security and integrity of the State's computing environment. Specifically, the Department should:

- Ensure that the DCMS Security Task Force meets on a regular basis, and effectively fulfills its objectives.
- Develop and institute a formal security awareness program to keep users informed, and aware of security issues.
- Require all employees to sign a Statement of Understanding to verify that they have read, understand, and agree to act in accordance with Department Policies.
- Ensure that adequate resources are allocated to security administration.

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

Visitor Access - Formal procedures exist for the issuance of badges and for granting visitors and guests access to the building. Different types of temporary badges can be issued to visitors and guests, depending on their access needs. Employees who forget their badge or visitors are required to sign-in and register with security guards to gain access to the facility; however, our testing identified over 86% of the entries on the registers sampled contained incomplete data.

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

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

Tape Management - The Department has formal tape procedures in place to control the movement of magnetic tapes to and from the CCF. In addition to agency tapes being rotated to the off-site storage location, CCF staff physically rotate operating system backups to its off-site storage locations below the Capitol Building and electronically to the Harris facility's computer room. In addition, the Department has contracted with a distant off-site storage facility, which will be used to store critical information and data. The Department should store media within the fire protection boundaries of the tape library and add the procedures for the electronic vaulting to the Library Guide.

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

- quality assurance function; and

- status of 2000 Department application systems development findings.

We reviewed application systems development controls and noted the following:

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

Standards, Methodology, and Procedures Manuals - The ASD Methodology (Methodology) (revised December 2000) and Standards and Documentation Requirements (revised April 2000) are the guides, developed in-house, for new system developments and modifications to existing systems, user manuals, the purchase of third party software, establishing user training, performing testing, and performing post-implementation reviews. During our review, we noted provisions in the Standards did not always agree with the Methodology; however, the Standards are being rewritten, with limited enforcement, until the rewrite is finalized.

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

The Methodology outlines four system development phases:

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

When the Methodology was developed in 1994, the Department established a Standards Committee for reviewing current development standards, proposing new or modified standards, and implementing changes to the Methodology. We reviewed Standards Committee minutes for the first six months of fiscal year 2001, and determined that the Committee met regularly, pertinent topics were discussed, and appropriate staff attended meetings regularly.

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

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

- Microsoft Project 98 for developing project plans
- Microsoft Project Manager for managing multiple projects
- Service Request Registration System (SRRS) for tracking system development or enhancement projects
- QA Project Tracking System for verification of ASD projects

User Participation and Testing - Per the Methodology, "user involvement is vital for system development to be successful. Users are to participate in each phase of system development and assist with defining the business rules and designing the system. Users are responsible for developing and executing system tests according to the business rules."

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

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

Post-Implementation Review - The Methodology provides guidance for performing a post-implementation review 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 and Quality Assurance staff must participate in the review. The purpose of a post-implementation review is to provide for a comprehensive review of the implemented project, to assure the project meets the user's needs and stated objectives, and adheres to the requirements of the system development methodology.

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

Controls over the Production Library - Program Library Procedures exist to maintain program library security. The Program Library Procedures state that Library Control is to maintain program library security and perform special assignments, when required. The procedures are designed to ensure that new programs and modification to existing programs are thoroughly documented and approved before production moves are performed. We reviewed 82 Move Requests and determined that all were properly approved.

We reviewed four systems development projects that were either started or completed during fiscal year 2001. The projects included the implementation of Electronic Data Interchange (EDI) in the Accounting Information System (AIS), a modification to the Business Enterprise System to provide an interface between small business and the Illinois Governmental Purchasing System, the Warehouse Control System, and the Web-enablement of AIS. The Web-enablement project did not comply with the system development standards and procedures. Although the other projects generally complied with procedures, we also found several instances of noncompliance with specific standards and procedures.

We recommend the Department increase its efforts to ensure compliance with system development standards and procedures. Compliance with standards and procedures will help ensure that projects are properly authorized, approved, tracked, controlled, tested and documented to promote consistent and thorough system development activities. In addition, we recommend that QA aggressively enforce compliance with the Methodology, Standards and procedures. We specifically recommend that QA not sign-off on a systems development phase until they have made certain that all required deliverables for the phase are completed in compliance with the Methodology, Standards and procedures.

TELECOMMUNICATION CONTROLS

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

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

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;
- analyzing security and controls of telecommunications, Internet, and Local Area Network (LAN) environments; and
- selecting available 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 diagnosing and logging telecommunication problems;
- documentation of the telecommunication network and attached networks;
- procedures for securing the Department's Internet and LAN connections;
- policies and procedures for the use of the Internet and LAN;
- Telecommunication Data Service Request and Terminal Generation Request Forms; and
- the status of 2000 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 communications network diagrams for the Central Computer Facility (CCF), including Transmission Control Protocol/Internet Protocol (TCP/IP) and Systems Network Architecture (SNA) networks. The Department also maintains Local and Wide Area Networks diagrams.

