THIRD PARTY REVIEW

Department of Central Management Services
Bureau of Communication and
Computer Services

July 2008

TABLE OF CONTENTS

REPORT DIGEST

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
BUREAU OF COMMUNICATION AND COMPUTER SERVICES

THIRD PARTY REVIEW
For the Year Ended:
June 30, 2008

Release Date:
July 9, 2008

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
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 agencies.

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, 2008 to May 16, 2008. 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	2008
Mainframes	4 Units Configured as 12 Production Systems and 6 Test Systems 1 Unit Configured as 5 Systems for Business Continuity
Services/Workload	Impact Printing – 11.8 Million Lines per Month Laser Printing – 15.4 Million Pages per Month
State Agency Users	97
Bureau Employees	2005 -- 775 2006 -- 777 2007 -- 748 2008 -- 708
Historical Growth Trend**	2005 -- 3,217 -- MIPS 2006 -- 3,217 -- MIPS 2007 -- 3,962 -- MIPS 2008 -- 4,018 -- 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 and Current Acting Director: Maureen O’Donnell Deputy Director/Bureau Manager: Doug Kasamis

REPORT SUMMARY

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

Security Policies

Security policies had not been updated to reflect current environment

The Department has 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.

The policies outlined in the Department's Description of Control as current and approved, were actually not in effect, and were not published by posting them to the appropriate repository. The Department developed several updated policies in December 2007; however, the policies published on the Intranet still did not reflect the current technological environment or address security concerns.

Even though this deficiency was included in the last two Third Party Reviews, the Department had not taken comprehensive action to remedy the control weakness. To ensure the framework exists to promote and guide security practices, the Department should thoroughly review and update security policies to address the current technological environment, consolidation issues, and present-day risks. Once finalized, the policies (and associated procedures) should be implemented, formally communicated, and disseminated (along with being placed in the appropriate repository) to all affected parties. (page 6)

The Department concurred with our recommendation. Department officials stated the Department is taking steps to address the recommendation.

Information Technology Billings

Billing methodology weaknesses were identified

The Department billed user agencies for various services, based on utilizations and rates developed by the Department. However, based on inquiries and review of billing data, the Department had not implemented an adequate process/methodology to ensure the appropriateness of billings to agencies.

Billing invoices were the foundation for user agencies to make payments to the Department, including payments from the 11 agencies included in the consolidation of various functions of State government into the Department.

To ensure the accuracy of the billings, the Department should:

- Develop a process to ensure billings are appropriate and accurately reflect services rendered.
- Develop a formal methodology to clearly document the allocations of rates and charges to user agencies. (pages 6-7)

The Department concurred with our recommendation. Department officials stated that at the beginning of fiscal year 2008, BCCS instituted several new rates for services that had been previously billed through the IBiS system. Many of the issues found during the review were related to these newly rated services and BCCS is working diligently to correct any deficiencies and ensure proper controls are in place. The Department will also work to document the methodology used to develop these rates, as this is a requirement for the fiscal year 2008 Statewide Cost Allocation Plan. Department officials stated, by the beginning of fiscal year 2009, BCCS hopes to have rates for all services and no longer utilize the IBiS system.

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

Disaster Contingency Planning

Disaster Contingency Planning Weaknesses

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.

The Department had not adequately implemented 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 conduct comprehensive tests of the plans on an annual basis. (page 7)

The Department partially concurred with our recommendation. Department officials stated they agree that they need to improve and update the plans, procedures and overall recovery documentation. However, the Department believes it has demonstrated through local and regional tests that it is able to recover the State's Category 1 applications where the agencies have provided appropriate documentation to do so.

AUDITORS' OPINION

With the exception of the two 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

SPRINGFIELD OFFICE:
ILES PARK PLAZA
740 EAST ASH • 62703-3154
PHONE: 217/782-6046
FAX: 217/785-8222 • TTY: 888/261-2887

CHICAGO OFFICE:
MICHAEL A. BILANDIC BLDG. • SUITE S-900
160 NORTH LASALLE • 60601-3103
PHONE: 312/814-4000
FAX: 312/814-4006

OFFICE OF THE AUDITOR GENERAL
WILLIAM G. HOLLAND

AUDITOR'S REPORT

The Honorable William G. Holland
Auditor General
State of Illinois

We have examined the accompanying description of controls related to the systems and procedures used to control data processing operations at the Bureau of Communication and Computer Services of the Department of Central Management Services (Department). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the Department's controls that may be relevant to a user agency's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user agencies applied the controls contemplated in the design of the Department's controls; and (3) such controls had been placed in operation as of May 16, 2008. Our examination, started in July 2007 and primarily performed between January 2, 2008 and May 16, 2008, was limited to controls at the Department. The control objectives were specified by management of the Department. Our examination was performed in accordance with the Illinois State Auditing Act, applicable generally accepted auditing standards, and "Government Auditing Standards" issued by the Comptroller General of the United States. We included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

The accompanying description identifies several controls that were deemed inaccurate, based on test work performed. The identified controls are outlined in Appendix C.

In our opinion, except for the matters referred to in the preceding paragraph, the accompanying description of the aforementioned systems and procedures presents fairly, in all material respects, the relevant aspects of the Department's controls that had been placed in operation as of May 16, 2008.

The Department's description stated the Department had developed new security policies. However, based on inquiries of staff and inspection of activities, we determined the policies had not been implemented and the policies that were in effect did not reflect the current technological environment or address security concerns.

In addition, the description stated the Department billed user agencies for various services, based on utilizations and rates developed by the Department. However, based on inquiries and review of billing data, the Department had not implemented an adequate process/methodology to ensure the appropriateness of billings to agencies.

Also, in our opinion, except for the matters referred to in the preceding paragraphs, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user agencies applied the controls contemplated in the design of the Department's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in the body of the report, to obtain evidence about their effectiveness in meeting the control objectives, during the period from January 2, 2008 through May 16, 2008. 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 agencies and to their auditors to be taken into consideration, along with information about the internal control at user agencies, when making an assessment of control risk for user agencies. In our opinion, except for the matters referred to in the preceding paragraphs, 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 2, 2008 through May 16, 2008. However, the scope of our engagement did not include tests to determine whether control objectives at the user agencies were achieved.

The relative effectiveness and significance of specific controls at the Department, and their effect on assessments of control risk at user agencies, are dependent on their interaction with the controls and other factors present at individual user agencies. We have performed no procedures to evaluate the effectiveness of controls at individual user agencies.

The description of controls at the Department is as of May 16, 2008, and information about tests of the operating effectiveness of specified controls covers the period from January 2, 2008 through May 16, 2008. 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.

Will J. Say
William J. Samplas, CISA
Director, Information Systems Audits

Mary K Love
Mary Kathryn Lovejoy, CPA, CISA
Information Systems Audit Manager

May 16, 2008

REPORT SUMMARY

INTRODUCTION

The Department of Central Management Services' (Department) Bureau of Communication and Computer Services (Bureau) carries out statutory responsibilities relating to data processing and telecommunication services (20 ILCS 405/405-10; 20 ILCS 405/405-20; 20 ILCS 405/405-250; 20 ILCS 405/405-255; 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 agencies (see Appendix B).

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. The Third Party Review addressed controls which were included in the Department’s Description of Control. The control associated with the midrange environment for the 11 consolidated agencies was not included in the Department’s Description of Control and, therefore, not included in our review. In addition, we did not review the controls over the 11 consolidated agencies’ environments or other user agencies. As a result of our review, 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 the following systems maintained by the Department for State agencies' use:

- Accounting Information System;
- Central Payroll System;
- Central Inventory System; and
- Central Time and Attendance System.

We identified several control deficiencies that appear in pages 43 through 183; in addition, we noted two significant deficiencies for which we could not obtain reasonable assurance over the controls.

Security Policies

The Department has 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.

The policies outlined in the Department's Description of Control as current and approved, were actually not in effect, and were not published by posting them to the appropriate repository. The Department developed several updated policies in December 2007; however, the policies published on the Intranet still did not reflect the current technological environment or address security concerns.

Even though this deficiency was included in the last two Third Party Reviews, the Department had not taken comprehensive action to remedy the control weakness. To ensure the framework exists to promote and guide security practices, the Department should thoroughly review and update security policies to address the current technological environment, consolidation issues, and present-day risks. Once finalized, the policies (and associated procedures) should be implemented, formally communicated, and disseminated (along with being placed in the appropriate repository) to all affected parties. (See pages 112-116 for additional information)

Department Response

The Department concurs with the recommendations of this report and is taking steps to address.

Information Technology Billings

The Department billed user agencies for various services, based on utilizations and rates developed by the Department. However, based on inquiries and review of billing data, the Department had not implemented an adequate process/methodology to ensure the appropriateness of billings to agencies.

Billing invoices were the foundation for user agencies to make payments to the Department, including payments from the 11 agencies included in the consolidation of various functions of State government into the Department.

We also identified problems with the accurate reconciliation of desktop and midrange software that had a bearing on agency billings.

To ensure the accuracy of the billings, the Department should:

- Develop a process to ensure billings are appropriate and accurately reflect services rendered.
- Develop a formal methodology to clearly document the allocations of rates and charges to user agencies. (See pages 53-61 and 85-88 for additional information)

Department Response

The Department concurs with the Auditor's recommendations. At the beginning of fiscal year 2008, BCCS instituted several new rates for services that had been previously billed through the IBiS system. Many of the issues found during the review were related to these newly rated services and BCCS is working diligently to correct any deficiencies and ensure proper controls are in place. The Department will also work to document the methodology we used to develop these rates, as this is a requirement for the fiscal year 2008 Statewide Cost Allocation Plan. By the beginning of fiscal year 2009, BCCS hopes to have rates for all services and no longer utilize the IBiS system.

Other Control Deficiencies

Although not covered under audit standards as a significant deficiency, the deficiency outlined below may impact the service organization's ability to process information in the future; therefore, we include the following information.

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.

The Department had not adequately implemented 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 the continuation of critical computer operations in the event of a disaster. In addition, the Department should conduct comprehensive tests of the plans on an annual basis. (See pages 75-80 for additional information)

Department Response

The Department partially concurs with the finding and recommendations. The Department agrees that we need to improve and update the plans, procedures and overall recovery documentation. The Department however, has demonstrated through local and regional tests that it is able to recover the State's Category 1 applications where the agencies have provided appropriate documentation to do so.

The Department responses were provided on June 11, 2008, by Doug Kasamis, Deputy Director/Bureau Manager, Bureau of Communication and Computer Services of the Department of Central Management Services.

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

This Page Intentionally Left Blank

SERVICE ORGANIZATION - DESCRIPTION OF CONTROLS

The following Description of Controls section (pages 9 through 40) consists of text provided by the Department of Central Management Services.

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
BUREAU OF COMMUNICATION AND COMPUTER SERVICES
DESCRIPTION OF CONTROLS

The Department of Central Management Services' (Department) Bureau of Communication and Computer Services (Bureau) organizational structure is described below, followed by the description of controls which have been organized by the eight major control areas.

BUREAU ORGANIZATION

The Department of Central Management Services' (Department) Bureau of Communication and Computer Services (Bureau) is statutorily mandated to provide "use of electronic data processing equipment, including necessary telecommunications lines and equipment, available to local governments, elected State officials, State educational institutions, and all other governmental units of the State requesting them." (20 ILCS 405/405-250)

To fulfill this responsibility, the Department operates the Central Computer Facility (CCF), the Communications Center, and various branch facilities.

The Bureau has six Divisions, which, in turn, have several subdivisions:

- Chief of Staff
  - Acquisitions and Inventory Management
  - Workforce Development and Logistics
  - Enterprise Program Management Office
- Infrastructure Services
  - Network Services
  - End User Computing
  - Infrastructure Support
    - Change Management
    - Production Quality Assurance and Methods
  - Enterprise Production Operations
  - Data Center Operations
    - Enterprise Backup And Storage
    - Midrange Computing
    - Mainframe
- Enterprise Applications and Architecture
  - Enterprise Architecture and Strategy
  - Enterprise Business Applications and Services

    - Personal Information Management (PIM)
- Security and Service Delivery
    - Service Delivery and Implementation
    - Risk Management
- Business Services
    - Revenue Management
    - CRF Expenditure and Invoice Verification
    - SSRF Invoice Verification
    - Appropriations Management
- Customer and Account Management
    - Agency Relations
    - Field Operations
    - Customer Solution Center
    - Communications Management Center
    - Service Reporting

DESCRIPTION OF CONTROLS

1. Administration

a. Strategic and Business Planning

The Bureau monitors technological trends through strategic and business planning.

The Bureau's Strategic Plan is developed by the Leadership Team based on both personal knowledge and external information. This knowledge is then correlated with Bureau initiatives and documented in the Strategic Plan. The Plan is used by the Leadership Team as an internal guide for Bureau strategy.

Business planning is accomplished by collecting relevant budgetary information from Consolidated Agencies, Illinois State Police, Department of Corrections, and the Department of Children and Family Services. The Bureau requests this information via a memo from the Deputy Director addressed to agency executive directors, chief financial officers, and chief information officers. This information is captured and maintained within the Consolidated Project Portfolio database. Collected information identifies planned business initiatives and anticipated changes to Business as Usual expenditures. This data is analyzed by Enterprise Architecture and Strategy (EA&S) to provide a forecast of anticipated IT and telecom expenditures resulting in a coordinated Spending Plan and a coordinated Budget Submittal.

Identification of current business applications are tracked in the Business Reference Model (BRM) and current technology standards are tracked in the Technical Reference Model (TRM). EA&S is responsible for the maintenance of these databases. Agencies are responsible for updating information in the BRM. EA&S and the Architecture Rationalization Board (ARB) manage and document architectural standards via the TRM, Product Standardization Requests, and ARB meeting minutes.

b. Project Management

Project management is the responsibility of the Enterprise Program Management Office (EPMO). Projects are initiated by submittal of a Project Charter. Projects requiring governance are monitored by the EPMO and/or responsible divisional staff using various methods including Microsoft Project Professional.

For projects that meet governance criteria, the EPMO or responsible division assigns a project manager or work coordinator for oversight of the project. For projects directly managed by the EPMO, a team site is created within a SharePoint repository and project status information is captured within Microsoft Project Professional. Specific project management processes including planning, execution, and operational transition vary by project based upon the specific needs of each project. The EPMO provides a recommended set of project management tools and artifacts that should be utilized (as appropriate) for most projects.

An Executive Dashboard, listing projects identified by the Leadership as those requiring special attention, is maintained by the EPMO and updated weekly for review by the Leadership Team to keep Bureau management informed of their status.

c. IT Governance

The Bureau's IT governance process aids in the consistent business and technical alignment of proposed initiatives which are subject to governance (criteria explained below). These initiatives are reviewed by the EPMO's IT Governance team and EA&S to determine business and technology alignment as defined in the BRM and TRM.

The IT governance process is defined by a series of "Gates" as outlined on the IT Governance web site (www.illinois.gov/governance/default.cfm) and is managed by the EPMO. IT Governance information is maintained in a Remedy-based application.

The IT Governance process (www.illinois.gov/governance/governance.cfm), requires that a Project Charter and Business (functional) and Technical (non-functional) requirements be provided for each initiative or project subject to governance. This information is utilized by the EPMO and EA&S to evaluate business and architectural alignment. IT Governance is required for those initiatives that meet one or more of the following criteria:

- Adding new business functionality
- Moving to a new or updated platform such as a new database, architecture, or programming language

- Replacing an old system (lifecycle)
- Outsourcing or in-sourcing a system, either partially or completely
- Potentially instantiating an enterprise application or service.

For Infrastructure projects, the Infrastructure Services Division (ISD) organizes, plans, and controls these projects and participates in reviewing charters, functional and non-functional requirements, gathering and organizing detail design information, tracking and documenting issues and action items, status reporting, documenting work processes and coordinating activities between client agencies and the Bureau. The following policies guide ISD staff activities:

- Charter Review Process, dated March 5, 2007,
- Charter Review PAR Procedures, dated March 5, 2007, and
- BCCS Charter Review, dated April 18, 2006.

d. Billing

The Department is statutorily authorized to provide data processing and telecommunications services for State agencies. The Department and state agencies share the costs of those services. Funding is obtained through the Statistical Services Revolving Fund (SSRF), the Communications Revolving Fund (CRF), internal service funds, and the General Revenue Fund (GRF).

The Department requires the agencies to remit the total amount on the invoice. Payment is to be made within one billing cycle of receipt. The Department's Accounting Division is responsible for pursuing outstanding SSRF and CRF accounts. If an agency persists in not paying delinquent amounts, the Department's Director may send a letter to the Director of the delinquent agency requesting payment.

Business Services pursues outstanding Network accounts. Non payment for Network Services results in submission to the IOC offset program through the Department's Accounting Division.

SSRF

The KOMAND IV system (system) is the primary system used to compile the SSRF billing. The system provides a means for charging resource utilization data back to the users of the computer systems. Users are billed for various services, such as use of the Local Area Network, on-line storage, mainframe usage, and print jobs. In addition, users are charged for the usage of the "Common Systems": Accounting Information System; Central Inventory System; Central Time and Attendance System; and Central Payroll System. The Department has developed procedures for each phase of the SSRF billing process. At the end of each phase, verification is performed to ensure all totals are correct. Reports from each source are verified against each other to ensure accuracy of the information. Throughout the process, an "Edit Check" is conducted to ensure completeness and accuracy of each phase. In order to comply with the Federal

Department of Human Services' requirements (A-87), the Department annually performs an analysis of the previous years' cost and revenue by service center and determines the profit/loss for each service. Excess revenues are subject to reimbursement to the Federal Department of Human Services, and may involve billing credits.

CRF

BCCS uses a database called EMS11 to generate approximately 90-95% of billings for the CRF. BCCS uses the Accounting Information System (AIS) for the remaining telecommunications billings. Most statewide telecommunications services are billed to CMS by telecommunications carriers. CMS then bills users based on their consumption of these services. Vendors charge CMS based either on contractual rates or on tariff rates published with the ICC. CMS re-bills users to recover vendor charges plus administrative expenses. Generally the administrative markup is 10%. In June, 2007, a conversion to the EMS11system instituted the procedure of one billing run per month. Billings for network bandwidth usage and/or other network services for constituents which are non-state agencies are billed monthly through the MAS90 system. The Department has developed procedures for each phase of the CRF and MAS90 billing processes. At the end of each phase, verification is performed to ensure all totals are correct. Reports from each source are verified against each other to ensure accuracy of the information. In order to comply with the Federal requirements (A-87), the Department annually performs an analysis of the previous years' cost and revenue by service center and determines the profit/loss for each service. Excess revenues are subject to reimbursement to the Federal Government.

Internet Billing System (IBiS)

Due to the consolidation of various functions of State government into the Department, IBiS was developed to provide a mechanism to bill agencies for consolidated services for which there is no rate. The billing invoices are the foundation for agencies to make payments to the Department. Additionally, the invoices are to provide documentation for agencies to use for Federal Fund participation purposes.

IBiS was utilized by the consolidated agencies:

- Department of Agriculture
- Department of Commerce and Economic Opportunity
- Department of Natural Resources
- Department of Employment Security
- Department of Financial and Professional Regulation
- Department of Human Services
- Department of Healthcare and Family Services
- Department of Public Health
- Department of Revenue
- Department of Transportation
- Environmental Protection Agency

The Department bills for the following consolidated services through IBiS:

- Facility Management,
- Information Technology, and
- Communication.

The IBiS file contains salary and fringe benefits costs for consolidated agency personnel whose time is charged back to a specific consolidated agency (agencies). The data is based upon the service center code entered into the Service Center Allocation System (SCAS) and applied to the employee's payroll cost for each pay period that month.

For AIS file support documentation Business Services downloads the AIS billing file from the mainframe. The file is sorted by Agency, and a spreadsheet is created for each agency. The detail file lists each invoice that was paid on behalf of the agency that month and includes the agency service center, cost center, DOC, voucher control number, voucher date and number, vendor name, vendor invoice number, beginning and ending dates of the service, and the amount. It is the agencies responsibility to review the monthly billing statement and verify the accuracy of the charges.

The Department has developed procedures for the IBiS billing process for Salaries/Fringe Benefits and for AIS files. At the end of the procedure verification is performed to ensure all totals are correct.

In order to comply with the Federal Department of Human Services' requirements (A-87), the Department annually performs an analysis of the previous years' cost and revenue by service center and determines the profit/loss for each service. Excess revenues are subject to reimbursement to the Federal Department of Human Services, and may involve billing credits.

e. Help Desk

Customer Management Center (CMC)

The CMC is the 24/7 network support center for the State of Illinois. The CMC supports the backbone and customer access circuits for all legacy ICN customers such as the educational community, which includes K-12 schools as well as libraries, museums, hospitals and other not for profit organizations. The CMC also supports state agencies, boards, and commissions. After 5:00 PM and during non-business hours, weekends and holidays, the CMC provides emergency help desk support for voice, wireless, and data services. In coordination with the Command Center, the CMC assists with after hour IT emergency support issues including taking customer calls and monitoring enterprise servers via Hobbit for ICN customers (educational and State agencies), the CMC acts as the first point of contact between the trouble initiator or end-user and any internal/external vendor/resource that has a required step in isolating and repairing network incidents. Incidents are managed in accordance with established procedures.

The CMC has vendor management procedures that are followed. Vendors supply updated lists identifying their hierarchical management chain with detailed contact information (desk, cell and home numbers). These resources (i.e. people) are available 24/7. The CMC staff provides status to the customer on an hourly basis, and escalates if required, to the vendor until an issue is resolved (service restored). Upon every escalation, CMC staff updates the end-user or affected party of status. All of this is captured and documented via ticketing tools such as ICN Remedy or CMS Remedy, (depending under which ticket tool the asset is inventoried).

