REPORT DIGEST

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES BUREAU OF COMMUNICATION AND COMPUTER SERVICES

THIRD PARTY REVIEW
For the Year Ended:
June 30, 2007

Release Date:
July 11, 2007

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

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

This Report Digest and Full Report are also available on the worldwide web at http://www.auditor.illinois.gov

INTRODUCTION

The Department of Central Management Services' (Department) Bureau of Communication and Computer Services carries out statutory responsibilities relating to data processing and telecommunication services (20 ILCS 405/405-10; 20 ILCS 405/405-20; 20 ILCS 405/405-250; 20 ILCS 405/405-255; 20 ILCS 405/405-260; 20 ILCS 405/405-270 and 20 ILCS 405/405-410). To fulfill its responsibilities, the Department operates the Central Computer Facility (CCF), the Communications Center, and branch facilities. Through its facilities, the Department provides data processing services to approximately 97 user entities.

The Department is mandated to manage or delegate the management of the procurement, retention, installation, maintenance, and operation of all electronic data processing equipment used by State agencies to achieve maximum economy consistent with development of adequate and timely information in a form suitable for management analysis, in a manner that provides for adequate security protection and back-up facilities for that equipment.

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

We reviewed data processing general controls at the Department primarily during the period from January 2, 2007 to May 31, 2007. We performed tests to determine compliance with policies and procedures, conducted interviews, performed observations, and identified specific control objectives and procedures we considered necessary to evaluate the controls.

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

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

STATISTICS	2007
Mainframes	3 Units Configured as 10 Production Systems and 5 Test Systems 1 Unit Configured as 5 Systems for Business Continuity
Services/Workload	Impact Printing – 12 Million Lines per Month Laser Printing – 18.4 Million Pages per Month
State Agency Users	97
Bureau Employees	2004 -- 303 2005 -- 775* 2006 -- 777 2007 -- 748 * Increase due to IT consolidation into the Department per Public Act 93-25
Historical Growth Trend**	2004 -- 3,614 -- MIPS 2005 -- 3,217 -- MIPS 2006 -- 3,217 -- MIPS 2007 -- 3,962 -- MIPS -- Million Instructions Per Second ** In the month of April for each year listed

Information provided by the Department - Unaudited

DEPARTMENT DIRECTOR AND DEPUTY DIRECTOR/BUREAU MANAGER
During Audit Period: Director: Paul Campbell (7/1/2006 to 3/9/2007) Deputy Director/Bureau Manager: Tony Daniels (7/1/2006 to 2/22/2007) Currently: Acting Director: Maureen O'Donnell (3/10/2007 to present) Acting Deputy Director/Bureau Manager: Doug Kasamis (2/23/2007 to present)

REPORT SUMMARY

We identified three significant deficiencies for which we could not obtain reasonable assurance over the controls.

Midrange Environment

Public Act 93-25 authorized the Department of Central Management Services to consolidate Information Technology (IT) functions of State government. From May 2006 to April 2007 over 775 servers were transferred to the Department from agencies participating in the consolidation project.

No standardized process to administer, secure, and monitor midrange environment

During our analysis, it became apparent a standardized process to administer, secure, and monitor the midrange environment had not been implemented. Since a standardized process had not been implemented to manage the midrange environment, we were not able to develop a method to effectively test midrange installation, maintenance, operations, and security controls. Due to the lack of a standardized process, we were unable to perform tests to provide positive assurance that administration, security, and monitoring controls in the midrange environment were consistently applied to all systems.

As the Department's responsibilities for controlling the midrange environment continue to increase, it is imperative the Department implement a standardized process to ensure controls over all servers are consistently applied and meet Department requirements.

The Department should develop, obtain formal approval, and implement policies and procedures across the midrange environment. Specifically, the Department should develop and implement a standardized process to administer, secure, and monitor servers in the midrange environment. (pages 6-8)

The Department concurred with our recommendation. Department officials stated they will move forward to more effectively standardize the midrange environment.

Security Policies

The Department had the primary responsibility for providing IT services to State Government. Thus, it is imperative the Department implement a framework to promote and apply prudent, comprehensive, and effective security practices. The expanding use of information technology, increased sharing of sensitive information, and emerging IT risks make it imperative that security be appropriately addressed.

Security policies had not been updated to reflect current environment

Although new IT security policies/procedures were approved in December 2006; they had not been implemented or disseminated. The IT security policies posted on the Department's Intranet site had not been updated since at least February 2003, and did not reflect the current technological environment or address current security concerns.

The Department should thoroughly review and update security policies to address the current technological environment, consolidation issues, and present-day risks. (page 8)

The Department concurred with our recommendation. Department officials stated security policies and procedures had been reviewed, updated, and published on the BCCS web portal.

Information Technology Billings

Due to the consolidation of various functions of State government into the Department, the Internet Billing System (IBiS) was developed to provide a mechanism to bill agencies for consolidated services. The billing invoices were the foundation for agencies to make payments to the Department. Additionally, the invoices were to provide documentation for agencies to use for Federal Fund participation purposes. The Department billed for Information Technology services to consolidated agencies through IBiS. We reviewed the Information Technology portion of IBiS.

Billing methodology weaknesses were identified

A formal methodology clearly documenting the allocation of charges to consolidated agencies did not exist. In addition, the process and associated documentation did not provide the necessary support to verify the appropriateness of charges to consolidated agencies.

To ensure that billing statements accurately reflect services rendered to consolidated agencies, the Department should:

- Develop and implement a formal methodology to clearly document the billing rate structure and allocation of charges.
- Develop a process to review and verify the accuracy of billing statements.
- Provide adequate documentation to agencies to support billing statements and comply with federal fund reimbursement guidelines. (pages 8-9)

The Department concurred with our recommendation. Department officials stated although documentation for the IBiS charging methodology does exist and training was provided to staff, the process was not fully optimized during the period under review.

Although not covered under audit standards as a deficiency, the deficiency outlined below may impact the Department's ability to process in the future.

Disaster Contingency Planning

Although the Department had developed some basic strategies to address the disaster contingency needs of the State's Central Computer Facility, the plans and operational provisions need to be enhanced to provide assurance that all of the State's critical applications and network operations can be recovered within required timeframes.

State lacks preparedness

The Department had not implemented and tested procedures to protect critical information resources, minimize the risk of unplanned interruptions, and ensure the availability of critical information resources within acceptable timeframes.

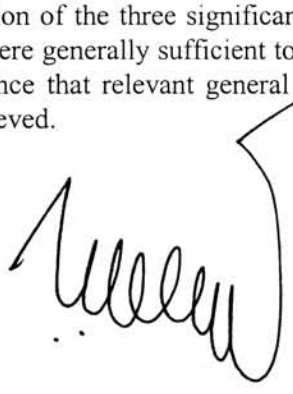
The State is placing great reliance on the Department's ability to provide data processing and network services in the event of a disaster. As such, comprehensive and thoroughly tested disaster contingency plans are an essential component of recovery efforts.

The Department should ensure the necessary components (plans, equipment, and facilities) are available to provide for continuation of critical computer operations in the event of a disaster. In addition, the Department should obtain a suitable regional alternate location for recovery services, and conduct comprehensive tests of the plans on an annual basis. (pages 9-10)

The Department partially concurred with our recommendation. Department officials stated they agree that they do not have a comprehensive midrange disaster recovery plan as a result of the current state of the consolidation effort. Prior to the consolidation, the degree in which an agency had a midrange disaster recovery plan varied significantly.

AUDITORS' OPINION

With the exception of the three significant deficiencies described above, 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