The network diagrams document the host-to-mainframe connections, network control program connections, State agency users, and the SNA network interconnects to both State and private sector data centers. The TCP/IP network diagram documents direct connections for State agency users, as well as connections via the frame relay network to the Department's Internet network.

Change Requests - Network changes are associated with telecommunications software, data communications equipment or facilities (circuits), and voice equipment. Each type of change requires a different request form. Data communications facilities and equipment changes require a user to submit a TDR (Telecommunications Data Service Request). A TGR (Terminal Generation Request) is used to request software changes. Each user agency has a designated person that is responsible for approving these forms.

Local Area Network Security - The Department maintains and supports local area networks (LANs) for the Department as well as the Governor's Office, Lieutenant Governor's Office, and the Department of Labor. In addition, the Department provides LAN connections for e-mail purposes to 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 in September 1996 and is protected by two firewalls.

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 purpose of the Statewide Information Security Policy "…is to establish appropriate security procedures a State agency must implement in order to be allowed to access the Internet through the Department". We determined that the Policy does not reflect the current environment. In addition, the Policy stated that "it is to be reviewed at least annually and updated where needed to accommodate advances in technology and organizational changes".

The Policy states that State agencies must acquire Internet access from the Department and all exceptions must be approved by the Department's Director. In addition, "connections to the State's Internet or the protected information environment will not be permitted until the agency's configuration has been reviewed and approved by the Department". The Department is currently utilizing a checklist/questionnaire and an illustration of the agency's environment for this review.

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

With the continued reliance State agencies place on the Department's Internet service, we recommend the Department implement controls to ensure the protected environment is adequately safeguarded from unauthorized access from sources external to State agencies, especially as the Department is moving forward with incorporating new technology. The Department should also increase the allocation of resources toward administering, testing, and securing the firewalls and Internet connection.

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 review and monitor security violations; and
- the status of 2000 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. No significant weaknesses were identified in our review of MVS.

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

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

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

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

DataBase 2 (DB2) - DB2 is a relational database management system for the MVS environment that the Department makes available to user agencies. No significant weaknesses were identified in our review of DB2.

Customer Information Control System (CICS) – CICS is a program product that enables transactions entered into remote terminals to be processed concurrently by user-written application programs. The Department supports CICS and makes it available to user agencies. No significant weaknesses were identified in our review of CICS; however, we recommend that the Department evaluate the current time-out setting to determine if the setting meets the control objectives for the Department.

Resource Access Control Facility (RACF) - The Department uses the RACF security system to control and monitor access to data maintained on its mainframe computers and other resources. RACF operates as an extension of, and an enhancement to, the basic MVS and VM operating systems. It provides a mechanism for controlling access and for monitoring secured computer resources.

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

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

During our review of RACF security, we reviewed DSMON reports, RACF parameters and security options selected on both the MVS and VM operating systems, and the status of the RACF issues identified in the 2000 BCCS Third Party Review.

Although RACF was reasonably well instituted, the Department should:

- Store passwords using the federal government standard for encryption rather than scrambled text.
- Ensure all RACF profiles clearly identify the person or device assigned to the RACF ID. As individual accountability is a primary security objective, the Department should, wherever possible, avoid the use of generically assigned IDs, unassigned IDs, and shared IDs. While there are cases where the use of such IDs is necessary, it should generally be prohibited unless absolutely necessary.
- Increase the minimum password length, require the use of special characters in passwords, and increase the password history limitation.
- Develop formal policies and procedures governing RACF administration and security.
- Assign the system-level AUDITOR attribute to an individual who is segregated from RACF administration.
- Increase efforts to review and monitor security issues, security parameters, and unauthorized access attempts.
- Ensure adequate responses to security violations are obtained, and that sufficient action is taken when unjustified security violations occur.

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) is an on-line, menu driven mainframe application consisting of screens and databases. AIS functions as an automated expenditure control and invoice/voucher processing system. AIS, in processing invoices, allocates invoice amounts into subaccounts; groups invoices, according to the Comptroller's Statewide Management System (SAMS), for the preparation of vouchers; and allows users to track cost centers.

The Accounting Information System (AIS) application was implemented in March 1995. AIS is currently utilized by 56 entities (see page 43 for the list of user agencies).