Customer Solution Center

The CSC is responsible for providing Tier 1 support for Telecommunications (excluding Illinois Century Network and Radio) and IT services. The CSC is a single point of contact (SPOC) where client solutions are handled for different technologies and simplifying end user support. The CSC is responsible for managing timelines and the value of the products and services offered through the CSC Service Desk and the vendors and internal teams supporting those products and services. The CSC has processes and guidelines in place for enterprise-wide management, escalation and notifications, and other operational needs.

The CSC IT Service Desk is responsible for providing Tier 1 IT technical and end user support to the consolidated agencies as well as the multiple boards, commissions and non-consolidated agencies. The IT Service Desk is the single point of contact for reporting IT incidents and requesting new services. The IT Service Desk is staffed during normal business hours Monday thru Friday 8 am to 5 pm, with extended coverage from 8 am to 4 pm on Saturday and Sunday for HFS and DHS. Evening coverage for HFS and DHS is provided by production operations staff working at the legacy agency locations.

The physical consolidation of service desk staff for 11 of the 12 agencies in Springfield has been completed. Chicago-based IT Service Desk staffs (DES and DFPR) have been consolidated to the James R. Thompson Center utilizing the CMS Remedy for ticketing and the Avaya phone system.

Customers contact the IT Service Desk via phone or email to report an incident. The Service Desk staff opens a ticket in BCCS Remedy and records the category, type, and item (CTI), as well as the customer name, agency, contact and demographic information and a detailed incident description. If the IT Service Desk is unable to resolve the incident, the ticket is assigned to Tier 2 or Tier 3 support teams based on the CTI and/or predefined summary field. Procedures exist for the Help Desk task.

The IT Service Desk receives an Enterprise Service Request form (ESR) from an authorized IT coordinator. All IT changes require a request form. The IT Service Desk has standardized on the ESR process and the intake of service requests in the Remedy system for all consolidated agencies. Service requests are submitted via email.

Each agency head delegates, in writing, an IT coordinator(s) authorized to expend funds. The IT Coordinator database is maintained by Agency Relations. The IT coordinator is responsible for submitting the appropriate request forms to the IT Service Desk for all IT changes. The IT Service Desk staff is responsible for verifying the submitter is an authorized coordinator in the database. The coordinators can locate the instructions for completing these forms on the Bureau's Web site (www.bccs.illinois.gov/downloads.htm) and are provided guidance by the IT staff when necessary. Procedures exist for the ESR processing task.

Telecommunications Service Desk

The Telecommunications Service Desk is responsible for maintenance and provisioning of voice, video, data and wireless systems and services for State agencies, constitutional officers, commissions, boards, universities and institutions. The Telecommunications Service Desk handles all calls for telecommunications services during regular business hours Monday thru Friday 8am through 5pm, excluding ICN and Internet calls which are routed directly to the CMC. All telecommunications service calls outside regular business hours and on holidays are handled by the CMC.

The Help Desk records all reported incidents in the Remedy Help Desk module. Customers contact the Help Desk via phone to report an incident. The Help Desk is responsible for all reported incidents from the time reported until resolution and confirmation from the customer is achieved. Procedures exist for the Help Desk task.

Monthly reports are generated from the Remedy system based on a fiscal year to track and monitor vendor performance levels for voice related services. These figures are reconciled with the appropriate vendor(s). The CSC managers and Quality Assurance staff attend a quarterly meeting with the vendor(s) to review task related reports.

The Provisioning unit receives forms via email or mailed paper copies from the authorized agency coordinator. All telecommunications changes require a request form. Different forms are required for different services. Data requests require a Telecommunications Data/Intercity Service Request form (TDR); voice and cellular requests require a Telecommunications Service Request (TSR); paging requests require a Paging Service Request (PSR); IWIN requests require a Wireless Service Request (WSR) form.

Each agency head delegates, in writing, a telecommunications coordinator(s) authorized to expend funds. The Telecom Coordinator database is maintained by the CSC Administration staff and an alternate. The agency coordinator is responsible for submitting the appropriate request forms to the Telecommunications Service Desk for all telecommunications changes. The CSC Provisioning staff is responsible for verifying the submitter is an authorized coordinator in the database. The coordinators can locate the instructions for completing these forms on the Telecom Web site (www.state.il.us/cms/telecom) and are provided guidance by the Provisioning staff when necessary. Procedures exist for the Provisioning task.

The agency coordinators have access to the Bureau's Expense Management System (EMS) and can check status of their agency orders only. The EMS system tracks ordered facilities and telecommunications equipment. The inventory module provides the asset's recurring monthly charge, location information, 'AU' code, maintenance vendor description, catalog description and model description in addition to user name, tag number and serial number if applicable to the inventory item. The inventoried asset's installation cost can be found for all rated catalog codes in the Inventory Service Catalog Maintenance module. Anytime an inventoried piece of equipment is installed, removed or moved from one location to another, an order is entered into the EMS system to update the system inventory.

Tagged data equipment is received and tagged by the Acquisitions & Inventory Management (AIM) warehouse staff while tagged voice equipment is sent directly to the site. A Property Control Form (PCF) is completed for newly tagged voice systems and attached to the original invoice before it is sent to Business Services for processing and entry into the Common Inventory System (CIS). The voice system is tagged by the CSC Consulting and Procurement staff at the time of acceptance. Tagged data and voice equipment listed in EMS is reconciled to the listed equipment in CIS annually by AIM. Discrepancies are reported to CSC management and investigated.

Monthly reports are generated from the EMS system based on a fiscal year to track and monitor vendor performance levels for completion of voice orders in the Springfield and Chicago dedicated areas, the non-dedicated areas, non-routine orders and the overall vendor performance levels. These figures are reconciled with the appropriate vendor(s). The CSC managers and Quality Assurance staff attend a quarterly meeting with the vendor(s) to review task related reports.

The Consulting and Procurement unit provides agencies with an assigned Communications Systems Specialist 2 (CSS2). There are two Consulting and Procurement staff members in the JRTC Building in Chicago. The CSS2s work closely with the agency coordinators to consult and analyze their present and future telecommunications needs and design systems to meet those requirements in the most efficient and economical manner. The CSS2s are responsible for managing non-routine service requests. Procedures exist for the Consulting and Procurement unit tasks.

End User Computing (EUC)

EUC provides personal computer, printer, software, and peripheral support to Consolidated Agencies and CMS Supported Non-Consolidated Agencies and ensures resources support is provided in a consistent manner. Responsibilities of EUC include:

- Tier 2 Support
- Diagnoses and resolves break/fix incidents.

- New Installations
- Assesses, plans, and executes the installation of personal computers (desktop and laptop) and associated software.
- Add/Move/Change Services
- Assesses, plans, and executes the relocation of and/or modification to personal computer (desktop and laptop) resources.

EUC receives break/fix incident assignments via Remedy. The supervisor of the assigned EUC Unit assigns the incident to an EUC technician and creates tasks (if required). The technician executes applicable diagnostic and repair actions, updates the Remedy work log to reflect said actions, and resolves the Remedy incident record.

EUC receives installation service requests via Remedy. The supervisor of the assigned EUC Unit or designee executes applicable assessment, planning, task creation (if required), and EUC technician assignments for necessary installation services. The technician then updates the Remedy work log to reflect said actions, and closes the Remedy incident/task to reflect completion of the installation.

EUC receives change requests via Remedy. The supervisor of the assigned EUC Unit or designee executes the applicable assessment, creates tasks (if required), and EUC technician assignments for necessary modification and/or relocation services. The technician updates the Remedy work log to reflect said actions, and closes the Remedy change request to reflect the completion of the change.

EUC Incident, ESR, and task workload is monitored by the EUC Manager via Remedy sampling that is loaded into an Excel spreadsheet.

f. Recovery Services

The Bureau provides recovery services in order to minimize the risk of disrupted services or loss of resources. Recovery utilizes satellite locations and vendor contracted services.

The following contingency plans address restoration of various client environments:

- Continuity Methodology
- Recovery Activation Plan.

Each consolidated agency is responsible for coordinating recovery services with the Bureau.

The Bureau purchases exercise time annually to conduct a comprehensive recovery exercise at the vendor provided recovery location. Additional exercise opportunities are afforded to any state entity and are conducted at one of the Bureau’s satellite locations.

The Bureau maintains a Statewide Critical Application Listing based on information received from State agencies. State agencies are required to categorize, prioritize and define the recovery time objective for their applications as follows:

A recovery time objective (RTO) schema has been super imposed over the existing classification scheme – Categories 1 through 5. The schema is defined by three stages of RTO – Stage 0 (< 72 hours), Stage 1 (< 168 hours), and Stage 2 (long-term). Information for RTO is captured in the Business Reference Model. Agencies will continue to be required to complete and submit the Statewide Data Collection forms which include information on the Category 1 through 5 classification schemas, as well as the prioritization of the applications within the classification.

- Human Safety: (Category One) Resources that directly impact the lives and safety of Illinois citizens, including state employees.
- Welfare Human Service: (Category Two) Resources that directly impact the well being of Illinois citizens.
- Non-Welfare Human Service: (Category Three) A human service resource that indirectly impacts the welfare of Illinois citizens.
- Administrative State Functions & Processes: (Category Four) Resources that support the administration of state processes.
- Support of Specific Agency Functions & Processes: (Category Five) Resources related to the maintenance of a specific agency function or process.

In the event of a regional disaster, the Bureau will only recover Category One applications for those State agencies that have met the recovery requirements. State entities with these application types are required to participate in the comprehensive exercise if requested by the Bureau, conduct exercises annually at one of the Bureau's satellite facilities or through contracted services, and participate in the Statewide Data Collection which requires filing of recovery plans and exercise results.

Customers who have data residing on the Bureau's mainframe are responsible for backing the data up properly and indicating which data should be stored off-site. The Department utilizes a regional off-site storage facility for storage of critical information.

The Bureau has developed scripts and/or procedures for the recovery of operating system platforms. Recovery Services staff assist in updating and rehearsing these procedures when building the operating systems for customer recovery exercises.

The Bureau has submitted a Request for Proposal for posting to provide failover services for critical distributed applications. Until those services are in place, the Bureau will continue to maintain its current vendor contract for cold site recovery services at a remote center.

g. Internal Audit

The statewide Information Technology (IT) audit function is part of the Illinois Office of Internal Audit (IOIA), which addresses those entities under the Governor's jurisdiction. IT is addressed on a statewide basis, which reduces duplication of efforts and increase efficiencies. IOIA performs various types of IT audits including system development audits, application audits, special audits, and internal audits.

The Fiscal Control and Internal Auditing Act (30 ILCS 10/2003 (a) (3)) mandates IOIA review the design of major new electronic data processing systems and major modifications to those systems. IOIA has established a process for identifying major new systems and major changes to existing systems for system development audits to determine which systems development projects are major and require an audit.

IOIA has developed a database of system development projects for all agencies under the Governor. Periodically, IOIA contacts each agency to update the information and request a list of new planned projects. Based on the implementation date, IOIA performs a risk assessment for the project. The risk assessment consists of review of the following documentation, if applicable: project charter, RFP, system objectives, design documentation, cost benefit analysis, and other relevant documentation to gain an understanding of the project. Based on these documents, an interview with agency staff is conducted to gather and verify information to complete a risk matrix and risk questionnaire. Based on this information, the auditor, supervisor and manager make a determination as to whether the project is a major new system development or a major modification to a major system. Finally, it is reviewed by the Chief Internal Auditor and a letter is issued to the agency with IOIA's determination.

h. Personnel

The Workforce and Development and Logistics unit coordinates and facilitates internal personnel paperwork, workforce training, development and implementation, and workforce logistics for the Bureau. This unit uses several policies/procedures which allow for proper processing of transactions. Specifically, for HR related transactions we refer to and comply with: the Personnel Rules, the Personnel Code, the CMS Policy Manual, the union contracts, the pay plan, the personnel transactions manual and the alphabetic index.

The Workforce Training, Development, and Implementation unit works with the Bureau's fiscal office for approval of training requests. A hard copy training request form and procedure are used. When training involves travel, applicable travel rules and regulations are used for approval and reimbursement of training related travel expenses.

i. Vendor Management

Management of vendor agreements for infrastructure products and services is the responsibility of Acquisitions and Inventory Management (AIM).

Information specific to vendor agreements/contracts is entered and maintained in an Access database for reference and monitoring purposes.

Duties performed to manage Bureau contracts include:

- Entering product/service and terms and conditions information into an Access database for monitoring and tracking purposes;
- Acting as the liaison with vendors;
- Responding to questions from users and customers;
- Monitoring and reporting utilization and compliance;
- Performing contract and utilization reconciliations with vendors when appropriate;
- Providing contract and utilization information for internal, external, and vendor audits;
- Recommending changes to services, deliverables, terms and conditions;
- Performing periodic cost benefit analyses when appropriate; and
- Initiating renewal or rebid process when the contract nears expiration.

Documented procedures for reconciling desktop, mainframe and midrange software are outlined in the AIM/Vendor Management Guide located on a secure, limited access, SharePoint site. Upon receipt of software and/or licenses, staff enter licensure information into a shared Excel spreadsheet for tracking purposes. An inventory list is maintained and used to locate media and/or documentation in the library. All software media or documentation is filed in the software library, in a secured cabinet, by call name.

The activities involved in the administration of the software library include receiving and logging software information into tracking spreadsheet, maintaining the software physical inventory, verifying software requests against the Enterprise Architecture Technical Reference Model (TRM) database to ensure software is considered a standard enterprise infrastructure software, initiating Product Standardization Request for software not included in the TRM, verifying license availability to satisfy requests for installs, and/or initiating procurement of additional licenses.

j. Service Reporting and Agency Communication

Service Reporting

The Bureau conducts recurring trending analyses in order to measure and assess service performance. Areas included in these analyses include: Service Desk (CMC and CSC), Mainframe, Email, and Change Management. The Bureau prepares monthly and quarterly reports for each consolidated agency with key performance data. The reports are distributed via email to consolidated agency CIOs on a recurring basis and are made available to Bureau leadership via a shared network drive. The Service Reporting team continually reviews the performance data looking for data anomalies or changes in performance. Issues/problems are informally referred to the appropriate Bureau manager for a more thorough review. Additionally, members of the Bureau's leadership team meet periodically with the agency CIOs to review the monthly and quarterly performance reports and respond to agency questions. Informal follow-up occurs as necessary.

Agency Communications:

The Bureau utilizes multiple methods for communicating with its customers. The Bureau website, www.bccs.illinois.gov, serves as a central location for communicating available services including the Service Catalog, key contact information, forms and guides for requesting services, announcements/bulletins, and a variety of other Bureau information. Recurring CIO meetings provide a forum for the consolidated CIOs and Bureau leadership staff to exchange key information regarding initiatives and priorities. Meeting dates, locations, and agenda are sent to the consolidated agency CIOs via email. Periodically, the Bureau hosts topic specific meetings/forums with various customer interest groups. Additionally, Bureau staff meet informally with their consolidated agency counterparts to address agency specific initiatives, issues, and concerns. These meetings may occur face-to-face or via telephone as appropriate. This past year the Bureau introduced a customer-focused newsletter to provide another vehicle for sharing information with our customers. The newsletter is distributed to telecommunications and IT customers via email and is posted to the Bureau website.

2. Operations

a. Storage and Backup

Enterprise Storage and Backup (ESB) is responsible for the allocation, backup and removal of storage for the Bureau's mainframe systems. ESB procedures, located on the ESB SharePoint site, help ensure that z/OS cleanup, restores, and DASD adds and deletes are successfully completed. These procedures include the Weekly Daily Cleanups, DASD Addition Checklist, DASD Removal Checklist, DASD Return to Spare, DASDadd, DailyRMF, RMF2nd, RMFspec, RMFweek, and ADRDSSU Restore. Daily Remote Monitoring Facility (RMF) reports are run and sent to management for use in measuring system resources and mainframe performance such as CPU utilization.

z/OS Backups are performed on the mainframes' systems data. System data is backed up daily and weekly with the weekly copies sent to the regional vault. Backups are also performed by HSM. These backups are controlled by the SMS routines and are set by the customer at allocation time. When the customer allocates a new file, a management class is assigned which determines how long the data is kept.

z/OS Restores are performed at the request of mainframe technicians via Remedy. ESB restores the data, updates the Remedy work log, and closes the record to reflect said actions.

ESB manages both SMS Pools and Private Pools for the mainframe systems. System automation notifies ESB technicians when storage falls below a pre-determined threshold. Technicians migrate data, delete data, or add additional disk space to replenish pool space.

b. Enterprise Production Operations Services

Unless specified below, an agency's legacy procedure remains in effect and is the responsibility of that agency.

The Enterprise Production Operations Services (EPOS) area is made up of four functional areas: Command Center, Input/Output (I/O) Control, Production Control, and Library Services.

<u>Command Center Operations</u>

The Command Center supports continuous monitoring and operation of the Bureau's computing resources to ensure availability, performance, and response necessary to sustain customer business demands. The Command Center operates 24 hours a day, 7 days a week, 365 days a year. The Command Center utilizes the Information Management System (INFO) to coordinate and oversee implementation of changes to the computing environment. Remedy is used to record and monitor incident resolution. The Command Center Data Processing Guide is utilized as a reference for operational tasks. The Focal application is used to assist Command Center in monitoring and maintaining system availability in an efficient and consistent manner. Daily Shift Reports are generated and distributed by the Command Center and are used to document outages/issues. Shift Change Checklists are utilized by the Command Center to ensure consistent verification of system availability. SYSLOG is utilized as a tool to reference system activity.

<u>Input/Output (I/O) Control</u>

The Input side monitors all production jobs the departments of Central Management Services (CMS), Human Services (DHS), Health and Family Services (HFS), Public Health (DPH), Commerce and Economic Opportunity (DCEO), Transportation (DOT), and the Environmental Protection Agency (EPA). Collectively, these can be referred to as I/O-managed agencies.

I/O-managed agency production jobs that do not complete successfully are examined for the cause of their abnormal termination (Abend) and are repaired if possible by the technicians on duty. If the technicians are unable to affect the proper repairs, Production Control or Applications personnel are contacted via a Job Call List. This Call List is used to contact the necessary personnel to attain the information necessary to resolve the abnormal termination. After the problem has been resolved, I/O will reinitiate the process and monitor the job until such time as the job comes to a successful completion. Automated scheduling is used at most locations and monitors or manipulates job streams as necessary to ensure proper production processing.

I/O instructions are embedded within JCL streams as well as recorded in hard copy documentation maintained by Production Control organized by production job. System logs, hardcopy flows, and schedules are used for informational purposes. I/O daily shift reports that contain abends, restores, and corrections to production jobs are created and emailed to each legacy agency.

The Output section is responsible for printing and distribution of all documents and reports generated as a result of processing jobs for the departments mentioned above. Hardware includes high-speed Xerox laser printer types DP180 and DP65, and impact printer type IBM6262. Print queues are manipulated for resource management purposes. Backups of forms, fonts, logos, and signatures, stored on the printers, are performed and sent offsite. Reprint needs are reported to and completed by Production Control or Input personnel. Service personnel are contacted for hardware problems. Printer usage is logged and monthly reports are produced. Monthly job performance reports are produced and submitted to management. Inventory is monitored, orders are created and tracked.

Physical control over the distribution of printed material picked up at the Harris Facility is explained in written correspondence to each consolidated agency. This correspondence outlines how individuals picking up a report must identify themselves and state which report(s) they are to receive, be listed in the "Focal" system which contains a list of individuals authorized to pick up reports from I/O Control, and sign a report manifest indicating receipt of the correct report(s).

Production Control

The Production Control Section of EPOS ensures that production processing activities are documented and executed in accordance with approved schedules to normal completion. Standards and naming conventions exist for job acceptance as documented in each agency's standards manual.

Proc Acceptance - Any new or changed job or system that is presented for acceptance by CMS, DHS, HFS, DPH or EPA to be placed into the production environment must first pass through the Production Control area. The documentation is checked for adherence to production standards, naming conventions, and run procedures.

Job setup and processing - All jobs that are processed in the production environment, for CMS, DHS, DCEO, HFS, DPH, or EPA whether they run through CA-Scheduler or are manually submitted must be setup and processed by Production Control. This includes the initial setting up/coding of the criteria according to job specs for all new jobs (procs) at the job coding level within CA-Scheduler, as well as setting up the schedules at the schedule level. Department security software ensures only authorized individuals are allowed to submit production processing.

Abend Resolution - When a job abnormally terminates due to a cart problem or a problem with how the job was setup for processing, production control staff correct the problem and restart the job. When it is a problem with the job itself, the application staff corrects the problem. After the application staff fixes the problem, production control is notified and they resubmit the job. All production abends are recorded listing the cause, who was contacted, and when the job was corrected. This documentation is provided daily to all Production Control, I/O, and Library Services staff, as well as to each legacy agency being monitored.

Automatic Distribution and on-line viewing of reports –The Department uses an automated tool that allows for on-line viewing of reports. All jobs that produce output, whether it is to be printed or to be viewed on-line are setup by staff in the Reporting unit of the Production Control Section. Access to the on-line viewing tool is controlled by system security software access controls.

Library Services

Library Services consists of four functional units: CCF Tape Library, CCF Tape Media, Library Support, and Tape Administration.

CCF TAPE LIBRARY:

The Tape Library is located at the Central Computer Facility and is responsible for media storage and movement. This unit provides 24 X 5 (Monday thru Friday) services fulfilling customer requests and ensuring security and tracking of all mainframe cartridges. Tape Library is responsible for all tape orders, initializing, labeling, degaussing, or destruction. The "Library Services Vault Transmittal Procedures" outlines the procedures to be followed during the movement of media. This includes transportation of media to and from the secured off site vault. Security and Service Delivery staff and Tape Librarians are responsible for confirming that individuals are authorized to deliver or remove media. A Security and Service Delivery staff person and a Tape Librarian verify that the triplicate Media Transmittal/Services Authorization Request forms are correct, signed, and retain a copy. All media is identified with unique tracking alpha numeric identification numbers (volume serial number). The Tape Management System (TMS) is utilized to track and record the location of media. Carts not listed in TMS are transient carts recorded in a database called the Transient Tape System (TTS). The media in and out transmittals are used in the same manner for these types of tapes. Twice a year, Security and Service Delivery staff send user agencies Security Authorization List, an Information Management System Authorization List, and a Tape Diskette Authorization List, which are to be updated.