AIS transactions are entered online in a real-time environment, with the ability to batch transactions for processing at a later date. Data entered into the system is entered by the user agency and is the responsibility of the agency. To help ensure the accuracy of the data, AIS has several edit checks to alert the user of errors. AIS provides online and batch reports, as outlined in the AIS Users Manual, that may be used for reconciliation. During our review we selected two agencies' AIS data and tested for proper input, edits, and date fields. No significant weaknesses were identified.

Access to AIS is controlled through Resource Access Control Facility (RACF) software, in addition to AIS' internal security. Users must have a properly authorized RACF user ID and password to gain access to the operating environment. Assignment and authorization of access rights is the responsibility of agency security administrators. Once access to the operating environment has been allowed, users must have a separate application user ID and password to gain access to AIS. Two levels of application security enforce AIS' functional restrictions. One level permits initial transaction entry and maintenance functions; the second level allows auditing and final transaction approval.

Management stated that there have been no major changes to AIS in the past year. However, over the next fiscal year several changes to AIS are anticipated. These include changes to comply with Government Accounting Standard Board number 34 (GASB 34) requirements, promote an interface with Central Inventory System and Central Payroll System, and implement the Billing and Accounts Receivable Cash Systems.

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

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

- Verify that only accurate and authorized data are entered into AIS. It is the agency's responsibility to ensure that only properly authorized transactions are entered into the system.

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

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

- Establish policies and procedures for the administration of RACF IDs and regularly review the RACF profiles and defined user groups with access to AIS to ensure access authorized is appropriate.

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

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 Insurance
13. Department of Labor
14. Department of Lottery
15. Department of Military Affairs
16. Department of Natural Resources
17. Department of Professional Regulation
18. Department of Public Health
19. Department of Veterans' Affairs
20. Department on Aging
21. Emergency Management Agency
22. Environmental Protection Agency
23. General Assembly Retirement System
24. Guardianship and Advocacy Commission
25. Historic Preservation Agency
26. Human Rights Commission
27. Illinois Arts Council
28. Illinois Community College Board
29. Illinois Criminal Justice Information Authority
30. Illinois Deaf and Hard of Hearing Commission
31. Illinois Educational Labor Relations Board
32. Illinois Health Care Cost Containment Council
33. Illinois Industrial Commission
34. Illinois Law Enforcement Training and Standards Board
35. Illinois Racing Board
36. Illinois Student Assistance Commission
37. Illinois Violence Prevention Authority
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.

The CPS is currently utilized by 85 entities (see page 47 for the list of user agencies). The CPS users can enter data online or they can request their data be entered by Department personnel. It is the goal of the Department to have all agencies enter their data online and currently 81 user agencies do enter their data online.

The CPS has online edit checks, which prevent a user from entering a transaction with invalid data. If an error occurs during data entry, users are not allowed to continue until the error has been corrected. During our review, we selected two agencies' CPS data and tested social security numbers, voucher numbers, warrant amounts and date fields for proper input, and edits; no significant weaknesses were identified.

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

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

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 at the agency level, staff, internal auditors, and external auditors of agencies using CPS should:

- Verify that only accurate and authorized data are entered into CPS. It is the 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 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 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.

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

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

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 Liquor Control Commission
47. Illinois Math and Science Academy
48. Illinois Planning Council on Developmental Disabilities
49. Illinois Racing Board
50. Illinois Rural Bond Bank
51. Illinois State Board of Investment *
52. Illinois State Police
53. Illinois Student Assistance Commission
54. Joint Committee on Administrative Rules
55. Judges' Retirement System
56. Judicial Inquiry Board *
57. Legislative Audit Commission
58. Legislative Information System
59. Legislative Printing Unit
60. Legislative Reference Bureau
61. Legislative Research Unit
62. Legislative Space Needs Commission
63. Medical District Commission *
64. Office of Banks and Real Estate
65. Office of the Attorney General
66. Office of the Auditor General
67. Office of the Governor
68. Office of the Lieutenant Governor
69. Office of the 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
76. 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.

In 1998, the Department developed a new Central Inventory System and all users were migrated to the new system by August 1999. 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 management stated they are currently restricting the use of the Depreciation Process to DCMS' Accounting Division; however, it is expected that this feature will be provided later to agency users. The CIS is currently utilized by 31 entities (see page 51 for the list of user agencies).

The system is equipped with online edit checks, which provide the user with immediate notification if errors are encountered during data entry, and processing edit checks, which report processing errors online. Error reports are available to CIS staff and to user agencies. The Department generates a Location Balance Report nightly to determine whether transactions were processed correctly. Additional reports are also available to users for reconciliation purposes.

During our review, we selected three months of data for two agencies' containing 164,905 inventory items. We tested inventory tag numbers, changes in the price of each item from month to month, composition of date fields, and for reasonable relationships between date fields. We found no instances of duplicate inventory tags and all date fields contained 4 digit years. Although no significant problems were identified, we identified some problems with select date fields and transaction codes.

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

Management stated there were no significant changes to CIS in the past year; however, CIS will be rewritten to meet the needs of changing Accounting Standards in the near future. The CIS rewrite is awaiting Government Accounting Standard Board number 34 (GASB 34) requirements from the Office of the Illinois Comptroller, to enable the rewrite to encompass the defined parameters. The CIS rewrite is scheduled for completion by June 30, 2001.

CIS is automatically backed up nightly and backups are rotated to the off-site storage location on a monthly basis.

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

- Verify that only accurate and authorized data are entered into CIS. It is the agency's responsibility to ensure that only properly authorized transactions are entered into the system.

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

- 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 CIS to ensure access authorized is appropriate.

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

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 in 1992 by the Department and is currently utilized by 30 entities to provide a comprehensive system for recording and managing employee benefit time (see page 55 for the list of user agencies).

CTAS provides for attendance information to be recorded using the positive or exception method. The positive method of recording daily attendance requires the timekeeper to enter or confirm an employee's attendance information. The exception method assumes that an employee's scheduled work time is the correct attendance unless the timekeeper enters something different.

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

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

Management stated that there have been no major changes to CTAS in the past year.

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

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

- Verify that only accurate and authorized data are entered into CTAS. It is the agency's responsibility to ensure that only properly authorized transactions are entered into the system.

- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions. Auditors should verify that agency personnel review timekeeping reports prepared by the system to ensure the reports are correct.

- 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 CTAS 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 Professional Regulations
12. Department of Public Health
13. Department of Revenue
14. Department of Veterans' Affairs
15. Emergency Management Agency
16. Environmental Protection Agency
17. Guardianship and Advocacy Commission
18. Human Rights Commission
19. Illinois Criminal Justice Information Authority
20. Illinois Deaf and Hard of Hearing Commission
21. Illinois Education Labor Relations Board
22. Illinois Health Care Cost Containment Council
23. Illinois Industrial Commission
24. Illinois Law Enforcement Training and Standards Board
25. Illinois Planning Council on Developmental Disabilities
26. Office of Banks and Real Estate
27. Office of the Attorney General
28. Office of the Governor
29. Property Tax Appeal Board
30. 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:
   - Submit to the Department a listing of critical applications, with all pertinent information.
   - Develop and update disaster contingency plans to ensure the plans meet current disaster recovery needs, and submit their plans to the Department.
   - Ensure all data is backed up and stored off-site.
   - Annually test all critical applications and submit test results to the Department.

2. **Available security mechanisms should be used.**
   User agency RACF coordinators should utilize the capabilities of RACF, and perform periodic reviews of existing RACF profiles to ensure that access rights are appropriate. In addition, user agency RACF coordinators should:
   - Formally encourage users (until the Department enforces more secure RACF parameters) to select longer passwords, and include a non-alphabetic in their passwords, to protect the security of their account.
   - Review revoked IDs, and delete unneeded IDs.
   - Determine which data sets under the agency's control have a UACC of ALTER, and change the UACC to a more restrictive parameter.

3. **Security over Internet use should be reviewed**.
   To enhance Internet security agencies should:
   - Monitor staff use of the Internet and filter Internet content.
   - Avoid any insecure transmission of confidential or sensitive information across the Internet.
   - Obtain Internet service exclusively from the Department so as not to pose a potential threat to the protected environment. The Statewide IT Security Policy requires State agencies to acquire their Internet access from the Department, unless written approval for an exception is granted by the Director of the Department of Central Management Services.
   - Install virus detection software to protect computer resources.

4. **Security of VM systems should be reviewed.**
   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 requesting telecommunication equipment and changes should be reviewed.**
   When a request requires both a Terminal Generation Request form and a Terminal Data Service Request form, the user agency should ensure that the forms are submitted at the same time, to reduce the likelihood of inefficiencies and implementation delays.

6. **Bills for computer services should be reviewed.**
   User agencies should monitor their monthly billing to ensure charges are correct. In addition, the agencies should ensure their name and address on the billing are correct.

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 39 through 55 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.**
   User agencies should:
   - Update and return their Security Authorization and Tape, Print, and Diskette Lists to the CCF Security Administrator within the required timeframe.
   - Ensure users are aware of their responsibilities when using Department resources.

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. Human Rights Commission
43. Illinois Arts Council
44. Illinois Commerce Commission
45. Illinois Commission on Intergovernmental Cooperation
46. Illinois Community College Board
47. Illinois Criminal Justice Information Authority
48. Illinois Deaf and Hard of Hearing Commission
49. Illinois Development Finance Authority
50. Illinois Educational Labor Relations Board

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