CCF TAPE MEDIA:
CCF Tape Media staff performs tape drive monitoring functions, drive maintenance, tape mounting, dismounting, and file interface with the Automated Cartridge System (ACS) to satisfy system and sub-system requests. Services are provided 24 X 7 to fulfill customer requests. The CCF Tape Media Guide is utilized for reference in performing job functions.

LIBRARY SUPPORT:
Library Support staff are responsible for migrating test environments to production libraries. Production libraries are protected by security software to allow only updates or edits to be performed by Library Support. Backups associated with all production libraries are performed by Library Support and will have designated backups sent to and from vault. All moves are performed with documentation and verification.

TAPE ADMINISTRATION
For CMS, DHS, HFS, and DOT, Tape Administration staff document tape activities on the daily TGS report and a manually produced report. Tape Administration staff manages technical duties in conjunction with the development and control of the Tape Management System (TMS) and Tape Generating System (TGS). They also recommend and implement tape control features, project tape media usage, manage the resolution of tape control features, tape media listings and reports for the various agencies.

3. Change Control

The Department's change management services are currently facilitated through separate systems based on processing platform and/or technology area.

Mainframe Platform: All mainframe changes are tracked in the Information Management System (INFOMAN) and governed by the CMS Change Management Policy and the Department's Information Management System guidelines.

Network Platform: Network Operations, LAN Services, and Enterprise Network Support changes are tracked in the Remedy Change module governed by the CMS Change Management Policy and Remedy Change Guide. In parallel to this process, Network Operations and Enterprise Network Support changes are also tracked in the ICN Remedy Trouble Ticket module. The CMS/ICN WAN Change Management process is utilized by Network Services and Field Operations teams responsible for making network related changes, and follows the CMS Change Management Policy.

Regardless of platform, the below described path is followed for control of change:

- Changes are initiated by the Shared Services Technician or Manager as a result of an Enterprise Service Request (ESR), internal work assignment, or a configuration change.
- The Shared Services Technician or Manager identifies the changes to be made and generates a change request.
- Change requests are assessed for content and readiness.

- Changes are approved and appropriate parties are notified based on change impact.
- Changes are implemented.
- Changes are reviewed.

4. Security Administration

The Department's security posture is comprised of compliance and auditing functions that include corrective action planning, security assessments, security awareness promotion, policy development, and continuity of operation planning.

Corrective action plans that enhance the overall security posture of the Department are developed by Risk Management and are based on recommendations generated by external audit reviews and internal security assessments.

Security assessments are conducted and include vulnerability scans, penetration testing, and patch level review to identify weaknesses. The Technical Safeguard Unit Security Audit Procedures Rules of Engagement document, located on a secure, shared network drive, outlines the steps to follow when conducting these assessments.

Security awareness is provided through the state's Enterprise web which includes a link to the IT Risk Management site (http://intra.state.il.us/it-risk/default.htm) that provides security-related news releases, tips, security posters, and other guidelines.

Current approved security policies include Change Management, Data Breach, Laptop Data Encryption, Midrange Backup, and Resource Access. These policies have been developed based on information supplied at informal meetings with Bureau staff, from known operational practices, and from principles outlined in industry best practices. Prior to submission to the Deputy Director, policies are reviewed by the Bureau's Chief Security Officer and the Bureau's Deputy General Counsel. Policies are published by posting to the appropriate repository dependent upon the sensitivity of the material and the targeted audience. The Information Technology Security Policy, Chapter 4 Section 3 of the Department Policy Manual remains in effect.

Continuity of Operations Plan (COOP) information, based on a COOP checklist, has been collected and submitted to the Department's Emergency Management Coordinator in the ongoing development of the Department Continuity of Operations Plan (COOP).

PKI

The State of Illinois Public Key Infrastructure (PKI) is required to have a PKI compliance audit conducted on the Illinois Root certification authority on an annual basis. This is to validate the operational compliancy of the system. The most recent compliance audit is located at http://www.illinois.gov/pki/default.cfm

5. Physical Security

The Department protects information system hardware and other assets through the use of access control and video surveillance.

Access control includes limiting physical entry into buildings and/or locations within a building and uses Access Cards, Badges, and/or Pin Codes to control entry. Access Cards and PIN Codes are issued by the Physical Security Coordinator to Department personnel based on business need and job responsibility. Badges are issued by contracted Security Guards to visitors for temporary entry into a building.

The Bureau Physical Security Coordinator processes emailed access requests from only designated authorities as identified in the Approval Authorization Matrix and Badge Production Matrix.

The Hirsch/Velocity (H/V) system is used to create and track Access Cards. Creation of an Access Card requires identity authentication based on generally accepted identification sources such as a valid driver's license, State ID card, or U.S. passport. A picture of the individual is taken and stored in the H/V system along with credentialing source information. The H/V System Administrator's Manual contains instructions to create the physical card or badge.

Access Cards are FIPS 201-1 compliant and contain text that outlines cardholder responsibilities as well as instructions on what to do if a lost badge is found. Access Cards contain the name and photo of the "owner", an anti-counterfeit feature, and expiration date. Once the Physical Security Coordinator is notified of employee separation or other circumstance for disabling access, card access is disabled by making the appropriate entry into the H/V system. Recovery of a separated employee's Access Card is the responsibility of the supervisor per Chapter 2, Section 13 of the Department's Policy Manual.

For those buildings staffed with 24/7 security guard protection, Badges are issued to visitors and to employees who forget their assigned Access Card. Those issued a Badge sign the Building Admittance Register recording their name and Badge ID. This is used as a log to track who is in the building. Security Guards have been instructed to inventory Badges at the start of each shift to ensure accountability.

For those buildings not staffed with 24/7 security guard protection, each entry door remains locked. Only a limited number of people from the inside may release the locked door. Audio and visual capabilities allow verification of the person entering.

The H/V system, Access Cards, Badges, and video surveillance are used to limit or monitor physical entry into the Central Computer Facility, Communications Building, the Business Services Building, the BCCS Warehouse, and the Harris Facility.

Physical security at the Harris Facility is a joint effort between the Department of Human Services (DHS) and the Department's Bureau of Property Management. Access Card and Badge issuance to non-Departmental areas is the responsibility of DHS. Physical security controls protecting the Department's assets housed at the Harris Facility include:

- Security guards in the front entry way;
- Video cameras strategically located inside and outside the building;
- Proximity card readers requiring an active Access Card to allow entry; and
- Limited access, brightly colored badges for use by individuals entering the building to pick up printed output from the I/O Control area.

The H/V system records and logs the use of Access Cards. Reports can be produced to list who has access to what buildings and locations as well as which credential was used where and when. Reports are generated upon request by the Resource Custodian or by Personnel.

In addition, application of employee pass-back functionality and absentee limits help control physical access to facilities.

Networked video cameras monitor exterior doors and sensitive interior entrances. Security Guards as well as the Bureau Physical Security Coordinator have remote view capability for all networked cameras.

The Bureau of Property Management (BOPM) maintains fire suppression and detection systems on the third floor of the Central Computer Facility, at the Communications Building, and at the Business Services Building. BOPM is also responsible for the issuing and maintenance of real property keys. Although the Bureau may provide information to BOPM regarding key provisioning, BOPM has the final authority and responsibility for real property keys. BOPM also manages a contract for security guard services at select locations. Security guard services are based on contract documented requirements (general orders), post orders, and special instructions. These special instructions are communicated via email from the facility manager to the security guards and are then included in the Pass Down Book. Fundamental activities of security guards include but may not be limited to access control, incident reporting, and perimeter patrol. In addition, BOPM contracts with janitorial services to perform duties at these facilities on a daily, weekly, and/or monthly basis. The contracts outline duties and timeframes. BOPM is responsible for ensuring that background checks and training are conducted for each janitorial employee.

In order to mitigate the risk of a power failure, the Central Computer Facility is supplied by two different sources and is equipped with an uninterruptible power supply (UPS). Within an allotted time the Department's generators will engage. The Department has in place a service contract for the UPS to provide routine preventive maintenance and remedial services as required.

6. System Software: Mainframe

z/OS

The primary operating system at the Department's Central Computer Facility is Zero Downtime Operating System (z/OS). z/OS is a complex operating system used on mainframes and functions as the system software that controls the initiation and processing of work within the computer. The System Management Facility (SMF) records the activity within the operating system. Some of the subsystems that run on z/OS are CICS, DB2, IMS, RACF, MQ series, NEON, SMS, HSM, TSM, JES, CA-scheduler, Mobius, HSC, TMS, etc. The agency security software administrator must submit a request to the CMS security software staff if a user ID needs to have TSO access on the mainframe. Security software and system options are implemented to secure libraries, and to protect resources and data.

z/VM

The Department's secondary operating system utilized at the Central Computer Facility is Zero Downtime Virtual Machine (z/VM). z/VM is time-sharing, interactive, multi-programming operating system for IBM mainframes. The major subsystem that is supported in z/VM is NOMAD. The agency security software administrator must request and obtain a VM User ID from the z/VM staff. Agencies are assigned user IDs with the most restrictive security rights. The z/VM directory is restricted, which contains information regarding user IDs, mini-disk size and location, and operating functions. Security software and system options are implemented to secure libraries, and to protect resources and data.

CICS

The Customer Information Control System (CICS) is a software product that enables online transaction processing. CICS allows numerous transaction types, entered from multiple terminals, to be processed concurrently by customer written application programs. CICS acts as an interface between the operating system and application programs. The Department offers three different levels of CICS support for customers, described as follows:

- Level One: The Department supports only the CICS software. The customer is responsible for all security for the customer owned CICS regions.
- Level Two: The Department supports the CICS software, and maintains CICS System Definition File (CSD)/table definitions for the customer. The customer supplies the definitions to the Department and controls the application support. The Department and the customer owning agency share security responsibilities.
- Level Three: The Department supports the CICS software, maintains CSD/table definitions, and supports both CICS and the application software for the agency. The Department is also responsible for security for these regions.

Production regions are segregated from test and development regions to restrict access, based upon the various needs for each type of region. Restricted access to sensitive CICS transactions is established over production regions. Test regions have fewer access restrictions. Test regions allow programmers to test and debug against non-production files.

Security software and system options are implemented to secure libraries, and to protect resources and data.

DB2

DataBase 2 (DB2) is a relational database management system for z/OS environments, which the Department makes available to customers. The Department has established ten+ subsystems at the Central Computer Facility. The Department has assigned staff to monitor the performance and problems of DB2. The DB2 staff is also responsible for software installation, maintenance and security. All customers who access DB2 are required to have a security software ID and password. The customer must authenticate to the security software first. If the customer authenticates, DB2 allows access. DB2 internal security verifies access rights to specific data. The Department authorizes one user ID at each agency to coordinate the use of DB2 within the agency. This user ID allows each agency to create its own authority. The DB2 Software Support Group will monitor specific application problems when customers call. System performance is monitored on a continuous basis. The Department's Information Management System is utilized to report and document problems.

IMS

Information Management System (IMS), which is an online database software subsystem, is used as the control architecture under which online database system applications process. An IMS system is capable of running many different applications within a single definition of one or more "Message Processing Region" and one "Control Region". The IMS applications can access IMS, DB2 and CICS data files. Customers control their own TIMS and GIMS RACF definitions. Currently, there are four production IMS regions with 10+ testing regions. Security software and system options are implemented to secure libraries, and to protect resources and data.

Security Software

The Department utilizes security software to control access and protect resources. The security software is the primary tool for controlling and monitoring access to the Department's computer resources. A user ID is used to identify the client along with a password to verify the client's identity. The Department maintains a log of all access attempts, which is used to monitor unauthorized access attempts and identify areas of weakness. Clients are responsible for protecting their program and data files. The Department has appointed staff with primary responsibility for the implementation and administration of the security software. The Department has a procedure in place for the monitoring of security violations. The CMS Data Security Administrator reviews violations with CCF violation reports being distributed to staff for which they must be signed and returned with an explanation. The agency security software administrators have the capability of producing the reports for their agency. System options and parameters are implemented to protect data and resources. Written procedures exist for the managing and maintenance of the security software.

7. Telecommunications/Network Services

The Bureau provides telecommunications/network services to a variety of agency, boards and commissions, educational institutions, and other governmental and non-profit entities. Bureau staff monitor these systems to confirm that devices and systems are properly, installed, configured, and maintained. Management reviews performance and capacity of the network services being provided.

a. Network Services

Network Services is responsible for management and oversight of the Illinois Century Network (ICN), Local Area Networking (LAN) for select agencies, the Illinois Wireless Information Network, and all engineering responsibilities related to State of Illinois telecommunications services. The Division consists of three teams which includes Network Operations, LAN Services, and Enterprise Network Support.

The ICN obtains public Internet services from the following Internet providers: Sprint; Level 3; ATT; Qwest. Multi-point and redundant firewall hardware is maintained through Access Control Lists (ACL's) at the head ends of the MPLS VPN/VRF network to protect the agency networks. Additionally, firewall services are provided (both hardware and configuration) for each agency to protect their networks from each other.

Network Services - Network Operations

Network Operations is responsible for installing, maintaining and managing the ICN Backbone including backbone circuits, egress circuits, routers, firewalls, switches, fifteen Point of Presence (POP) sites, WAN monitoring tools and WAN services. Solarwinds Orion is used to manage and monitor the ICN Backbone. Routers authenticate authorized individuals for device configuration and maintenance.

Network Operations staff are responsible for the backbone and POP site management and support. Support includes: delivery, removal and inventory of equipment; installation, maintenance and documentation of all POP site equipment; test and turn-up of all backbone and egress circuits; installation and management of POP sites. Network Operations staff are responsible for installing, customizing, maintaining and supporting WAN management and monitoring. Solarwinds Orion is used to manage and monitor the ICN Backbone. Additionally, Network Operations is responsible for WAN Services including DNS, registrar for the il.us domain, the educational content filtering solution, as well as the new state agency enterprise filtering solution, and IP Video. WAN services support includes installation, configuration, maintenance and support.

Network Services - LAN Services

LAN Services is responsible for entering rules into the firewalls and monitoring security violations. Security logs are sent to the Mainframe and violations are reported by alarms and reports sent via the Mainframe. These reports are sent to members of LAN services and the mainframe group. They are reviewed for performance issues and/or intrusion prevention.

Additionally, the LAN Networking Services group is responsible for installation, configuration and support of the Department's LAN networking infrastructure including: switches, routers, hubs, firewalls, wireless switches and inside cabling. LAN Services maintain these configuration standards for LAN infrastructure devices. These standards are implemented on newly deployed equipment.

Network Services – Enterprise Network Support

Enterprise Network Support is responsible for design and support of State agency network access. Responsibilities include installation and support of access routers, WAN switches, VOIP, video conferencing, fiber, DNS, and Internet. Enterprise Network Support also performs Tier 3 technical support for the CMC as well as for state agencies.

Enterprise Network Support provides customer consultation, access and distribution router configuration, ongoing maintenance, head-end router installations/troubleshooting, making equipment and connectivity recommendations, performing equipment installation/recovery at state agency sites in Springfield and surrounding area, and the provisioning for new circuits, moves and changes. ENS utilizes established architectural and methodologies standards such as the Basic MPLS Connectivity Model to serve as a foundation for design and support of State Agency network access. Routers authenticate authorized individuals for device configuration and maintenance.

Enterprise Network Support is responsible for the installation, maintenance, and protection of the MAN fiber Network. Responsibilities include overseeing installation of fiber facilities and outside plant construction projects, fiber plant locating services, and maintenance of accurate fiber records. ENS is a member of the Monitor Illinois One Call (J.U.L.I.E.) dig notification system in order to protect fiber assets. The Monitor Illinois One Call (J.U.L.I.E.) group forwards dig notifications to a Department email distribution list. ENS screens the notifications for those requiring a dispatch. The Customer Solutions Center (CSC) opens a CMS Remedy Helpdesk ticket for each dispatch.

Backup and Recovery:

Network Operations and Enterprise Network Support backup firewall, router, and switch configurations via two servers. The servers are backed up to tape weekly and when a major change occurs. Tapes are then rotated off-site.

Configuration Standards:

Network Services has established standard network configuration templates for core, distribution, access routers, and LAN routers and switches.

Architectural Standards and Methodologies:

Established standards currently include: POP Site Power Strategy, Basic MPLS

Connectivity Model, and Common Connection Methodology for LAN, and Quality of Service. Network Services staff conducts, coordinates, and serves as lead(s) on feasibility studies and projects involving wide-area network systems.

b. IWIN

The Department and Illinois State Police (ISP) have coordinated efforts to provide the Illinois Wireless Information Network (IWIN), a wireless wide area data network using Code Division Multiple Access (CDMA). The Department administrates the IWIN network and ISP provides the connection to the Law Enforcement Agencies Data System (LEADS), National Crime Information Center (NCIC), Secretary of State, National Law Enforcement Telecommunications System (NLETS), and Criminal History Record Information (CHRI) that the network utilizes to provide information to IWIN users.

The "Illinois Statewide Policy Manual," located on the Internet, outlines the responsibilities for the Department, ISP, local agency IWIN coordinator and the IWIN user, as well as appropriate usage, necessary certifications to obtain IWIN access and Motorola client functions.

Transmissions are sent from the users' Mobile Data Computer (MDC), equipped with the client software Premier MDC, to the nearest cellular tower equipped with CDMA equipment. The Department has a contract with Verizon Wireless (Verizon) to provide data connectivity throughout the State, as well as with Motorola to provide the software utilized by the IWIN network. Once the cellular tower has received the transmission from the user's MDC, the transmission is then forwarded to a Verizon -owned and -operated messaging switch. From the messaging switch, the transmission is forwarded to one of the Department's redundant Premier MDC Servers and then to the Department's network for access to the appropriate data. Redundant routers, maintained by the Department, connect Premier MDC Servers to the Verizon Network.

The IWIN network infrastructure utilizes redundant routers which connect servers to the provider network. Routers authenticate authorized individuals for device configuration and maintenance.

The IWIN infrastructure is comprised of a multi-layer security approach. This approach secures access to the infrastructure from the IWIN user community by utilizing strong authentication such as user IDs, passwords, and unit IDs.

c. Field Operations

Field Operations, within the Bureau's Customer and Account Management unit, consists of a decentralized staff operating out of nine statewide Regional Technology Center (RTC) offices (see http://www.illinois.net/rtc/default.htm for a listing of site staff and office locations). The RTCs are strategically placed to provide close proximity to the constituents they serve. Field Operations staff includes a Regional Manager, four Supervisors, twenty-one Network Engineers, and four Administrative Assistants.

Field Operations serves two primary constituent groups- 1) Legacy Illinois Century Network (ICN) constituents of K12 schools, community colleges, universities, museums, libraries, municipalities, and other not-for-profit groups, and 2) State agencies.

Field Operations utilizes two versions of Remedy for constituent connectivity provisioning. Agency provisioning utilizes a Bureau version of Remedy. Other constituent and non-agency provisioning and trouble ticketing utilizes ICN Remedy.
Field Operations is responsible for the following:

- Services (www.illinois.net/services/default.htm#tech contains a listing of services)
  - Consultation – help constituents design efficient and cost effective network connectivity, identify circuit options, and identify appropriate equipment.
  - Filtering – perform sales and ongoing support for content filtering software designed to allow constituents to restrict access to inappropriate content on the Internet. Support includes router configurations, setting up user accounts, adding IP addresses, providing end user training, and troubleshooting problems. Primary constituents using this product include municipalities and K12 education sites.
  - IP Video – consultation, installation and troubleshooting IP based video conferencing systems.
  - Monitoring/Analysis – monitor constituent connections for up/down status and provide constituent access to utilization data for their circuits.
  - Configuration services – multicast and quality of service (QoS) configurations for specific applications including video streaming, IP voice and video, and preference cueing.
  - Technical Support – support and dispatch for circuits, equipment, and services.
  - IP Addressing – maintain and assign Internet Protocol (IP) addresses.
  - DNS – configure and maintain Domain Name Service (DNS) for domain name resolution services.
- Provisioning
  - Circuit orders – place orders for circuits with telecommunication companies (telcos) and maintain a database (ICN Remedy of all circuits connected to the ICN for both legacy ICN constituent connections and State Agency connections. Track installation dates and keep constituents notified of status via email and phone. Process Moves/Adds and Changes (MAC) to existing services. CMS Remedy is used by Field Operations staff for processing work orders initiated by the Customer Service Center (CSC).
  - Installations – visit constituent sites, install and configure equipment, connect and test circuits. Track and record inventory.
- Support
  - Technical Support – Provide Tier 2 and 3 level support for constituent connections, equipment and services. Perform or arrange for repairs, replacements, upgrades, configuration changes and provide information. Work is

documented and tracked using the trouble ticketing module of ICN Remedy and via Email.

  - Maintenance – Provide on site emergency repair and regular maintenance and equipment installation at network backbone points of presence (POP sites).
  - Cost Recovery – Provide quotes, bandwidth allocations and adjustments, vendor pricing verifications and invoicing support.

Policies, Procedures and Documentation

- Network Services' SharePoint is used for housing internal policy and procedural documentation as well as white papers, project outlines and progress reports, contact lists and technical resources.
- Shared servers are used to store non-agency constituent documents including telco and equipment quotes, completed applications, and participation agreements.
- Illinois.net (www.illinois.net) is used to house all non-agency forms and information distributed to constituents, announcements of new services, conferences and policy meetings, costs and bandwidth allocations, instructions on how to access services, and historical data about the network and associated committees. Agency customer information is housed at http://www.cms.il.gov/telecom/default.htm.

d. LAN Application Development / Web Services

LAN Application Development:

Responsibilities of LAN Development include the development of custom application software on microcomputers, local area networks (LANs), and Internet, Intranet, and mainframe client server environments

The section follows the set standards and methodology for rapid application development maintained by the EBAS Quality Assurance Section. Access to the data for both the users and support staff follows the Active Directory/ Novell login process required by each platform or tool. Tracking the status of requests is performed using a local Access database and/or the Service Request Registration System (SRRS). For projects that are classified as enhancements or new development, QA requires a checklist of deliverables to be created and delivered. QA reviews the required documents and time-stamp approves each required task as complete on their checklist tracking system.

Prior to being placed into production, all updates and modifications are reviewed and approved via email by the owner. Once approval is obtained, the developer requests the supervisor to move the changes into production. The supervisor copies the application onto the production drive and then re-tests the application to verify that the application works in the production environment.

Web Services

The Bureau provides web services that enable more than thirty state agencies to communicate their specific and broadly related information to both public and private sectors. This is accomplished through development and continued support of a variety of internal and external web applications and high profile web sites as well as enterprise-wide standardization and guidance to the agencies. Web Services supports (which includes creation, implementation, and on-going update and maintenance) both static and dynamic web sites. Static web sites consist of agency specific documentation, offerings, programs, etc., and applicable linking to other supporting information (including internal, external, and other public arenas). Dynamic web sites consist of interactive, data-driven web-based applications, which allow staff members from state agencies to perform various functions and reporting efficiently and securely (i.e. using public key infrastructure, PKI) via the Internet.

Websites and web applications provide anywhere, anytime access. Web Services also takes direct responsibility for website maintenance if an agency requests. Websites maintained by Web Services utilize the Official State Web Templates developed and administered by Web Services. Web sites are reviewed by the Department's Illinois Office of Information and Communication for compliance with the Illinois Web Accessibility Standards (IWAS), which are based on the Federal "Section 508" and World Wide Web Consortium accessibility guidelines. Additionally, in an effort to address the needs of all users, prior to implementation, web applications are thoroughly reviewed for IWAS compliance. Prior to being placed into production, all updates and modifications are reviewed and approved by the owner. Once approval is obtained, the developer requests that their supervisor move the changes into production. This is accomplished by an email sent by the Web Services supervisor to the developer to tell them the content owner has approved the final content change. The web developer then replies back to one of the Web Services supervisors requesting that it be moved into production.

Web Services Third Level Domain Registration application (Domain Name Service/Server (DNS) /Universal Resource Locator (URL)) provides both a user interface for agencies, counties, municipalities and other authorized organizations to request an illinois.gov domain as well as an administrative component for Web Services staff to review and approve these requests.

e. PIM

PIM provides a centralized and consolidated platform that facilitates a statewide common architecture for managing email.

Services include: account provisioning, calendaring, supporting user interaction with messaging application, monitoring/reporting service levels, technical support and problem resolution. PIM applications include limited FAX service, Mobile Messaging, Anti-Virus, Anti-Spam and Content Filtering, and directory support for State of Illinois email.

A secure, limited access SharePoint site is established that contains instructions for PIM staff on how to manage email accounts. The following procedural documents are stored on this site; a migration PowerPoint presentation (Towards a Common Standard - Email Migration for the State of Illinois) outlining the migration approach, migration responsibility schedules for agencies converted, and a migration instruction template. Meeting minutes and status reports from completed migrations are also available on this site.

8. Common Systems

The Department of Central Management Services, Bureau of Communications and Computer Services (Bureau) has developed four applications that are used by multiple State agencies. The applications, known as the "common systems," are:

- Accounting Information System (AIS)
- Central Inventory System (CIS)
- Central Payroll System (CPS)
- Central Time and Attendance System (CTAS).

The common systems run on the department's mainframe, processing millions of transactions each month. Each Common System is available for use during business hours and on a limited basis on the weekends.

Each Common System is secured using security software, in addition to internal security requirements. Users must have an authorized ID and password to gain access. Assignment and authorization of access rights is the responsibility of the user agency. Once access has been gained to the operating system, users must have a separate application user ID and password to gain access.

Changes to the common systems are controlled through the Application System Development (now referred to Enterprise Business Applications) Methodology. Changes are initiated through the use of a Service Request Form. The changes are approved and tested before implementation into the production environment. The Library Control Group will then move the change into production.

The Common Systems are backed up daily, weekly, and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.

Project Administration includes requirements gathering, drafting charters, facilitating and organizing project management activities, tracking and documenting issues and action items, project status reporting, maintaining task and resource plans, documenting work processes, etc.

EBAS Quality Assurance applies to all common systems.

a. **AIS**

AIS functions as an automated expenditure control and invoice/voucher processing system. AIS, in processing invoices, allocates invoice amounts into sub accounts; groups invoices, according to the Comptroller's Statewide Accounting Management System (SAMS) procedures, for the preparation of vouchers; and allows users to track cost centers. AIS interfaces with the Illinois Governmental Purchasing System (IGPS), the Accounts Receivable Posting System (ARPS), the Central Inventory System (CIS) and the Central Payroll System (CPS).

The AIS User Manual, which is located on the State's Enterprise Web Server (Intranet), provides guidance on the use of the Accounting Information System.

AIS transactions are entered online in a real-time environment, with the ability to batch transactions for processing at a later date. AIS was developed with edits that force correction of errors and completion of critical fields before a transaction is accepted. All data entry is performed by user agencies and is the responsibility of user agencies.

A disaster recovery plan for AIS provides guidelines for restoration.

AIS provides various on-line and batch reports to assist in the balance of transactions. A complete listing of the various reports is maintained in the AIS Users Manual. Retention of the various reports is the responsibility of the user agency.

b. **CIS**

CIS is an online real time system; therefore, inventory data is updated immediately to reflect the transactions entered. CIS has the ability to utilize an optical scanner to read bar code labels during a physical inventory. CIS allows user agencies to maintain records of inventory and to comply with the Department's Property Control Division's rules of reporting and processing. CIS has an interface with AIS.

The Department has developed a user manual, the CIS User Manual, which is available from the Department. The manual provides guidance to the user when utilizing the various functions.

Data is entered online by user agencies. CIS has several edit checks to alert users of errors. Errors must be corrected before the transaction is accepted. The Department generates a Location Balance Report nightly to determine whether transactions processed correctly. Additional reports are available to users. The accuracy and reconciliation of data is the responsibility of the user agency.

c. **CPS**

CPS was designed to provide assistance in preparing payrolls for state agencies. The system will accommodate agencies which are governed by the Rules of the Personnel Code and agencies that are exempt from the Personnel Code (Non-Code Agencies). The payroll system is a tool to be used by qualified personnel with SAMS and payroll procedure knowledge. The User Manual is a guideline for using the payroll system and is not intended to provide SAMS or payroll rules and regulations. Guidelines for payrolls are set forth in the current version of SAMS and the Illinois Compiled Statutes. CPS enables state agencies to maintain automated pay records and provide a file that is submitted to the Comptroller's Office for the production of payroll warrants. CPS has an interface with AIS and CTAS.

CPS has an edit feature designed to reject invalid information entered into the system. When invalid data has been entered into the system, an error message will appear at the top of the screen and the field that is in error will be highlighted. The system will not accept the entry until the error has been corrected or deleted. The Department has procedures in place to handle errors that occur during processing.

The payroll vouchers/reports that are produced from the batch process are printed by the Department's Production Operations Services and delivered to Central Payroll. Central Payroll separates the vouchers/reports for each agency to pickup or to be delivered by Mail Messenger, UPS, or Fed Ex. Each agency must fill out an informational sheet provided by Central Payroll that contains the list of individuals that are approved to pick up payroll related materials. This list is reviewed periodically by the user agencies. The retention of these payroll vouchers/reports is the responsibility of the user agency.

Disaster Recovery guidance is included in the User Manual.

d. CTAS

CTAS is an online system used to maintain "available benefit time". Additionally, CTAS allows user agencies to monitor whether usage of time is in accordance with state rules. CTAS provides for attendance information to be recorded using either the positive or exception methods. CTAS interfaces with the Central Payroll System.

Data is entered online by user agencies. CTAS has edit checks to alert users of errors. Transactions with errors will be rejected. CTAS provides online and batch reports that user agencies may use for reconciliation purposes. During the "close" process, CTAS generates error reports, reconciliation reports, and file maintenance activity reports. All transactions must be reconciled before the "close" process can be finalized. The accuracy and reconciliation of data is the responsibility of the user agency. The CTAS User Manual provides guidance to the user when utilizing the various functions.

Recovery procedures for CTAS provide guidelines for restoration.

SERVICE AUDITOR
DESCRIPTION OF TESTS AND OPERATING EFFECTIVENESS

We reviewed or confirmed data processing general and application controls at the Department. Using the Department's Description of Controls as the foundation for our review, we performed tests to determine compliance with policies and procedures, conducted interviews, performed observations, and identified specific control objectives and procedures we considered necessary in the circumstances to evaluate the controls.

The results of our review are included in the General Controls (pages 43 through 159) and Application Controls (pages 161 through 183) sections of this report.

This Page Intentionally Left Blank

BUREAU ORGANIZATION

EXISTING ENVIRONMENT

Department Description of Control: The Department of Central Management Services' (Department) Bureau of Communication and Computer Services (Bureau) is statutorily mandated to provide "use of electronic data processing equipment, including necessary telecommunications lines and equipment, to local governments, elected State officials, State educational institutions, and all other governmental units of the State requesting them." (20- ILCS 405/405-250).

Tests Performed: Reviewed statute and interviewed staff.

Test Results: The Department, through the Bureau of Communication and Computer Services provided data processing and telecommunication services to approximately 97 entities.

No significant exception noted.

Department Description of Control: To fulfill this responsibility, the Department operates the Central Computer Facility (CCF), the Communications Center, and various branch facilities.

Tests Performed: Reviewed facilities and interviewed staff.

Test Results: The Department operated the Central Computer Facility, the Communications Center, and various branch facilities in order to provide services to user agencies.

No significant exception noted.

Department Description of Control: The Bureau has six Divisions, which, in turn, have several subdivisions:

- Chief of Staff
  - Acquisitions and Inventory Management
  - Workforce Development and Logistics
  - Enterprise Program Management Office
- Infrastructure Services
  - Network Services
  - End User Computing
  - Infrastructure Support
    - Change Management
    - Production Quality Assurance and Methods
  - Enterprise Production Operations
  - Data Center Operations
    - Enterprise Backup And Storage
    - Midrange Computing
    - Mainframe

- Enterprise Applications and Architecture
    - Enterprise Architecture and Strategy
    - Enterprise Business Applications and Services
    - Personal Information Management (PIM)
- Security and Service Delivery
    - Service Delivery and Implementation
    - Risk Management
- Business Services
    - Revenue Management
    - CRF Expenditure and Invoice Verification
    - SSRF Invoice Verification
    - Appropriations Management
- Customer and Account Management
    - Agency Relations
    - Field Operations
    - Customer Solution Center
    - Communications Management Center
    - Service Reporting.

Tests Performed: Reviewed organizational chart and interviewed staff.

Test Results: The Bureau was comprised of six divisions, with several subdivisions.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives.

ADMINISTRATION
Strategic and Business Planning

EXISTING ENVIRONMENT

Department Description of Control: The Bureau monitors technological trends through strategic and business planning. The Bureau's Strategic Plan is developed by the Leadership Team based on both personal knowledge and external information. This knowledge is then correlated with Bureau initiatives and documented in the Strategic Plan. The Plan is used by the Leadership Team as an internal guide for Bureau strategy.

Tests Performed: Reviewed FY08 Strategic Plan and interviewed staff.

Test Results: The Bureau's Leadership Team provided input to the Deputy Director who was the primary author of the "FY08 Information Technology and Network Strategic Plan". The Plan was finalized on January 22, 2008.

No significant exception noted.

Department Description of Control: Business planning is accomplished by collecting relevant budgetary information from Consolidated Agencies, Illinois State Police, Department of Corrections, and the Department of Children and Family Services. The Bureau requests this information via a memo from the Deputy Director addressed to agency executive directors, chief financial officers, and chief information officers. This information is captured and maintained within the Consolidated Project Portfolio database. Collected information identifies planned business initiatives and anticipated changes to Business as Usual expenditures. This data is analyzed by Enterprise Architecture and Strategy (EA&S) to provide a forecast of anticipated IT and telecom expenditures resulting in a coordinated Spending Plan and a coordinated Budget Submittal.

Tests Performed: Reviewed memorandums, individual agency and coordinated spending plans, and BCCS Strategic Portfolio.

Test Results: On September 21, 2007 the Deputy Director sent a memorandum to Consolidated Agencies, Illinois State Police, Department of Corrections, and Department of Children and Family Services requesting FY08 and FY09 business and resource needs. Information received from the agencies was incorporated into individual and combined budget and forecast spreadsheets, and the BCCS Strategic Portfolio – Three – Year Plan.

No significant exception noted.

Department Description of Control: Identification of current business applications are tracked in the Business Reference Model (BRM) and current technology standards are tracked in the Technical Reference Model (TRM). EA&S is responsible for the maintenance of these databases. Agencies are responsible for updating information in the BRM. EA&S and the Architecture

Rationalization Board (ARB) manage and document architectural standards via the TRM, Product Standardization Requests, and ARB meeting minutes.

Tests Performed: Reviewed the Enterprise Architecture Taxonomy Database Management System, ARB meeting minutes, Product Standardization Requests, and interviewed staff.

Test Results: The Enterprise Architecture Taxonomy Database Management System contains information on business applications (Business Reference Model) and products (Technical Reference Model).

The TRM contained information on the State's products (technology standards). The TRM categorized all products into one of seven lifecycles:

- Proof of Concept.
- Target.
- Standard.
- Supported.
- Not Supported.
- Retired.
- Legacy.

Per Department staff, EA&S had input in the overall strategy as it related to technical standards, setting up new services, and financial forecasting through the budgeting process.

The ARB held several meeting during the audit period and addressed issues including standards, reference models, and Product Standardization Requests.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives.

ADMINISTRATION
Project Management

EXISTING ENVIRONMENT

Department Description of Control: Project management is the responsibility of the Enterprise Program Management Office (EPMO). Projects are initiated by submittal of a Project Charter. Projects requiring governance are monitored by the EPMO and/or responsible divisional staff using various methods including Microsoft Project Professional.

Tests Performed: Reviewed projects and interviewed staff.

Test Results: According to EPMO Management, project management only monitored Department projects. Agency projects, which required governance, were monitored by Infrastructure Services or agency staff, and user agency project managers.

During the audit period, EPMO indicated they were responsible for 35 Department projects, of which 15 had been completed. We reviewed three completed projects noting a Project Charter had been completed and the project had been monitored by a project manager.

However, during our detailed testing, we noted six additional Department projects which met the governance criteria; but, did not have oversight by EPMO or a project manager.

Project management was not consistently applied to all projects.

Department Description of Control: For projects that meet governance criteria, the EPMO or responsible division assigns a project manager or work coordinator for oversight of the project. For projects directly managed by the EPMO, a team site is created within a SharePoint repository and project status information is captured within Microsoft Project Professional. Specific project management processes including planning, execution, and operational transition vary by project based upon the specific needs of each project. The EPMO provides a recommended set of project management tools and artifacts that should be utilized (as appropriate) for most projects.

Tests Performed: Reviewed projects, team sites, recommended project management tools, and interviewed staff.

Test Results: According to EPMO Management, project managers were only assigned to Department projects which met the governance criteria.

The Department had not developed project management policies and procedures to ensure consistency in the management of projects. The EPMO had published on their SharePoint site a set of templates and guidelines. However, according to EPMO Management, the templates and guidelines were only recommended and were not required to be followed.

In addition, EPMO had developed a recommended set of project management tools.

During our review of the three completed Department projects, we noted a project manager had been assigned, and two of the three had a team site in a SharePoint repository. According to EPMO Management, the third project predated the use of the SharePoint repository. We reviewed these projects and found inconsistencies in project management, status reports, and documentation. Specifically, we were unable to determine how the project management approach helped achieve the projects' goals and objectives. In addition, based on the documentation, we were unable to determine if the projects were successful.

EPMO had not implemented formal policies and procedures to ensure all projects were consistently, efficiently and effectively developed and monitored.

Department Description of Control: An Executive Dashboard, listing projects identified by the Leadership as those requiring special attention, is maintained by the EPMO and updated weekly for review by the Leadership Team to keep Bureau management informed of their status.

Tests Performed: Reviewed the Executive Dashboard and interviewed staff.

Test Results: According to EPMO staff, the Executive Dashboard listed projects which had been selected by the Leadership Team.

In addition, the Leadership Team utilized the Executive Dashboard as their agenda for the weekly meetings.

We reviewed the Executive Dashboard for the Leadership meetings of July 2007 through January 2008, noting the Executive Dashboard had been completed for each month.

No significant exception noted.

OVERALL CONCLUSION

The Department had not implemented a formal process to ensure all staff were efficiently and effectively meeting its goals and objectives.

To enhance the current process, the Department should develop policies and procedures which clearly define EPMO's responsibilities.

ADMINISTRATION
IT Governance

EXISTING ENVIRONMENT

Department Description of Control: The Bureau's IT governance process aids in the consistent business and technical alignment of proposed initiatives which are subject to governance. These initiatives are reviewed by the EPMO's IT Governance team and EA&S to determine business and technology alignment as defined in the BRM and TRM.

The IT governance process is defined by a series of "Gates" as outlined on the IT Governance website (www.illinois.gov/governance/default.cfm) and is managed by the EPMO. IT Governance information is maintained in a Remedy-based application.

The IT Governance process (www.illinois.gov/governance/governance.cfm), requires that a Project Charter and Business (functional) and Technical (non-functional) requirements be provided for each initiative or project subject to governance. This information is utilized by the EPMO and EA&S to evaluate business and architectural alignment.

Tests Performed: Reviewed IT Governance process flowcharts, project documentation, and interviewed staff.

Test Results: EPMO maintained a website which documented the IT Governance process.

On October 25, 2007, IT Governance was revised to "streamline the process making it easier for agencies to complete the documents." Additionally, the website stated, "Governance, as a process, develops the IT component of business initiatives into projects. This is a building process that starts with the Project Charter, followed by the Business and Technical Requirements. Following the production deployment, a Post Implementation Review is conducted."

We selected five projects, which met the IT Governance criteria and began the IT Governance process after the October 2007 update. We tested the projects for compliance with the IT Governance process. We found several instances where the process was not followed. For example, required Business Impacts Analyses were not conducted for any of the five projects. In addition, although Business (functional) and Technical (non-functional) requirements were required to be provided for each initiative or project subject to governance, such reviews were not documented in any of the projects reviewed.

In addition, we reviewed 23 projects which were classified as closed from July 1, 2006 through April 2008. Documentation to support compliance with the IT Governance process was lacking for eight projects, including the omission of required IT Governance approvals.

As of February 4, 2008, EPMO moved IT Governance information from the Remedy Database to the EPM Portal Database.

Although IT Governance had a process in place, it had not been followed to effectively guide initiatives and projects.

Department Description of Control: IT Governance is required for those initiatives that meet one or more of the following criteria:

- Adding new business functionality
- Moving to a new or updated platform such as a new database, architecture, or programming language
- Replacing an old system (lifecycle)
- Outsourcing or in-sourcing a system, either partially or completely
- Potentially instantiating an enterprise application or service.

Tests Performed: Reviewed website, projects, and interviewed staff.

Test Results: According to the IT Governance process, IT Governance is needed when an initiative:

- Added a new business functionality,
- Moved to a new or updated platform,
- Replaced an old system,
- Outsourced or in-sourced a system, or
- Instantiated an enterprise application or service.

The guidelines applied whether the work was considered to be maintenance or a new development. Governance was required for all organizations under the Governor, unless exempted by legislation.

During our review of the IT Governance process, it became apparent IT Governance was not consistently applied to all initiatives.

During our review of projects, we identified two projects (Sun Server Project and the VMWARE Project) which met the criteria (moving to a new or updated platform), but did not follow the IT Governance process.

IT Governance was not consistently applied to all initiatives or projects.

Department Description of Control: For Infrastructure projects, the Infrastructure Services Division (ISD) organizes, plans, and controls these projects and participates in reviewing charters, functional and non-functional requirements, gathering and organizing detail design information, tracking and documenting issues and action items, status reporting, documenting work processes and coordinating activities between client agencies and the Bureau. The following policies guide ISD staff activities:

- Charter Review Process, dated March 5, 2007.
- Charter Review PAR Procedures, dated March 5, 2007.
- BCCS Charter Review, dated April 18, 2006.

Tests Performed: Reviewed procedures, project documentation, and interviewed staff.

Test Results: The Department developed (and recently revised) the following procedures to assist ISD:

- ISD PAR Process, effective April 18, 2006, revised on January 15, 2008.
- ISD Charter Review Procedure, effective March 28, 2006, revised on January 15, 2008.
- PAR Form Detail Description, effective April 18, 2006, revised on January 15, 2008.

ISD PAR Process
The purpose of the ISD PAR Process was to "document sequence of activities if Project Assessment Requirements (PAR) form is used to collect Infrastructure components."

ISD Charter Review Procedure
The purpose of this process was to "document the means by which Infrastructure Services will be introduced to charter requests in order to design, procure and implement solution."

PAR Form Detail Description
The purpose of this procedure was to provide a detailed description on how to complete the PAR form.

We reviewed two infrastructure projects under the jurisdiction of ISD and tested for compliance with established procedures.

Sun Server Project
In August 2006, the Department of Healthcare and Family Services (HFS) submitted a Project Charter for the Sun hardware and software infrastructure. As of April 1, 2008, the project had not been completed. According to Department management, the project is behind schedule due to "delays experienced jointly by HFS and the Department in code design, system design and compatibility of versions of software; as well as other competing priorities."

According to the IT Governance Database, the Sun Server Project was canceled in October 2006; however, we found the project was still active and on-going under the jurisdiction of ISD.

We reviewed the project documentation and found limited records to support project management activities performed by ISD. In addition, we found the documentation of the project did not support the use of, or conformity with, ISD procedures.

Newborn Metabolic Screening Project
In December 2004, the Department of Public Health (DPH) submitted a project charter for the development of a new application. The project was to develop an off-the-shelf commercial metabolic screening system to replace an existing, out dated, and end-of-life custom system for the State's mandated Newborn Metabolic Screening Program. The program was a critical high volume testing application, which processed over 800 samples each day for all infants born in the State of Illinois.

Per the RFP, the Department was responsible for the infrastructure in which the application would be hosted.

We reviewed the project documentation and found limited records to support project management activities performed by ISD. In addition, we found the documentation of the project did not support the use of, or conformity with, ISD procedures.

Although the development of the screening application had progressed on schedule there had been numerous problems with the supporting infrastructure. Infrastructure requirements approved by DPH and the Department in September in 2007 were subsequently modified by the Department. The change in the supporting infrastructure delayed the full implementation of the system and even lead to a 36 hour outage in system availability.

Although procedures existed to help ISD organize, plan, and control projects, the procedures had not been effectively implemented

OVERALL CONCLUSION

The Department had not implemented a formal process to ensure all staff were efficiently and effectively meeting its goals and objectives. We noted a lack of documentation to support decisions, and a lack of defined roles and responsibilities for the Department or user agencies which led to inconsistencies in the application of the governance process.

To enhance the current process, the Department should ensure policies, procedures, and guidelines, clearly define roles and responsibilities and provide clear and consistent guidance to staff and user agencies. The guidance should promote a formal evaluation process, compliance with requirements, and maintenance of documentation and records to support decisions for each project. Failure to adequately provide clear and consistent guidance to staff and user agencies could negatively affect user agencies’ ability to successfully develop and implement projects to support their mission and objectives.

ADMINISTRATION
Billing
Statistical Service Revolving Fund (SSRF)
and
Internet Billing System (IBiS)

EXISTING ENVIRONMENT

Background Provided by the Department: The Department is statutorily authorized to provide data processing and telecommunications services for State agencies. The Department and state agencies share the costs of those services. Funding is obtained through the Statistical Services Revolving Fund (SSRF), the Communications Revolving Fund (CRF), internal service funds, and the General Revenue Fund (GRF).

Department Description of Control: The Department requires the agencies to remit the total amount on the invoice. Payment is to be made within one billing cycle of receipt. The Department's Accounting Division is responsible for pursuing outstanding SSRF and CRF accounts. If an agency persists in not paying delinquent amounts, the Department's Director may send a letter to the Director of the delinquent agency requesting payment.

Business Services pursues outstanding Network accounts. Non payment for Network Services results in submission to the IOC offset program through the Department's Accounting Division.

Tests Performed: Reviewed Administrative Code and interviewed staff.

Test Results: Agencies were required to "process payments within 30 days after physical receipt of Internal Service Funds bills" as contained in the Department's Administrative Code (74 Ill. Admin Code 1000.50).

According to the Department's Accounting Division and Business Service staff, there had been no accounts which were required to be submitted to the IOC offset program during the fiscal year.

Each month, the Department's Accounting Division sent delinquency notices requesting payment to agencies with account balances 90 days past due. However, per Department staff, delinquency letters from the Department's Director had not been sent due to staffing shortages.

No significant exception noted.

Department Description of Control: In order to comply with the Federal Department of Human Services' requirements (A-87), the Department annually performs an analysis of the previous years' cost and revenue by service center and determines the profit/loss for each service. Excess revenues are subject to reimbursement to the Federal Department of Human Services, and may involve billing credits.

Tests Performed: Reviewed annual analysis and interviewed staff.

Test Results: Annually, the Department submits the State of Illinois Statewide Cost Allocation Plan to the Federal Department of Human Services. The Allocation Plan indicated the Department's analysis of costs and revenues by service center.

The Department submitted the FY07 Allocation Plan in March 2008.

According to Department staff, there were no billing credits resulting from the Allocation Plan during the fiscal year.

No significant exception noted.

Statistical Service Revolving Fund (SSRF)

Department Description of Control: The KOMAND IV system (system) is the primary system used to compile the SSRF billing. The system provides a means for charging resource utilization data back to the users of the computer systems. Users are billed for various services, such as use of the Local Area Network, online storage, mainframe usage, and print jobs. In addition, users are charged for the usage of the "Common Systems": Accounting Information System; Central Inventory System; Central Time and Attendance System; and Central Payroll System.

Tests Performed: Reviewed KOMAND procedures, SSRF billings, and interviewed staff.

Test Results: The KOMAND system compiled the rated SSRF billings. The agencies were billed for various services, including the common systems, each month on a rate basis.

For July through December 2007, the Department billed user agencies approximately $41 million.

No significant exception noted.

Department Description of Control: The Department has developed procedures for each phase of the SSRF billing process. At the end of each phase, verification is performed to ensure all totals are correct. Reports from each source are verified against each other to ensure accuracy of the information. Throughout the process, an "Edit Check" is conducted to ensure completeness and accuracy of each phase.

Tests Performed: Reviewed SSRF Billing Procedures, Edit Check process, agency billings, agency credits, and interviewed staff.

Test Results: The Department developed the ISD/IMS Monthly Bill procedures, dated December 2007, which provided guidance on the completion and reconciliation of the monthly billings.

The Department utilized several reports to assist with the accuracy of the billing information. The "Edit Check" process was routinely completed to promote billing completeness and accuracy.

We reviewed the Edit Check process for the months of December 2007 and January 2008 and found the Department:

- Lacked verifications and reconciliations to ensure the underlying information to support billings was valid.
- Double billed an agency for mainframe services.
- Charged an incorrect rate for a service.
- Lacked a consistent methodology for the development of new rate calculations.

Although we identified problems with the supporting information, we were able to reconcile the information in the various billing reports to three agencies' billings for the months of December 2007 and January 2008.

In the event the Department and agency determine an inappropriate charge was assessed, the agency could request a credit. We reviewed documentation associated with 14 issued credits, noting six had not been properly approved.

A formal methodology clearly documenting the allocation of charges to agencies did not exist.

The Department had not established an adequate process to ensure billings were appropriate and accurately reflected services rendered.

Internet Billing System (IBiS)

Background Provided by the Department: Due to the consolidation of various functions of State government into the Department, IBiS was developed to provide a mechanism to bill agencies for consolidated services for which there is no rate. The billing invoices are the foundation for agencies to make payments to the Department. Additionally, the invoices are to provide documentation for agencies to use for Federal Fund participation purposes.

IBiS was utilized by the consolidated agencies:

- Department of Agriculture
- Department of Commerce and Economic Opportunity
- Department of Natural Resources
- Department of Employment Security
- Department of Financial and Professional Regulation
- Department of Human Services
- Department of Healthcare and Family Services
- Department of Public Health
- Department of Revenue
- Department of Transportation
- Environmental Protection Agency

The Department bills for the following consolidated services through IBiS:

- Facility Management,
- Information Technology, and
- Communication.

Our review of IBiS was concentrated on the Information Technology billings.

Department Description of Control: The IBiS file contains salary and fringe benefits costs for consolidated agency personnel whose time is charged back to a specific consolidated agency (agencies). The data is based upon the service center code entered into the Service Center Allocation System (SCAS) and applied to the employee's payroll cost for each pay period that month.

Tests Performed: Reviewed SCAS, payroll charges, and interviewed staff.

Test Results: The Service Center Allocation System (SCAS) was the primary source to bill consolidated agencies for specific services provided to agencies by Department employees.

Per Department staff, Department employees entered their daily time (hours worked by service center) into SCAS. Each consolidated agency had at least one service center code allocated for their agency specific services. Consolidated agencies were charged based upon the time entered by service center code from Department employees.

We requested job duties for six employees noting they performed a variety of jobs for several agencies; however, their SCAS' time was allocated to one agency. In addition, agencies were charged a 25% administrative markup on all payroll charges. We requested the methodology for the calculation of the markup; however, one was not provided.

The current process, methodology, and associated documentation did not provide the necessary support to ensure the appropriateness of charges to consolidated agencies.

Department Description of Control: For AIS file support documentation Business Services downloads the AIS billing file from the mainframe. The file is sorted by Agency, and a spreadsheet is created for each agency. The detail file lists each invoice that was paid on behalf of the agency that month and includes the agency service center, cost center, DOC, voucher control number, voucher date and number, vendor name, vendor invoice number, beginning and ending dates of the service, and the amount. It is the agencies' responsibility to review the monthly billing statement and verify the accuracy of the charges.

Tests Performed: Reviewed AIS billing detail and interviewed staff.

Test Results: Each month Enterprise Business Application Services (EBAS) exported AIS files into the IBiS system in order to direct bill agencies. In addition to the IBiS invoice, the agency was provided a spreadsheet indicating the details of the AIS charges; vendor, date of service, amount, and other information.

We reviewed seven AIS vouchers to ensure they were appropriately charged, noting:

- The Department charged an agency for an employee's travel expenses ($245.00); however, the employee's payroll had not been charged to the agency.
- The Department double billed an agency for AIS charges.
- The Department billed agencies rent for Department employees which resided at the agencies. However, the employees no longer resided at agencies and had been relocated to one of the Department's locations.

Department management stated they were working with agencies regarding the correctness of these charges.

It was the agencies' responsibility to review the monthly billing statement and verify the accuracy of charges. If agencies determined a charge was inaccurate they could request a credit. We reviewed five credits, noting they had been approved.

Total IBiS billings for July through December 2007 were approximately $4 million.

The current process and associated documentation did not provide the necessary support to ensure the appropriateness of charges to consolidated agencies.

<u>Department Description of Control:</u> The Department has developed procedures for the IBiS billing process for Salaries/Fringe Benefits and for AIS files. At the end of the procedure verification is performed to ensure all totals are correct.

<u>Tests Performed:</u> Reviewed IBiS Salaries/Benefits and IBiS AIS Files procedures, salary expenditures, agency billings and interviewed staff.

<u>Test Results:</u> The Department developed the IBiS Salaries/Benefits and IBiS AIS Files procedures, not dated, which provided guidance on the compilation of the IBiS billings.

According to the Business Services Manager, a visual verification was performed after the import of AIS and payroll data into IBiS. Documentation of the verification was not maintained.

We reviewed three agencies' IBiS billings, noting the charges traced to detail.

The Department did not document the verification of AIS and payroll charges.

OVERALL CONCLUSION

The Department had not implemented an adequate process/methodology to ensure the appropriateness of billings to agencies. To ensure the accuracy of the billings, the Department should:

- Develop a process to ensure billings are appropriate and accurately reflect services rendered.

- Develop a formal methodology to clearly document the allocation of rates and charges to user agencies.
- Document the verification of AIS and payroll charges.
- Formally approve all issued credits.

Note: We will recommend that a detailed review of the Internal Service funds be conducted as part of the Department's Financial Audit and Compliance Attestation Engagement for the period ending June 30, 2008.

ADMINISTRATION
Billing
Communications Revolving Fund (CRF)

EXISTING ENVIRONMENT

Background Provided by the Department: The Department is statutorily authorized to provide data processing and telecommunications services for State agencies. The Department and state agencies share the costs of those services. Funding is obtained through the Statistical Services Revolving Fund (SSRF), the Communications Revolving Fund (CRF), internal service funds, and the General Revenue Fund (GRF).

Department Description of Control: The Department requires the agencies to remit the total amount on the invoice. Payment is to be made within one billing cycle of receipt. The Department's Accounting Division is responsible for pursuing outstanding SSRF and CRF accounts. If an agency persists in not paying delinquent amounts, the Department's Director may send a letter to the Director of the delinquent agency requesting payment.

Business Services pursues outstanding Network accounts. Non payment for Network Services results in submission to the IOC offset program through the Department's Accounting Division

Tests Performed: Reviewed Administrative Code and interviewed staff.

Test Results: Agencies were required to "process payments within 30 days after physical receipt of Internal Service Funds bills" as contained in the Department's Administrative Code (74 Ill. Admin Code 1000.50).

According to the Department's Accounting Division and Business Service staff, there have been no accounts which were required to be submitted to the IOC offset program during the fiscal year.

Each month, the Department's Accounting Division sent delinquency notices requesting payment to agencies with account balances 90 days past due. However, per Department staff, delinquency letters from the Department's Director had not been sent due to staffing shortages.

No significant exception noted.

Department Description of Control: BCCS uses a database called EMS11 to generate approximately 90-95% of billings for the CRF. In June, 2007, a conversion to the EMS11 system instituted the procedure of one billing run per month. BCCS uses the Accounting Information System (AIS) for the remaining telecommunications billings.

Tests Performed: Reviewed CRF billing procedures and interviewed staff.

Test Results: In July 2007, the Department began utilizing the EMS11 system to bill agencies for telecommunication charges.

According to Business Services approximately 95% of the CRF billing were generated through the EMS system; the remaining 5% was generated through AIS. The EMS billing system and AIS allowed for re-rated charges as well as pass-thru charges.

No significant exception noted.

Department Description of Control: Most statewide telecommunications services are billed to CMS by telecommunications carriers. CMS then bills users based on their consumption of these services. Vendors charge CMS based either on contractual rates or on tariff rates published with the ICC. CMS re-bills users to recover vendor charges plus administrative expenses. Generally, the administrative markup is 10%.

Tests Performed: Reviewed billing process and interviewed staff.

Test Results: The Department received billing data and reports from several vendors. Once the vendor data was uploaded Business Services conducted several reconciliations.

After vendor files and the upload were reconciled, the files were sent to the EMS11 vendor in order to create the telecommunication billings. Once the final billing was created, Business Services performed a reconciliation to ensure the accuracy of the information.

The billing information was then processed for usage, inventory, and manual charges. Upon completion, the billing invoice information was forward to Accounting for the creation of agency invoices.

According to Department staff, "the method of determining most of the current rates for Telecommunication services was developed years ago." In addition, "the 10% markup was started years ago based on a management study that determined it was optimal to recover indirect costs without incurring excessive federal payback." A formal methodology clearly documenting the allocation of charges to agencies did not exist.

No significant exception noted.

Department Description of Control: Billings for network bandwidth usage and/or other network services for constituents which are non-state agencies are billed monthly through the MAS90 system. The Department has developed procedures for each phase of the CRF and MAS90 billing processes. At the end of each phase, verification is performed to ensure all totals are correct. Reports from each source are verified against each other to ensure accuracy of the information.

Tests Performed: Reviewed CRF Billing Procedures, MAS90 Invoice Processing Procedures, reconciliations, credits, and interviewed staff.

Test Results: The Department had developed procedures for the billing processes of CRF and MAS90; CRF Billing Procedures and MAS90 Invoice Processing Procedures.

Business Services received and uploaded network data into MAS90 in order to generate billings. Several reports were generated and reconciled to ensure the upload into MAS90 was complete and accurate.

We reviewed the various reports and reconciliations for the CRF and MAS90 billings for December 2007 and January 2008, noting no exceptions.

In the event the Department and agency determined an inappropriate charge had been assessed, the agency could request a credit. We reviewed documentation associated with ten issued credits, noting no exceptions

For July through December 2007, the Department billed user agencies approximately $37 million.

No significant exception noted.

Department Description of Control: In order to comply with the Federal Department of Human Services' requirements (A-87), the Department annually performs an analysis of the previous years' cost and revenue by service center and determines the profit/loss for each service. Excess revenues are subject to reimbursement to the Federal Department of Human Services, and may involve billing credits.

Tests Performed: Reviewed annual analysis and interviewed staff.

Test Results: Annually, the Department submits the State of Illinois Statewide Cost Allocation Plan to the Federal Department of Human Services. The Allocation Plan indicated the Department's analysis of costs and revenues by service center.

The Department submitted the FY07 Allocation Plan in March 2008.

According to Department staff, there were no billing credits resulting from the Allocation Plan during the fiscal year.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. However, the Department should develop a formal methodology to clearly document the allocations of rates and charges to user agencies.

Note: We will recommend that a detailed review of the Internal Service funds be conducted as part of the Department's Financial Audit and Compliance Attestation Engagement for the period ending June 30, 2008.

ADMINISTRATION
Help Desk
Customer Solution Center (CSC)

EXISTING ENVIRONMENT

Department Description of Control: The CSC is responsible for providing Tier 1 support for Telecommunications (excluding Illinois Century Network and Radio) and IT services. The CSC is a single point of contact (SPOC) where client solutions are handled for different technologies and simplifying end user support. The CSC is responsible for managing timelines and the value of the products and services offered through the CSC Service Desk and the vendors and internal teams supporting those products and services. The CSC has processes and guidelines in place for enterprise-wide management, escalation and notifications, and other operational needs.

Tests Performed: Reviewed procedures and monthly reports.

Test Results: According to the CSC Service Desk Guide, "the CSC is responsible for providing Tier 1 support for Telecommunications (excluding ICN and Radio) and IT services. The CSC is a single point of contact where client solutions are handled for different technologies and simplifying end user support."

In addition, "the CSC is responsible for managing timeliness and the value of products and services offered through CSC Service Desk and the vendors and internal teams supporting those products and services."

Each month a report was generated documenting the performance levels, such as the number of calls received, calls abandoned, and the average time it took to answer a call. For the months of November and December 2007, 12,674 calls were received with an abandonment rate of approximately 4%, and an average time to answer a call of 20.5 seconds.

No significant exception noted.

Department Description of Control: The CSC IT Service Desk is responsible for providing Tier 1 IT technical and end user support to the consolidated agencies as well as the multiple boards, commissions and non-consolidated agencies. The IT Service Desk is the single point of contact for reporting IT incidents and requesting new services. The IT Service Desk is staffed during normal business hours Monday through Friday 8 am to 5 pm, with extended coverage from 8 am to 4 pm on Saturday and Sunday for HFS and DHS. Evening coverage for HFS and DHS is provided by production operations staff working at the legacy agency locations.

Tests Performed: Reviewed management calendar and interviewed staff.

Test Results: The CSC IT Service Desk provided Tier 1 help desk support and customer service. The IT Service Desk was staffed during business hours, Monday through Friday (8am to 5pm). Additional coverage was available for HFS and DHS on Saturday and Sunday (8am to 4pm).

Evening coverage for HFS and DHS was provided by the legacy agency staff.

We reviewed the weekend staffing schedule for HFS and DHS, noting the shifts were staffed.

No significant exception noted.

Department Description of Control: The physical consolidation of service desk staff for 11 of the 12 agencies in Springfield has been completed. Chicago-based IT Service Desk staffs (DES and DFPR) have been consolidated to the James R. Thompson Center utilizing the CMS Remedy for ticketing and the Avaya phone system.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: The Department had consolidated the service desk for the consolidated agencies. The IT Service Desk had staff located in the Thompson Center to assist with DES and DFPR incidents. The staff utilized the CMS Remedy and the Avaya phone systems.

No significant exception noted.

Department Description of Control: Customers contact the IT Service Desk via phone or email to report an incident. The Service Desk staff opens a ticket in BCCS Remedy and records the category, type, and item (CTI), as well as the customer name, agency, contact and demographic information and a detailed incident description. If the IT Service Desk is unable to resolve the incident, the ticket is assigned to Tier 2 or Tier 3 support teams based on the CTI and/or predefined summary field. Procedures exist for the Help Desk task.

Tests Performed: Reviewed procedures, Remedy Help Desk tickets, and interviewed staff.

Test Results: The Department developed the CSC Service Desk Guide to assist staff with the operations of the CSC. In addition, the Department developed the Remedy User Guide to assist with the creation of Remedy tickets.

Customers contacted the IT Service Desk to report incidents. The IT Service Desk staff recorded the incident and subsequently updated the customer information within Remedy.

In the event the IT Service Desk staff was unable to resolve the problem, the ticket was escalated to a Tier 2 or Tier 3 support team member.

We reviewed 531 Remedy Help Desk tickets for the period of November 12, 2007 and December 18, 2007, noting all required fields had been completed. Additionally, we sampled 50 of the Remedy tickets, noting the average closure time was 5.38 days.

No significant exception noted.

Department Description of Control: The IT Service Desk receives an Enterprise Service Request form (ESR) from an authorized IT coordinator. All IT changes require a request form. The IT Service Desk has standardized on the ESR process and the intake of service requests in the Remedy system for all consolidated agencies. Service requests are submitted via email.

Tests Performed: Reviewed procedures, Remedy Service Request tickets, ESR forms, and interviewed staff.

Test Results: The Department developed the Enterprise Service Request Instructions, dated February 8, 2008. The Instructions provided guidance to the agency and the IT Service Desk staff on the completion of an ESR.

An ESR "provides the end user a means to request standard or routine software or hardware related additions, moves or changes to their desktop system." According to the Remedy User Guide, IT Service Desk staff were charged with reviewing ESRs for completeness and accuracy of information provided. We reviewed 100 ESRs completed by agency or IT Service Desk staff, noting 63 (63%) did not have the required fields properly completed.

Per the Operations Manager for the IT Service Desk, an ESR was required for all IT changes. After the receipt of the ESR, IT Service Desk staff were supposed to create a Remedy ticket, assign it to the appropriate team, and attach the ESR.

We reviewed 536 Remedy Service Request tickets for the months of November and December 2007, noting 25 (4.66%) did not have an ESR attached.

Procedures for the proper completion of Remedy tickets and ESRs existed; however, the ESRs were not always properly completed or attached to tickets.

Department Description of Control: Each agency head delegates, in writing, an IT coordinator(s) authorized to expend funds. The IT Coordinator database is maintained by Agency Relations. The IT coordinator is responsible for submitting the appropriate request forms to the IT Service Desk for all IT changes. The IT Service Desk staff is responsible for verifying the submitter is an authorized coordinator in the database. The coordinators can locate the instructions for completing these forms on the Bureau's Website (www.bccs.illinois.gov/downloads.htm) and are provided guidance by the IT staff when necessary. Procedures exist for the ESR processing task.

Tests Performed: Reviewed website, IT Coordinator authorizations, and interviewed staff.

Test Results: The Department maintained various IT forms and instructions on the website.

The Department maintained a database which listed agency coordinators authorized to expend funds. We reviewed 25 IT Coordinators, noting each had been authorized in writing by the agency head.

Additionally, we reviewed 100 ESRs and found each one was approved by an authorized IT Coordinator.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. To enhance the controls the Department should ensure all tickets and forms are properly completed.

ADMINISTRATION
Help Desk
Customer Management Center (CMC)

EXISTING ENVIRONMENT

Department Description of Control: The CMC is the 24/7 network support center for the State of Illinois. The CMC supports the backbone and customer access circuits for all legacy ICN customers such as the educational community, which includes K-12 schools as well as libraries, museums, hospitals and other not for profit organizations. The CMC also supports state agencies, boards, and commissions. After 5:00 PM and during non-business hours, weekends and holidays, the CMC provides emergency help desk support for voice, wireless, and data services. In coordination with the Command Center, the CMC assists with after hour IT emergency support issues including taking customer calls and monitoring enterprise servers via Hobbit for ICN customers (educational and State agencies), the CMC acts as the first point of contact between the trouble initiator or end-user and any internal/external vendor/resource that has a required step in isolating and repairing network incidents. Incidents are managed in accordance with established procedures.

Tests Performed: Reviewed procedures, staff schedule, and interviewed staff.

Test Results: The CMC provided (24 hours a day, 7 days a week, 365 days a year) support to various State agencies and entities. During non-business hours (after 5:00 pm, weekends, and holidays) the CMC was responsible for voice, wireless, and data services and help desk support. In addition, the CMC provided IT support, in conjunction with the Command Center.

We requested and reviewed the CMC time schedules for October 2007. Our review indicated two shifts per day, all of which were staffed.

The Department had developed several methods and procedures to assist CMC staff with incidents.

No significant exception noted.

Department Description of Control: The CMC has vendor management procedures that are followed.

Tests Performed: Reviewed procedures.

Test Results: The Department developed vendor management procedures, CMC M&P; Managing Escalation and Carriers. The procedures were issued in February 2005 and revised on October 20, 2007.

The procedures identified general escalation information along with guidance on escalating issues to vendors.

No significant exception noted.

Department Description of Control: Vendors supply updated lists identifying their hierarchical management chain with detailed contact information (desk, cell and home numbers). These resources (i.e. people) are available 24/7.

Tests Performed: Reviewed vendor listings.

Test Results: The Department had obtained several listings from various vendors regarding management contact information.

Our review of the vendor listings indicated some were not dated and several had not been updated since 2005.

No significant exception noted; however, several vendor contact listings had not been updated since 2005.

Department Description of Control: The CMC staff provides status to the customer on an hourly basis, and escalates if required, to the vendor until an issue is resolved (service restored). Upon every escalation, CMC staff updates the end-user or affected party of status. All of this is captured and documented via ticketing tools such as ICN Remedy or CMS Remedy, (depending under which ticket tool the asset is inventoried).

Tests Performed: Reviewed procedures and Remedy tickets.

Test Results: The Department developed the Management Escalation Procedures, which provided guidance on problem escalation. The Procedures documented the criteria to be utilized when escalating a problem.

We reviewed 25 Remedy tickets which had been escalated, noting the work logs captured information regarding the problem and resolution.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. To enhance the controls, the Department should periodically update all vendor contact listings.

ADMINISTRATION
Help Desk
End User Computing (EUC)

EXISTING ENVIRONMENT

Department Description of Control: EUC provides personal computer, printer, software, and peripheral support to Consolidated Agencies and CMS Supported Non-Consolidated Agencies and ensures resources support is provided in a consistent manner. Responsibilities of EUC include:

- Tier 2 Support - Diagnoses and resolves break/fix incidents.
- New Installations - Assesses, plans, and executes the installation of personal computers (desktop and laptop) and associated software.
- Add/Move/Change Services - Assesses, plans, and executes the relocation of and/or modification to personal computer (desktop and laptop) resources.

Tests Performed: Interviewed staff.

Test Results: The EUC provided computer, printer, software and peripheral support to a myriad of agencies and entities.

No significant exception noted.

Department Description of Control: EUC receives break/fix incident assignments via Remedy. The supervisor of the assigned EUC Unit assigns the incident to an EUC technician and creates tasks (if required). The technician executes applicable diagnostic and repair actions, updates the Remedy work log to reflect said actions, and resolves the Remedy incident record.

Tests Performed: Reviewed Remedy Help Desk tickets and interviewed staff.

Test Results: When the service desk received a call from a user regarding a technical problem; a break/fix ticket was created within Remedy and assigned to EUC. EUC staff evaluated and worked to resolve the problem. Upon completion of the task, the Remedy ticket and work log was updated.

We reviewed 531 Remedy Help Desk tickets for the months of November and December 2007 for completeness, noting no exceptions. In addition, we reviewed 50 Remedy Help Desk ticket work logs for completeness, noting one ticket did not have a work log completed.

No significant exception noted.

Department Description of Control: EUC receives installation service requests via Remedy. The supervisor of the assigned EUC Unit or designee executes applicable assessment, planning, task creation (if required), and EUC technician assignments for necessary installation services. The technician then updates the Remedy work log to reflect said actions, and closes the Remedy incident/task to reflect completion of the installation.

Tests Performed: Reviewed Remedy Service Request tickets and interviewed staff.

Test Results: The service desk created a service request for installation services and assigned it to EUC. The EUC supervisor then assigned the applicable ticket to a EUC technician for assessment and planning.

According to the EUC Manager, depending on the size of the installation, assessments for installation service requests could range from and consist of anything from a phone call to a customer/associate, to a walkthrough of a physical location, a large meeting with customers and other infrastructure support staff, or the development of a detailed spreadsheet.

An ESR provided the end user a means to request standard or routine software or hardware related additions/moves/changes and should be attached to a Remedy Service Request ticket.

We reviewed 536 Remedy Service Request tickets for the months of November and December 2007 for completeness, noting 25 did not have a required Enterprise Service Request (ESR) attached.

An ESR Computer Addendum provided a means for requesting hardware through the PC refresh program and should be attached to the Service Request ticket.

We reviewed 10 Remedy Service Request tickets associated with the PC refresh program to determine if the ticket had a corresponding ESR Computer Addendum, noting eight of the Addendums were not properly completed.

Although a process existed for the completion of Remedy tickets, ESRs, and ESR Computer Addendums were not properly completed or attached to tickets.

Department Description of Control: EUC receives change requests via Remedy. The supervisor of the assigned EUC Unit or designee executes the applicable assessment, creates tasks (if required), and EUC technician assignments for necessary modification and/or relocation services. The technician updates the Remedy work log to reflect said actions, and closes the Remedy change request to reflect the completion of the change.

Tests Performed: Reviewed Remedy Change Request tickets and interviewed staff.

Test Results: A Remedy Change Request ticket was created by the service desk and assigned to the EUC team for completion.

During the audit period, the EUC had one Remedy Change Request ticket assigned to them. We reviewed the ticket, noting no exceptions.

No significant exception noted.

Department Description of Control: EUC Incident, ESR, and task workload is monitored by the EUC Manager via Remedy sampling that is loaded into an Excel spreadsheet.

Tests Performed: Reviewed spreadsheet and interviewed staff.

Test Results: The EUC Manager created the Excel spreadsheet in August 2007, to assist in tracking help desk requests, ESRs, and other tasks assigned to EUC.

We reviewed the Excel spreadsheet, noting it indicated the number of tickets each month by category.

The EUC was assigned 7,971 tickets for the period of July 1, 2007 through December 31, 2007, of which 29 had not been resolved. The average resolution time per ticket was 11days.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. To enhance the controls, the Department should ensure all forms and tickets are properly completed.

ADMINISTRATION
Help Desk
Telecommunications Service Desk

EXISTING ENVIRONMENT

Department Description of Control: The Telecommunications Service Desk is responsible for maintenance and provisioning of voice, video, data and wireless systems and services for State agencies, constitutional officers, commissions, boards, universities and institutions. The Telecommunications Service Desk handles all calls for telecommunications services during regular business hours Monday through Friday 8am through 5pm, excluding ICN and Internet calls which are routed directly to the CMC. All telecommunications service calls outside regular business hours and on holidays are handled by the CMC.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: The Telecommunications Service Desk was responsible for telecommunication calls during regular business hours. CMC was responsible for ICN, Internet, and after-hours service calls.

No significant exception noted.

Department Description of Control: The Help Desk records all reported incidents in the Remedy Help Desk module. Customers contact the Help Desk via phone to report an incident. The Help Desk is responsible for all reported incidents from the time reported until resolution and confirmation from the customer is achieved. Procedures exist for the Help Desk task.

Tests Performed: Reviewed procedures, Remedy Help Desk tickets, and interviewed staff.

Test Results: The Department developed the Remedy User Guide to assist help desk staff in the creation of a Remedy ticket.

Upon notification from the customer, the help desk staff created an incident ticket within Remedy.

We reviewed 531 Remedy Help Desk tickets, noting all required fields had been populated.

No significant exception noted.

Department Description of Control: Monthly reports are generated from the Remedy system based on a fiscal year to track and monitor vendor performance levels for voice related services. These figures are reconciled with the appropriate vendor(s). The CSC managers and Quality Assurance staff attend a quarterly meeting with the vendor(s) to review task related reports.

Tests Performed: Reviewed reports and interviewed staff.

Test Results: Each month reports were generated from the Remedy system in order to track and monitor vendor performance. The Department utilized the reports to determine if the vendor met stated performance levels.

We reviewed three vendor reports for the months of July through December 2007, noting response times were reported based on the severity of tickets.

In addition, the CSC manager and the Quality Assurance staff met with the vendor to review the reports and discuss performance levels.

No significant exception noted.

Department Description of Control: The Provisioning unit receives forms via email or mailed paper copies from the authorized agency coordinator. All telecommunications changes require a request form. Different forms are required for different services. Data requests require a Telecommunications Data/Intercity Service Request form (TDR); voice and cellular requests require a Telecommunications Service Request (TSR); paging requests require a Paging Service Request (PSR); IWIN requests require a Wireless Service Request (WSR) form.

Tests Performed: Reviewed telecommunication change requests.

Test Results: We reviewed 25 TDRs, TSRs, PSRs, and WSRs, noting six had not been properly completed.

No significant exception noted; however, telecommunication change requests were not always properly completed.

Department Description of Control: Each agency head delegates, in writing, a telecommunications coordinator(s) authorized to expend funds. The Telecom Coordinator database is maintained by the CSC Administration staff and an alternate. The agency coordinator is responsible for submitting the appropriate request forms to the Telecommunications Service Desk for all telecommunications changes. The CSC Provisioning staff is responsible for verifying the submitter is an authorized coordinator in the database. The coordinators can locate the instructions for completing these forms on the Telecom Website (www.state.il.us/cms/telecom) and are provided guidance by the Provisioning staff when necessary. Procedures exist for the Provisioning task.

Tests Performed: Reviewed website, procedures, telecommunication change requests, Telecom Coordinator database, and interviewed staff.

Test Results: The Department maintained various telecommunication forms and instructions on the website.

The Department maintained a database of Telecom Coordinators who were authorized to expend funds. We reviewed 18 Telecom Coordinators, noting each had been authorized in writing by the agency head. In addition, we reviewed 25 telecommunication change requests, noting all had been approved by an authorized Telecom Coordinator.

No significant exception noted.

Department Description of Control: The agency coordinators have access to the Bureau's Expense Management System (EMS) and can check status of their agency orders only. The EMS system tracks ordered facilities and telecommunications equipment. The inventory module provides the asset's recurring monthly charge, location information, 'AU' code, maintenance vendor description, catalog description and model description in addition to user name, tag number and serial number if applicable to the inventory item. The inventoried asset's installation cost can be found for all rated catalog codes in the Inventory Service Catalog Maintenance module. Anytime an inventoried piece of equipment is installed, removed or moved from one location to another, an order is entered into the EMS system to update the system inventory.

Tests Performed: Reviewed EMS and interviewed staff.

Test Results: The Expense Management System (EMS) tracked orders, facilities, and telecommunications equipment. Agency coordinators had access to EMS in order to track their agency requests.

No significant exception noted.

Department Description of Control: Tagged data equipment is received and tagged by the Acquisitions & Inventory Management (AIM) warehouse staff while tagged voice equipment is sent directly to the site. A Property Control Form (PCF) is completed for newly tagged voice systems and attached to the original invoice before it is sent to Business Services for processing and entry into the Common Inventory System (CIS). The voice system is tagged by the CSC Consulting and Procurement staff at the time of acceptance. Tagged data and voice equipment listed in EMS is reconciled to the listed equipment in CIS annually by AIM. Discrepancies are reported to CSC management and investigated.

Tests Performed: Reviewed reconciliations and interviewed staff.

Test Results: According to the AIM staff a process exists to manage inventory. However, the Department had not developed policies and procedures over the tagging and recording of assets.

In January 2008, the AIM staff conducted its annual reconciliation between EMS and CIS, noting one discrepancy. We performed an independent reconciliation of the same January 2008 data and identified 114 discrepancies.

Although AIM had a process in place to manage assets, asset documentation was not properly completed and the reconciliations were not properly conducted.

Department Description of Control: Monthly reports are generated from the EMS system based on a fiscal year to track and monitor vendor performance levels for completion of voice orders in the Springfield and Chicago dedicated areas, the non-dedicated areas, non-routine orders and the overall vendor performance levels. These figures are reconciled with the appropriate vendor(s). The CSC managers and Quality Assurance staff attend a quarterly meeting with the vendor(s) to review task related reports.

Tests Performed: Interviewed staff.

Test Results: The development of vendor performance reports generated from EMS had not been completed. The Department was working to complete this task.

Monthly reports were not generated and the associated tracking and monitoring of vendor performance levels were not performed.

Department Description of Control: The Consulting and Procurement unit provides agencies with an assigned Communications Systems Specialist 2 (CSS2). There are two Consulting and Procurement staff members in the JRTC Building in Chicago. The CSS2s work closely with the agency coordinators to consult and analyze their present and future telecommunications needs and design systems to meet those requirements in the most efficient and economical manner. The CSS2s are responsible for managing non-routine service requests. Procedures exist for the Consulting and Procurement unit tasks.

Tests Performed: Reviewed procedures.

Test Results: The CSS2s worked with agency coordinators to conduct analysis of their respective telecommunication needs.

The Department developed the Remedy Soft Launch CSC Provisioning Request Non Routine CSS Level 1&2 procedures to assist staff when entering provisioning requests into Remedy.

In addition, we reviewed 23 provisioning tickets for appropriate signatures, completed procurement information, and Director’s signature, noting no exceptions.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. To enhance the controls, the Department should ensure all forms are properly completed, retain asset documentation, perform accurate reconciliations, and develop performance reports as outlined in the Description of Control.

ADMINISTRATION
Recovery Services

EXISTING ENVIRONMENT

Department Description of Control: The Bureau provides recovery services in order to minimize the risk of disrupted services or loss of resources. Recovery utilizes satellite locations and vendor contracted services.

Tests Performed: Reviewed recovery service provider contract and interviewed staff.

Test Results: The Department had a contract with an out-of-state disaster recovery service provider to provide recovery services in the event of a major regional disaster with prolonged outages. A local satellite location was available, and per Department staff it had sufficient computing and storage capacity to meet the State's critical recovery needs. However, a comprehensive and detailed analysis had not been conducted to ensure the satellite location met the State's recovery needs.

According to the contract, in the event of a disruption, the State will activate the agreement with the recovery service provider to supply mainframe recovery services, resources, personnel and other supplies and services to ensure recovery of essential information processing capabilities. The contract had been extended until December 2009, with an approximate cost of $263,000 for FY08.

No significant exception noted.

Department Description of Control: The following contingency plans address restoration of various client environments:

- Continuity Methodology.
- Recovery Activation Plan.

Tests Performed: Reviewed plans and interviewed staff.

Test Results: The Department developed the Continuity Methodology and the Recovery Activation Plan, both revised February 2007.

The Methodology and the Plan provided high-level guidance in the event the Department's Central Computing Facility was deemed inoperable. The Methodology and the Plan provided and made reference to documentation for the recovery of the mainframe environment.

Our review of the Methodology and the Plan indicated they had not been updated to reflect the current environment and referenced documentation which had not been fully developed.

The Continuity Methodology and the Recovery Activation Plan existed; however, they had not been updated to reflect the current environment and referenced documentation which had not been fully developed.

Department Description of Control: Each consolidated agency is responsible for coordinating recovery services with the Bureau.

The Bureau purchases exercise time annually to conduct a comprehensive recovery exercise at the vendor provided recovery location. Additional exercise opportunities are afforded to any state entity and are conducted at one of the Bureau's satellite locations.

Tests Performed: Reviewed exercise documentation and interviewed staff.

Test Results: According to the Methodology, exercises involving the Department's computing facilities and services are to be conducted at least twice a year.

The Activation Plan stated exercise documentation is to include the results, recommendations, lessons learned, cost and off-site retrieval.

The Department conducted testing of its computing facility and services at the recovery service provider's site in September 2007.

Our review of the exercise documentation (Activation Recovery Status Report) indicated four out of 12 agencies, including the Department, with Category One applications (applications considered critical that impact the lives and safety of Illinois citizens) participated in the exercise. A comprehensive exercise would include all 12 agencies with Category One applications.

The Report lacked detailed information regarding applications tested and the results of the tests. In addition, the Report indicated problems were encountered during the test; however, detailed information describing the problems and resolutions were not included in the Report, and Department staff were not able to provide additional details.

In addition, the Report did not document the results, recommendations, lessons learned, cost and off-site retrieval information as required by the Activation Plan.

From August through November 2007, four agencies conducted five separate exercises at a satellite location.

A recovery test was performed in September 2007; however, all Category One applications were not included in the test and the test and supporting documentation did not meet the requirements outlined in the Continuity Methodology or Recovery Activation Plan.

Department Description of Control: The Bureau maintains a Statewide Critical Application Listing based on information received from State agencies. State agencies are required to categorize, prioritize and define the recovery time objective for their applications as follows:

A recovery time objective (RTO) schema has been super imposed over the existing classification scheme – Categories 1 through 5. The schema is defined by three stages of RTO – Stage 0 (< 72 hours), Stage 1 (< 168 hours), and Stage 2 (long-term). Information for RTO is captured in the Business Reference Model. Agencies will continue to be required to complete and submit the Statewide Data Collection forms which include information on the Category 1 through 5 classification schemas, as well as the prioritization of the applications within the classification.

- Human Safety: (Category One) Resources that directly impact the lives and safety of Illinois citizens, including state employees.
- Welfare Human Service: (Category Two) Resources that directly impact the well being of Illinois citizens.
- Non-Welfare Human Service: (Category Three) A human service resource that indirectly impacts the welfare of Illinois citizens.
- Administrative State Functions & Processes: (Category Four) Resources that support the administration of state processes.
- Support of Specific Agency Functions & Processes: (Category Five) Resources related to the maintenance of a specific agency function or process.

Tests Performed: Reviewed the Statewide Critical Application Listing, Business Reference Model, and interviewed staff.

Test Results: The Department had not requested the completion of the Statewide Data Collection Forms from user agencies in order to update the Statewide Critical Application Listing. The Statewide Critical Application Listing had not been updated since 2006.

The latest Statewide Critical Application Listing, 2006, indicated 60 Category One applications; of which the Department was responsible for the recovery of the infrastructure for 51 of them.

The Statewide Critical Application Listing had not been updated since 2006.

Department Description of Control: In the event of a regional disaster, the Bureau will only recover Category One applications for those State agencies that have met the recovery requirements. State entities with these application types are required to participate in the comprehensive exercise if requested by the Bureau, conduct exercises annually at one of the Bureau's satellite facilities or through contracted services, and participate in the Statewide Data Collection which requires filing of recovery plans and exercise results.

Tests Performed: Reviewed exercise documentation, recovery plans and interviewed staff.

Test Results: We reviewed exercise documentation to determine if the State Agency Category One application met the Department's recovery requirements. Our review indicated four agencies had conducted exercises on ten Category One applications. Additionally, a fifth agency also had conducted an exercise within the last year; however, due to lack of documentation we were unable to determine the applications tested.

State agencies with Category One applications were not meeting the Department’s recovery requirements.

Department Description of Control: Customers who have data residing on the Bureau’s mainframe are responsible for backing the data up properly and indicating which data should be stored off-site. The Department utilizes a regional off-site storage facility for storage of critical information.

Tests Performed: Reviewed off-site storage facility.

Test Results: The Department utilized an off-site storage facility to maintain backups and critical recovery information.

The Recovery Activation Plan documented the critical information (hot boxes), which were to be maintained at the regional off-site storage facility. We reviewed the contents of the hot boxes noting several items, which were to be located in the boxes, were not updated. Specifically, we noted:

- Vendor contact listing was last updated in 2002.
- Computing Facility Floor Plan was last updated in 2006.
- Statewide Critical Application listing was dated 2003 and 2006.
- Equipment inventory listing was last updated in 2002.

In addition, the following items/documents were to be maintained in the hot boxes; however, they were not.

- BCCS/RM Recovery Plan.
- CSC Recovery Plan.
- Network Services LAN Recovery Plan.
- Architectural Drawings.
- Circuit configurations.

Additionally, the hot boxes which were supposed to maintain critical recovery information, had not been reviewed or updated since December 2006.

Critical information to assist in recovery efforts was often missing or outdated.

Department Description of Control: The Bureau has developed scripts and/or procedures for the recovery of operating system platforms. Recovery Services staff assist in updating and rehearsing these procedures when building the operating systems for customer recovery exercises.

Tests Performed: Reviewed scripts, procedures and interviewed staff.

Test Results: The Department had not developed scripts and/or procedures for the recovery of operating system platforms. Department staff stated the Department was in the process of developing a disaster recovery cookbook.

In addition, according to Department staff, they did not assist in the updating and rehearsing the various procedures during recovery exercises. This was the responsibility of the staff responsible for the operating system.

Scripts and/or procedures for the recovery of the Department's mainframe had not been developed. In addition, the Recovery Services staff did not assist in updating and rehearsing procedures for recovery exercises.

Department Description of Control: The Bureau has submitted a Request for Proposal for posting to provide failover services for critical distributed applications. Until those services are in place, the Bureau will continue to maintain its current vendor contract for cold site recovery services at a remote center.

Tests Performed: Reviewed Request for Proposal and interviewed staff.

Test Results: On December 12, 2007, the Department issued a Request for Proposal for an alternate data center/failover site and services. The Department anticipated awarding the contract before July 2008.

Until the contract is awarded, the Department has a contract in place with a disaster recovery services provider to provide recovery services in the event of a major regional disaster with prolonged outages.

No significant exception noted.

OVERALL CONCLUSION

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 can be recovered within required timeframes.

The Department had not adequately implemented 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 is mandated to manage all electronic data processing equipment used by State agencies, which include backup facilities for that equipment. Therefore, it is imperative the

Department have in place a framework to promote and apply disaster recovery services. To ensure an adequate recovery framework, the Department should:

- Ensure the necessary components (plans, equipment, and facilities) are available to provide for the continuation of critical computer operations in the event of a disaster.
- Perform a comprehensive and detailed analysis to ensure the satellite location meets the State's recovery needs.
- Conduct comprehensive tests of the plans on an annual basis. In addition, the Department should coordinate with the agencies and help ensure that recovery tests of critical applications are conducted at least annually.
- Ensure the Description of Controls is an accurate description of the current recovery services environment.
- Ensure plans and procedures have been implemented and tested to protect critical information resources.
- Ensure the agency information is timely updated and maintained to ensure recovery of critical information.
- Formally communicate with user agencies to gain an understanding of their individual recovery requirements, and establish and document guidelines that outline both the agencies and the Department's responsibilities.

ADMINISTRATION
Internal Audit

EXISTING ENVIRONMENT

Department Description of Control: The statewide Information Technology (IT) audit function is part of the Illinois Office of Internal Audit (IOIA), which addresses those entities under the Governor's jurisdiction. IT is addressed on a statewide basis, which reduces duplication of efforts and increase efficiencies. IOIA performs various types of IT audits including system development audits, application audits, special audits, and internal audits.

Tests Performed: Reviewed listing of projects, internal audits, and interviewed staff.

Test Results: Agencies were required to submit a listing of new system developments or major modifications, and the status of existing projects to IOIA each quarter.

It was the agencies' responsibility to inform IOIA of new system developments or major modifications.

The IOIA performed various types of IT audits during the audit period.

No significant exception noted.

Department Description of Control: The Fiscal Control and Internal Auditing Act (30 ILCS 10/2003 (a) (3)) mandates IOIA review the design of major new electronic data processing systems and major modifications to those systems. IOIA has established a process for identifying major new systems and major changes to existing systems for system development audits to determine which systems development projects are major and require an audit. IOIA has developed a database of system development projects for all agencies under the Governor. Periodically, IOIA contacts each agency to update the information and request a list of new planned projects.

Based on the implementation date, IOIA performs a risk assessment for the project. The risk assessment consists of review of the following documentation, if applicable: project charter, RFP, system objectives, design documentation, cost benefit analysis, and other relevant documentation to gain an understanding of the project. Based on these documents, an interview with agency staff is conducted to gather and verify information to complete a risk matrix and risk questionnaire. Based on this information, the auditor, supervisor and manager make a determination as to whether the project is a major new system development or a major modification to a major system. Finally, it is reviewed by the Chief Internal Auditor and a letter is issued to the agency with IOIA's determination.

Tests Performed: Reviewed the annual report.

Test Results: We reviewed the FY07 annual report, noting 61 risk assessments were performed during the year.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives.

ADMINISTRATION
Personnel

EXISTING ENVIRONMENT

Department Description of Control: The Workforce and Development and Logistics unit coordinates and facilitates internal personnel paperwork, workforce training, development and implementation, and workforce logistics for the Bureau.

Tests Performed: Interviewed staff.

Test Results: The Workforce and Development and Logistics unit was responsible for the Bureau's internal personnel paperwork, training and workforce logistics.

No significant exception noted.

Department Description of Control: The Unit uses several policies/procedures which allow for proper processing of transactions. Specifically, for HR related transactions we refer to and comply with: the Personnel Rules, the Personnel Code, the CMS Policy Manual, the union contracts, the pay plan, the personnel transactions manual and the alphabetic index.

Tests Performed: Interviewed staff.

Test Results: The Unit utilized policies/procedures established by the Bureau of Personnel, the Department, the Governor, Legislature, or other entities. The Unit did not establish its own policies/procedures.

Additionally, all transactions were sent to the Department's Bureau of Personnel for review and final approval.

No significant exception noted.

Department Description of Control: The Workforce Training, Development and Implementation unit works with the Bureau's fiscal office for approval of training requests. A hard copy training request form and procedure are used. When training involves travel, applicable travel rules and regulations are used for approval and reimbursement of training related travel expenses.

Tests Performed: Reviewed memo, training forms and interviewed staff.

Test Results: According to a memo sent to Bureau staff, dated February 5, 2007, a BCCS Training Request Form must be properly completed and approved for all training requests. If travel costs are to be incurred for the training, a Travel Arrangement Form must also be properly completed and approved.

We reviewed 26 training request forms and found a number of instances where approvals were missing, or dated after the completion of the training.

No significant exceptions noted; however, training request forms were not properly completed.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance the controls, the Development should ensure all training requests are properly completed and approved.

ADMINISTRATION
Vendor Management

EXISTING ENVIRONMENT

Department Description of Control: Management of vendor agreements for infrastructure products and services is the responsibility of Acquisitions and Inventory Management (AIM).

Tests Performed: Reviewed AIM/Vendor Management Guide and interviewed staff.

Test Results: AIM was responsible for the management of vendor agreements for mainframe, midrange, and desktop products and services.

No significant exception noted.

Department Description of Control: Information specific to vendor agreements/contracts is entered and maintained in an Access database for reference and monitoring purposes.

Tests Performed: Reviewed Access database and interviewed staff.

Test Results: The Access database contained contract information such as contract number, beginning and ending dates, renewal periods, and the number of renewals remaining on the contract.

Various reports from the Access database were utilized to assist in renewing contracts and services for the next fiscal year.

No significant exception noted.

Department Description of Control: Duties performed to manage Bureau contracts include:

- Entering product/service and terms and conditions information into an Access database for monitoring and tracking purposes;
- Acting as the liaison with vendors;
- Responding to questions from users and customers;
- Monitoring and reporting utilization and compliance;
- Performing contract and utilization reconciliations with vendors when appropriate;
- Providing contract and utilization information for internal, external, and vendor audits;
- Recommending changes to services, deliverables, terms and conditions;
- Performing periodic cost benefit analyses when appropriate; and
- Initiating renewal or rebid process when the contract nears expiration.

Tests Performed: Reviewed the AIM/Vendor Management Guide, reconciliations, and interviewed staff.

Test Results: The Access database contained some contract information; however, the terms and conditions of the contracts were not maintained in the database.

On a daily basis, Vendor Management was in contact with vendors, users and customers regarding software and maintenance purchases/contracts. Vendor Management also worked with users, customers and vendors on renewals and new contracts. During the renewal or new contracting process, Vendor Management made recommendations to management regarding contract services, deliverables, terms and conditions.

The AIM/Vendor Management Guide outlined several contract and utilization reconciliation procedures.

However, our review of the procedures indicated the reconciliations were to be performed to determine the cost of maintenance renewals and for the Department's billing purposes, not reconciliations between the number of software licenses in use and the number of licenses purchased from the vendor.

According to Vendor Management staff, complete reconciliations for desktop and midrange software were not performed.

Additionally, Vendor Management stated no internal, external, and vendor audits or cost benefit analyses had been performed during the audit period.

Although the Department managed contracts, it did not have a process to monitor and reconcile software licenses deployed verse the number of licenses purchased in contracts.

Department Description of Control: Documented procedures for reconciling desktop, mainframe and midrange software are outlined in the AIM/Vendor Management Guide located on a secure, limited access, SharePoint site. Upon receipt of software and/or licenses, staff enter licensure information into a shared Excel spreadsheet for tracking purposes. An inventory list is maintained and used to locate media and/or documentation in the library. All software media or documentation is filed in the software library, in a secured cabinet, by call name.

Tests Performed: Reviewed the AIM/Vendor Management Guide, Receipt Log, and interviewed staff.

Test Results: The Department developed the AIM/Vendor Management Guide, dated December 2007, to assist Vendor Management with its responsibilities. The Guide provided step-by-step instructions relating to contract management/administration, procurement needs, and hardware/software maintenance. The Guide also provided guidance on reconciling desktop, mainframe and midrange software.

The Guide was maintained on the Vendor Management SharePoint site, with limited access.

An Excel spreadsheet (Receipt Log) was utilized to document receipt of software and licenses from vendors. In addition to documenting the receipt of products, it also served as an inventory listing and a software library listing.

We tested the Receipt Log and found it did not contain comprehensive, detailed or accurate information on software licenses.

In addition, we selected 25 products from the Receipt Log to ensure the media and/or documentation was located in the library. However, our testing indicated 14 products (media or documentation) were not located in the library.

We found the controls over physical access to the software library lacking. Specifically, software media was not maintained in a secured cabinet or by call name as outlined in the Description of Control.

The Department did not maintain adequate controls over software inventory.

Department Description of Control: The activities involved in the administration of the software library include receiving and logging software information into tracking spreadsheet, maintaining the software physical inventory, verifying software requests against the Enterprise Architecture Technical Reference Model (TRM) database to ensure software is considered a standard enterprise infrastructure software, initiating Product Standardization Request for software not included in the TRM, verifying license availability to satisfy requests for installs, and/or initiating procurement of additional licenses.

Tests Performed: Reviewed the AIM/Vendor Management Guide, order tracking report, and interviewed staff.

Test Results: Per Vendor Management staff, software requests were verified against the TRM database to determine if it was standard enterprise infrastructure software. If the software was not included in the database, a PSR was developed for consideration and processing.

We reviewed the request process and determined it did not effectively evaluate license availability, and therefore, routinely endorsed the purchase of additional software licenses.

Although the Department had a process to review software requests, software license availability was not regularly evaluated.

OVERALL CONCLUSION

Vendor Management had not implemented procedures to ensure it met its goals and objectives. To ensure an adequate framework exists in controlling and monitoring software usage, the Department should:

- Implement a mechanism to effectively monitor software usage.
- Conduct frequent reconciliations between the actual number of licenses in use and the number of licenses purchased from each vendor.
- Ensure the Receipt Log properly records all software and its location.
- Ensure all software is properly secured and maintained in the software library.

ADMINISTRATION
Service Reporting

EXISTING ENVIRONMENT

Department Description of Control: The Bureau conducts recurring trending analyses in order to measure and assess service performance. Areas included in these analyses include: Service Desk (CMC and CSC), Mainframe, Email, and Change Management. The Bureau prepares monthly and quarterly reports for each consolidated agency with key performance data. The reports are distributed via email to consolidated agency CIOs on a recurring basis and are made available to Bureau leadership via a shared network drive.

Tests Performed: Reviewed trending analysis, monthly/quarterly reports, and interviewed staff.

Test Results: The Bureau conducted trending analyses by evaluating the performance measures of operational data each quarter. As part of the quarterly Service Performance Reports (Reports) review process, the quarterly performance data was reviewed against the prior quarter.

Each month and quarter the Bureau prepared and provided to the consolidated agencies' CIOs the Reports. The monthly Report provided the CIO information regarding operational data (Help Desk, Change Management, Mainframe, and ICN), and monthly billing charges. In addition to the monthly information, the quarterly Report provided information regarding strategic priorities, progress of the priorities, and status of the various consolidation efforts.

We reviewed the monthly Reports for August through December 2007, and the quarterly Reports for the first quarter of FY08, noting each agency received a Report, via email. In addition, we noted the various reports were maintained on a shared drive for Department management review.

According to the Service Reporting Manager, the operational measurements were manually compiled from various applications/systems. The data was pulled from the various applications/systems, downloaded into Excel, and then manipulated.

No significant exception noted.

Department Description of Control: The Service Reporting team continually reviews the performance data looking for data anomalies or changes in performance. Issues/problems are informally referred to the appropriate Bureau manager for a more thorough review.

Tests Performed: Interviewed staff.

Test Results: The Service Reporting Team reviewed performance data to determine anomalies and performance changes. If any issues arose, they were informally referred to the appropriate manager for review.

No significant exception noted.

Department Description of Control: Additionally, members of the Bureau's leadership team meet periodically with the agency CIOs to review the monthly and quarterly performance reports and respond to agency questions. Informal follow-up occurs as necessary.

Tests Performed: Reviewed meeting documentation and interviewed staff.

Test Results: The Department met periodically with the agencies' CIOs to review monthly and quarterly performance reports and to discuss any issues.

During our review, we noted from September 2007 to January 2008, the Department conducted one to two meetings for each consolidated agency. During the meetings, the monthly and quarterly reports were reviewed.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives.

ADMINISTRATION
Agency Communications

EXISTING ENVIRONMENT

Department Description of Control: The Bureau utilizes multiple methods for communicating with its customers. The Bureau website, www.bccs.illinois.gov, serves as a central location for communicating available services including the Service Catalog, key contact information, forms and guides for requesting services, announcements/bulletins, and a variety of other Bureau information.

Tests Performed: Reviewed methods of communicating with users and the website.

Test Results: The Bureau utilized the website (www.bccs.illinois.gov), Deputy Director communications, BCCS Pulse newsletters, and CIO meetings to communicate with user agencies.

Our review of the website indicated the Department's Service Catalog, contact information, forms and guides for requesting services, and announcements/bulletins were available. Additionally, a history of the Deputy Director communications was posted to the website.

No significant exception noted.

Department Description of Control: Recurring CIO meetings provide a forum for the consolidated CIOs and Bureau leadership staff to exchange key information regarding initiatives and priorities. Meeting dates, locations, and agenda are sent to the consolidated agency CIOs via email. Periodically, the Bureau hosts topic specific meetings/forums with various customer interest groups. Additionally, Bureau staff meet informally with their consolidated agency counterparts to address agency specific initiatives, issues, and concerns. These meetings may occur face-to-face or via telephone as appropriate.

Tests Performed: Reviewed agendas and interviewed staff.

Test Results: Each month leadership staff held meetings with the agency CIOs to discuss various topics. During our review, we noted the Department held monthly meeting for the period of July through November 2007. Agendas were created and provided to attendees for each meeting.

Additionally, the Bureau hosted two forums: Illinois Information Technology Accessibility Act, on September 13, 2007 and the Geographic Information Systems Update, on November 8, 2007.

In addition, each Agency Communications representative documented and maintained their own meetings and communications with user agencies.

No significant exception noted.

Department Description of Control: This past year the Bureau introduced a customer-focused newsletter to provide another vehicle for sharing information with our customers. The newsletter is distributed to telecommunications and IT customers via email and is posted to the Bureau website.

Tests Performed: Reviewed Bureau newsletters.

Test Results: Agency Communications staff created the Pulse Newsletter (published quarterly) to provide information to user agencies. The Newsletter provided users with information such as project status, security concerns, and new software which had been approved as a standard.

Agency Communications staff provided the Newsletter via email to the user agencies and also by posting it on the website.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives.

OPERATIONS
Storage and Backup

EXISTING ENVIRONMENT

Department Description of Control: Enterprise Storage and Backup (ESB) is responsible for the allocation, backup and removal of storage for the Bureau's mainframe systems.

Tests Performed: Interviewed staff.

Test Results: Enterprise Storage and Backup staff was responsible for the allocation, backup and removal of storage for the Bureau's mainframe systems.

No significant exception noted.

Department Description of Control: ESB procedures, located on the ESB SharePoint site, help ensure that z/OS cleanup, restores, and DASD adds and deletes are successfully completed. These procedures include the Weekly Daily Cleanups, DASD Addition Checklist, DASD Removal Checklist, DASD Return to Spare, DASDadd, DailyRMF, RMF2nd, RMFspec, RMFweek, and ADRDSSU Restore. Daily Remote Monitoring Facility (RMF) reports are run and sent to management for use in measuring system resources and mainframe performance such as CPU utilization.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: ESB procedures, located on the ESB SharePoint site, helped ensure that z/OS cleanup, restores, and DASD adds and deletes were successfully completed. These procedures included the Weekly Daily Cleanups, DASD Addition Checklist, DASD Removal Checklist, DASD Return to Spare, DASDadd, DailyRMF, RMF2nd, RMFspec, RMFweek, and ADRDSSU Restore.

Daily Remote Monitoring Facility (RMF) reports were run and sent to management for use in measuring system resources and mainframe performance such as CPU utilization.

No significant exception noted.

Department Description of Control: z/OS Backups are performed on the mainframes' systems data. System data is backed up daily and weekly with the weekly copies sent to the regional vault. Backups are also performed by HSM. These backups are controlled by the SMS routines and are set by the customer at allocation time. When the customer allocates a new file, a management class is assigned which determines how long the data is kept.

Tests Performed: Reviewed backup results maintained by ESB and interviewed staff.

Test Results: z/OS Backups were performed on the mainframes' systems data. System data was backed up daily and weekly, with the weekly copies sent to the Regional Vault.

Backups were also performed by Hierarchical Storage Management (HSM). These backups were controlled by the SMS routines and were set by the customer at allocation time. When the customer allocated a new file, a management class was assigned which determined how long the data was kept.

No significant exception noted.

Department Description of Control: z/OS Restores are performed at the request of mainframe technicians via Remedy. ESB restores the data, updates the Remedy work log, and closes the record to reflect said actions.

Tests Performed: Reviewed completed work log and interviewed staff.

Test Results: z/OS Restores were performed at the request of mainframe technicians via Remedy or INFOMAN. ESB restored the data, updated the Remedy work log, and closed the record.

No significant exception noted.

Department Description of Control: ESB manages both SMS Pools and Private Pools for the mainframe systems. System automation notifies ESB technicians when storage falls below a pre-determined threshold. Technicians migrate data, delete data, or add additional disk space to replenish pool space.

Tests Performed: Interviewed staff.

Test Results: ESB managed both System Management Storage (SMS) Pools and Private Pools for the mainframe systems. System automation notified ESB technicians when storage fell below a pre-determined threshold. Technicians migrated data, deleted data, or added additional disk space to replenish pool space as necessary.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls are operating with sufficient effectiveness to achieve the control objective.

OPERATIONS
Enterprise Production Operations Services
Command Center Operations

EXISTING ENVIRONMENT

Department Description of Control: The Command Center supports continuous monitoring and operation of the Bureau's computing resources to ensure availability, performance, and response necessary to sustain customer business demands. The Command Center operates 24 hours a day, 7 days a week, 365 days a year.

Tests Performed: Reviewed staff schedule and interviewed staff.

Test Results: The Command Center monitored the operation of the Bureau’s computing resources and operated 24 hours a day, 7 days a week, 365 days a year.

In order to maintain adequate Command Center staffing on each shift in October 2007, 186 hours of overtime were required.

No significant exception noted.

Department Description of Control: The Command Center utilizes the Information Management System (INFOMAN) to coordinate and oversee implementation of changes to the computing environment.

Tests Performed: Reviewed DP Guide, Scheduled Change Log, INFOMAN, and interviewed staff.

Test Results: The Command Center was responsible for ensuring changes which had been assigned to the Command Center were appropriately implemented. Once the change had been implemented, a Scheduled Change Log was printed.

According to Command Center Management, the Scheduled Change Log was maintained for approximately two to three months, and then destroyed, due to storage issues. However, summary information was maintained in the INFOMAN system.

We reviewed the Scheduled Change Log from January 1, 2008 to March 18, 2008, noting no significant exceptions.

For additional information on the change process, see the Change Control section of this report.

No significant exception noted.

Department Description of Control: Remedy is used to record and monitor incident resolution.

Tests Performed: Interviewed staff.

Test Results: The Command Center was responsible for monitoring the mainframe and selected midrange tape drives and servers. In the event a problem was detected, a Remedy incident ticket was opened. Command Center staff were responsible for monitoring the incident tickets until resolution.

According to Command Center Management, the Command Center began utilizing Remedy to record incident tickets in November 2007. However, Command Center staff had not received formal training, nor had the procedures been updated to reflect the implementation and use of Remedy.

For additional information on incident monitoring, see the Help Desk section of this report.

No significant exception noted; however, procedures had not been updated to include the Remedy system, and staff had not received formal training on the use of Remedy.

Department Description of Control: The Command Center Data Processing Guide is utilized as a reference for operational tasks.

Tests Performed: Reviewed Data Processing Guide (DP Guide) and interviewed staff.

Test Results: The DP Guide, which was dated by section, provided guidelines for various Command Center activities.

No significant exception noted.

Department Description of Control: The Focal application is used to assist Command Center in monitoring and maintaining system availability in an efficient and consistent manner.

Tests Performed: Reviewed DP Guide, Focal Application, and interviewed staff.

Test Results: The Command Center utilized the Focal Application to assist in monitoring and maintaining system availability.

The DP Guide contained a section on Focal Point Operations Procedures.

No significant exception noted.

Department Description of Control: Daily Shift Reports are generated and distributed by the Command Center and are used to document outages/issues. Shift Change Checklists are utilized by the Command Center to ensure consistent verification of system availability. SYSLOG is utilized as a tool to reference system activity.

Tests Performed: Reviewed Daily Shift Reports, Shift Change Checklist, SYSLOG, and interviewed staff.

Test Results: The Daily Shift Reports recorded all activities which occurred (downtimes, person contact, action taken, etc) on each shift. We reviewed 25 Daily Shift Reports for December 2007, noting all problems had a corresponding INFOMAN ticket or Remedy ticket.

The Shift Change Checklists were utilized to aid in reviewing the status of the various operating systems and applications. The Shift Change Checklist was also utilized to determine if there were problems with systems or applications. We reviewed 18 Shift Change Checklists for December 2007 and found the Checklists lacked supervisory sign-off, and required fields were not always completed.

The SYSLOG recorded all messages written to, and all commands entered into the system console. The main use of the system generated log for the Command Center was for the historical value in reviewing problems or questions as to what did or did not occur and what commands were entered in response to prompts for action to be taken.

No significant exceptions noted; however, all Shift Change Checklists were not properly completed.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. To enhance the controls, the Department should:

- Ensure all Shift Change Checklists are properly completed.
- Ensure all staff are properly trained, and procedures are updated to reflect the new Remedy system.
- Formally review staffing levels in the Command Center to determine if the use of overtime is more beneficial than hiring additional staff.

OPERATIONS
Enterprise Production Operations Services
Production Control

EXISTING ENVIRONMENT

Department Description of Control: The Production Control Section of EPOS ensures that production processing activities are documented and executed in accordance with approved schedules to normal completion. Standards and naming conventions exist for job acceptance as documented in each agency's standards manual.

Tests Performed: Interviewed staff.

Test Results: Production Control monitored processing activities for the Department and some agencies.

Approved schedules were submitted through CA-Scheduler or manually. Associated production processing activities were documented in logs and schedules.

Department staff stated comprehensive and standardized production control policies and procedures had not been developed, and individual agencies often followed their legacy policies and procedures.

No significant exception noted; however, standardized production control policies and procedures had not been developed for use by all consolidated agencies.

Department Description of Control: Proc Acceptance - Any new or changed job or system that is presented for acceptance by CMS, DHS, HFS, DPH or EPA to be placed into the production environment must first pass through the Production Control area. The documentation is checked for adherence to production standards, naming conventions, and run procedures.

Tests Performed: Interviewed staff and reviewed job documentation.

Test Results: According to Department staff, Production Control was not responsible for management of Proc Acceptance functions for HFS, DPH and EPA. These functions remained the responsibility of the individual agency. In addition, Production Control had limited responsibility for the management of Proc Acceptance functions for CMS.

Production Control was responsible for management of Proc Acceptance functions for DHS and documentation was maintained indicating it was in accordance with production standards, naming conventions, and run procedures.

No significant exception noted with DHS production control management; however, production control management was the responsibility of HFS, DPH, EPA, and CMS, and not managed by the Department's Production Control Area.

Department Description of Control: Job setup and processing - All jobs that are processed in the production environment, for CMS, DHS, DCEO, HFS, DPH, or EPA whether they run through CA-Scheduler or are manually submitted must be setup and processed by Production Control. This includes the initial setting up/coding of the criteria according to job specs for all new jobs (procs) at the job coding level within CA-Scheduler, as well as setting up the schedules at the schedule level. Department security software ensures only authorized individuals are allowed to submit production processing.

Tests Performed: Interviewed staff.

Test Results: According to Department staff, Production Control was not responsible for management of job setup and processing for HFS, DPH and EPA. These functions remained the responsibility of the individual agency. In addition, Production Control had limited responsibility for the management of job setup and processing for CMS.

DCEO and DHS jobs were scheduled manually or through the use of CA Scheduler. Security software was available to restrict the ability to submit production processing to authorized staff. The assignment of access rights to control an agency's job submissions was controlled by that agency.

No significant exception noted with DCEO or DHS job setup and processing; however, job setup and processing was the responsibility of HFS, DPH, EPA, and CMS, and not managed by the Department's Production Control Area.

Department Description of Control: Abend Resolution - When a job abnormally terminates due to a cart problem or a problem with how the job was setup for processing, production control staff correct the problem and restart the job. When it is a problem with the job itself, the application staff corrects the problem. After the application staff fixes the problem, production control is notified and they resubmit the job. All production abends are recorded listing the cause, who was contacted, and when the job was corrected. This documentation is provided daily to all Production Control, I/O, and Library Services staff, as well as to each legacy agency being monitored.

Tests Performed: Reviewed abend listings, daily reports, and interviewed staff.

Test Results: According to Department staff, Production Control was responsible for monitoring HFS, DHS, CMS and DOT abends.

Most abends had the procedures to fix the abend identified within the job. If the abend resolution was not identified in the warning, Production Control staff contacted the agency to obtain information to assist in problem resolution.

Documentation for Abends were recorded in the daily shift reports, which contained information on agency contacts, when the job was corrected, and the cause of the abend**.** We reviewed the daily shift reports for DHS, HFS, and CMS for the first week of December 2007, noting no exceptions.

No significant exception noted.

Department Description of Control: Automatic Distribution and online viewing of reports –The Department uses an automated tool that allows for online viewing of reports. All jobs that produce output, whether it is to be printed or to be viewed online are setup by staff in the Reporting unit of the Production Control Section. Access to the online viewing tool is controlled by system security software access controls.

Tests Performed: Interviewed staff.

Test Results: An automated tool allowed agencies online viewing and printing capabilities. The automated tool was utilized by DHS, HFS, DCEO and CMS.

Security software was available to restrict the ability to view or print reports to authorized staff. The authorization of access rights to view and print an agency's reports was the responsibility of that agency. After a valid authorization was received from an agency, Production Control staff would apply the updated access rights.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls that we were able to test, were operating with sufficient effectiveness to achieve the control objective. However, the description of controls for Proc Acceptance and job setup and processing did not apply to several agencies listed.

To strengthen the controls, we recommend the Department develop standardized production control policies and procedures for use by all consolidated agencies.

OPERATIONS
Enterprise Production Operations Services
Input/Output (I/O) Control

EXISTING ENVIRONMENT

Department Description of Control: The Input side monitors all production jobs the departments of Central Management Services (CMS), Human Services (DHS), Health and Family Services (HFS), Public Health (DPH), Commerce and Economic Opportunity (DCEO), Transportation (DOT), and the Environmental Protection Agency (EPA). Collectively, these can be referred to as I/O-managed agencies.

Tests Performed: Reviewed I/O processes and procedures and interviewed staff.

Test Results: The Input side monitored production jobs for CMS, DHS, HFS, DCEO, and DOT. The Department was not responsible for DPH and EPA input processes and procedures. These functions remained the responsibility of the individual agency.

Department staff stated comprehensive and standardized policies and procedures had not been developed, and the Department used individual agency legacy policies and procedures to monitor jobs.

No significant exception noted; however, standardized policies and procedures had not been developed. Additionally, the Department was not responsible for DPH and EPA Input processes and procedures.

Department Description of Control: I/O-managed agency production jobs that do not complete successfully are examined for the cause of their abnormal termination (Abend) and are repaired if possible by the technicians on duty. If the technicians are unable to affect the proper repairs, Production Control or Applications personnel are contacted via a Job Call List. This Call List is used to contact the necessary personnel to attain the information necessary to resolve the abnormal termination. After the problem has been resolved, I/O will reinitiate the process and monitor the job until such time as the job comes to a successful completion. Automated scheduling is used at most locations and monitors or manipulates job streams as necessary to ensure proper production processing.

Tests Performed: Reviewed processes and interviewed staff.

Test Results: For DHS and HFS production jobs that did not complete successfully, the processes to correct problems were defined and handled within the Proc Acceptance procedures.

For DCEO, DOT, DPH, EPA, and CMS, the procedures to correct problems were not identified within the Proc Acceptance procedures; therefore, it was up to each agency to identify and correct problems.

In the event I/O staff could not correct a problem, the Job Call List was used to contact the appropriate personnel. Once a problem had been resolved, I/O would reinitiate the process and would monitor the job until successful completion.

Automated scheduling was managed through the software, CA Scheduler, which monitored or manipulated job streams as necessary. Agencies set up regular jobs through CA Scheduler or sent an email to Production Control to run specified jobs. Production Control continued to identify job requests that could be placed into CA Scheduler. It was up to the agency to ensure production job requests were appropriately approved and authorized.

No significant exception noted; however, standardized policies and procedures had not been developed.

Department Description of Control: I/O instructions are embedded within JCL streams as well as recorded in hard copy documentation maintained by Production Control organized by production job. System logs, hardcopy flows, and schedules are used for informational purposes. I/O daily shift reports that contain abends, restores, and corrections to production jobs are created and emailed to each legacy agency.

Tests Performed: Reviewed documentation and interviewed staff.

Test Results: I/O instructions were embedded within JCL streams. System logs, hardcopy flows, and schedules were utilized for informational purposes. Hardcopy flows were sent to the night shift to assist in problem resolution.

I/O daily shift reports were created for CMS, HFS, DOT, and DHS. I/O daily shift reports were not created for DCEO, DPH and EPA.

No significant exception noted with CMS, HFS, DOT, and DHS I/O control; however, I/O control was the responsibility of DCEO, DPH, and EPA, and not managed by the Department.

Department Description of Control: The Output section is responsible for printing and distribution of all documents and reports generated as a result of processing jobs for the departments mentioned above. Hardware includes high-speed Xerox laser printer types DP180 and DP65, and impact printer type IBM6262. Print queue's are manipulated for resource management purposes. Backups of forms, fonts, logos, and signatures, stored on the printers, are performed and sent offsite. Reprint needs are reported to and completed by Production Control or Input personnel. Service personnel are contacted for hardware problems. Printer usage is logged and monthly reports are produced. Monthly job performance reports are produced and submitted to management. Inventory is monitored, orders are created and tracked.

Tests Performed: Reviewed monthly job performance reports, inventory processes, and interviewed staff.

Test Results: The Department's Description of Controls states, "The Output section is responsible for printing and distribution of all documents and reports generated as a result of processing jobs for the departments mentioned above." However, we noted the Output section was responsible for printing and distribution of all user agencies and not just these seven consolidated agencies (CMS, DHS, HFS, DCEO, DPH, DOT and EPA).

Department staff stated comprehensive and standardized policies and procedures had not been developed, and the Department used individual agency legacy policies and procedures to print and distribute documents.

Backups of printer forms, fonts, logos and signatures were performed once a week and then rotated to the Regional Vault.

Contact information for service personnel was posted by the printers and maintained by Department staff.

The Department used individual agency legacy policies and procedures for printer usage logs.

The Department used individual agency legacy policies and procedures for the creation of monthly job performance reports for HFS, DHS, and CMS. Performance reports were not created for DOT, DCEO, DPH and EPA.

Inventory was monitored and orders were created and tracked.

No significant exception noted; however, standardized policies and procedures had not been developed.

Department Description of Control: Physical control over the distribution of printed material picked up at the Harris Facility is explained in written correspondence to each consolidated agency. This correspondence outlines how individuals picking up a report must identify themselves and state which report(s) they are to receive, be listed in the "Focal" system which contains a list of individuals authorized to pick up reports from I/O Control, and sign a report manifest indicating receipt of the correct report(s).

Tests Performed: Reviewed correspondence, report manifest, and interviewed staff.

Test Results: On November 21, 2006, the Department distributed a memorandum to users of the Department's I/O Print Services documenting the relocation of the print shop and the new security controls in place for picking up the reports.

The Focal system documented the authorization listing of individuals who were authorized to pick up reports.

During our review, we reviewed the report manifest, noting one out of 34 individuals tested was not authorized to pickup reports.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls that we were able to test were operating with sufficient effectiveness to achieve the control objective. However, the Description of Control for Input and Output did not apply to some agencies listed.

To strengthen the controls, we recommend the Department develop standardized Input and Output policies and procedures for use by all consolidated agencies. In addition, the Department should ensure only authorized individuals are permitted to receive reports.

OPERATIONS
Enterprise Production Operations Services
Library Services

EXISTING ENVIRONMENT

Department Description of Control: The Tape Library is located at the Central Computer Facility and is responsible for media storage and movement. This unit provides 24 X 5 (Monday through Friday) services fulfilling customer requests and ensuring security and tracking of all mainframe cartridges. Tape Library is responsible for all tape orders, initializing, labeling, degaussing, or destruction.

Tests Performed: Reviewed ISD Media Guide, ISD Library Guide, staff schedules, and interviewed staff.

Test Results: The Tape Library, located at the Central Computer Facility (CCF), was responsible for the management of media storage and movement.

We reviewed the Tape Library staffing schedule for the month of October 2007. Our review indicated 13 of the 22 shifts were not staffed by Tape Library staff. Per Department staff, critical requests for tape library services would be performed by Command Center staff; routine tasks would be completed on the next shift by Tape Library staff.

The Department developed the ISD Media Guide and ISD Library Guide, dated by sections, which provided procedures on how to manage tape orders, initializing, labeling, degaussing, or destruction for media storage and movement.

No significant exception noted; however, the Tape Library was not adequately staffed to provide 24 X 5 services.

Department Description of Control: The "Library Services Vault Transmittal Procedures" outlines the procedures to be followed during the movement of media. This includes transportation of media to and from the secured off site vault. Security and Service Delivery staff and Tape Librarians are responsible for confirming that individuals are authorized to deliver or remove media. A Security and Service Delivery staff person and a Tape Librarian verify that the triplicate Media Transmittal/Services Authorization Request forms are correct, signed, and retain a copy.

Tests Performed: Reviewed the ISD Tape Library Guide, Media Transmittal/Services Authorization Request forms, authorization memos and listings, and interviewed staff.

Test Results: The Department developed the ISD Tape Library Guide, dated by section, which included procedures for Library Services Vault Transmittals. The Guide provided information for the step by step process in Tape Library’s daily functions.

Security and Service Delivery staff were responsible for updating the authorization listings to ensure only authorized personnel pick up media. In addition, Tape Librarians confirmed and verified that individuals were authorized to deliver or remove media by utilizing the authorization listings.

When a Tape Librarian received a Media Transmittal/Services Authorization Request form, they would ensure the form was properly completed. However, Security and Service Delivery staff did not verify the accuracy of the forms.

We reviewed 25 Media Check-In and 25 Media Check-Out Transmittal Forms for December 5, 2007, to ensure the forms were correctly completed, noting 49 of 50 were properly completed. We noted all 50 of the transmittal forms reviewed were approved by authorized staff.

No significant exception noted; however, Security and Service Delivery staff did not verify forms as outlined in the Description of Control.

Department Description of Control: All media is identified with unique tracking alpha numeric identification numbers (volume serial number). The Tape Management System (TMS) is utilized to track and record the location of media. Carts not listed in TMS are transient carts recorded in a database called the Transient Tape System (TTS). The media in and out transmittals are used in the same manner for these types of tapes.

Tests Performed: Reviewed tape locations and interviewed staff.

Test Results: The TMS tracked tapes by the VOLSER and was utilized by the tape librarians to track and record the location of tapes/cartridges. Tape librarians continually maintained and updated TMS to provide users with the proper location and status of their tapes.

Transient tape tracking began when the user checking transient tapes into the library used the Media Check-In Transmittal Form. The transient tape was logged into the library by adding it to TTS.

We reviewed over 180 tapes, noting all were identified with unique tracking alpha numeric identification numbers.

No significant exception noted.

Department Description of Control: Twice a year, Security and Service Delivery staff send user agencies Security Authorization List, an Information Management System Authorization List, and a Tape Diskette Authorization List, which are to be updated.

Tests Performed: Reviewed memos, agency updates, and interviewed staff.

Test Results: Twice a year the Security and Service Delivery staff request agencies to update the various security authorization listings.

During our review, we noted the Security and Service Delivery staff requested agencies to update the authorization listings in April 2007 and October 2007. In addition, we noted the agencies had returned updated authorization listings to the Security and Service Delivery staff.

No significant exception noted.

Department Description of Control: CCF Tape Media staff performs tape drive monitoring functions, drive maintenance, tape mounting, dismounting, and file interface with the Automated Cartridge System (ACS) to satisfy system and sub-system requests. Services are provided 24 X 7 to fulfill customer requests. The CCF Tape Media Guide is utilized for reference in performing job functions.

Tests Performed: Reviewed CCF Tape Media Guide, staffing schedules, and interviewed staff.

Test Results: CCF Tape Media staff performed tape drive monitoring functions, drive maintenance, tape mounting, dismounting, and file interface with the Automated Cartridge System (ACS) to satisfy system and sub-system requests.

The Department developed the ISD Tape Media Guide, dated by section, which provided staff guidance with job duties.

We reviewed the CCF Tape Media staffing schedule for the month of October 2007 and found staff were available to provide 24 X 7 services.

No significant exception noted.

Department Description of Control: Library Support staff are responsible for migrating test environments to production libraries. Production libraries are protected by security software to allow only updates or edits to be performed by Library Support. Backups associated with all production libraries are performed by Library Support and will have designated backups sent to and from vault. All moves are performed with documentation and verification.

Tests Performed: Reviewed production libraries, move to production documentation, and interviewed staff.

Test Results: The Department was responsible for production libraries for four agencies: Department of Human Services (DHS), Department of Healthcare and Family Services (HFS), Department of Central Management Services (CMS), and Department of Transportation (DOT). The Department was not responsible for other agency moves to production.

Department staff stated comprehensive and standardized policies and procedures for moves to production had not been developed. Department staff generally used the individual agencies' legacy processes.

We reviewed 34 moves to production forms from October 5, 2007 to January 15, 2008, noting all were appropriately authorized.

No significant exception noted; however, standardized policies and procedures had not been developed to control moves to production.

Department Description of Control: For CMS, DHS, HFS, and DOT, Tape Administration staff document tape activities on the daily TGS report and a manually produced report. Tape Administration staff manages technical duties in conjunction with the development and control of the Tape Management System (TMS) and Tape Generating System (TGS). They also recommend and implement tape control features, project tape media usage, manage the resolution of tape control features, tape media listings and reports for the various agencies.

Tests Performed: Reviewed TGS reports and interviewed staff.

Test Results: The TGS and manually produced reports were used to document tape activities.

DHS and HFS utilized the TGS report via an online reporting tool.

CMS and DOT used manually produced reports to review tape activities.

We reviewed the TGS and the manually produced reports for February 6, 2008, noting reports contained dates, report name, and appropriate detailed information regarding agency tapes.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. However, to enhance the Department's controls, the Department should:

- Develop standardized policies and procedures for moves to production.
- Provide adequate staffing levels to the Tape Library to ensure availability to user agencies 24 hours a day, five days a week.
- Ensure all media transmittal forms are properly completed.

CHANGE CONTROL

EXISTING ENVIRONMENT

Background Provided by the Department: The Department's change management services are currently facilitated through separate systems based on processing platform and/or technology area.

Department Description of Control: Mainframe Platform: All mainframe changes are tracked in the Information Management System (INFOMAN) and governed by the CMS Change Management Policy and the Department's Information Management System guidelines.

Tests Performed: Reviewed CMS Change Management Policy, Information Management System Guidelines, INFOMAN change requests, and interviewed staff.

Test Results: The Department developed the CMS Change Management Policy (Policy), effective December 1, 2007 and the Information Management System Procedures (INFOMAN Procedures), last revised January 15, 2008. During our review, the Department implemented the Policy to facilitate the management of change requests. However, our review of the Policy and the legacy INFOMAN Procedures indicated inconsistent instructions between the two.

Our detailed review of a sample of INFOMAN change requests indicated they complied with the INFOMAN Procedures; however, due to the inconsistencies between the Policy and INFOMAN Procedures, the INFOMAN change requests did not comply with the Policy.

The INFOMAN Procedures provided a step-by-step guide on how to enter a problem ticket or change request into the Information Management System. According to the procedures, "any alterations to the mainframe operating environment will be recorded and regulated within established process and procedural guidelines for Change management until such time that this process is folded into the Remedy System."

We reviewed 25 INFOMAN change requests to ensure all required fields were completed and each request was properly tested, noting no exceptions. Additionally, the INFOMAN Procedures required three approvals; Operations, Coordinator, and Floating Manager. Our review indicated the 25 INFOMAN change requests had been properly approved.

Changes followed the INFOMAN procedures; however, due to inconsistent policies and procedures, the INFOMAN change requests did not follow the Policy.

Department Description of Control: Network Platform: Network Operations, LAN Services, and Enterprise Network Support changes are tracked in the Remedy Change module governed by the CMS Change Management Policy and Remedy Change Guide. In parallel to this process, Network Operations and Enterprise Network Support changes are also tracked in the ICN Remedy Trouble Ticket module. The CMS/ICN WAN Change Management process is utilized by

Network Services and Field Operations teams responsible for making network related changes, and follows the CMS Change Management Policy.

Tests Performed: Reviewed CMS Change Management Policy, Remedy Change Guide, CMS/ICN WAN Change Management Process, Remedy Change tickets, ICN Remedy Change tickets, and interviewed staff.

Test Results: In January 2008, the Department implemented the Remedy Change Module to control Network Platform change requests. In addition, the Department developed and implemented the CMS Change Management Policy (Policy), effective December 1, 2007 and the Remedy Change Guide (Guide), effective January 9, 2008, to provide guidelines over Remedy change requests.

According to the Policy, "a CAC will meet regularly to review RFCs and ensure reviews and communications are being satisfactorily performed." We reviewed 25 change requests for CAC approval, noting eight did not indicate CAC approval.

Additionally, the Policy stated notification procedures would be documented in individual change management procedures; however, notification procedures for Remedy had not been developed.

The Remedy Procedures were divided into eight steps, which identified "specific instructions/requirements." During our review of the Remedy Procedures, we noted they did not include procedures which addressed the notification to users, the level of testing to be conducted and the process for emergency changes. In addition, the Remedy Procedures made reference to the "Change Specification Template", which had not been developed.

We reviewed 25 Remedy change requests, noting none complied with the Remedy Procedures. Specifically, we noted:

- Deliverables were not identified.
- Business Owner reviews were not indicated.
- Notifications were not documented.
- Verification of change implementation was not indicated.

During our review of the 25 Remedy change request, we noted 23 requests had an impact criteria of medium or high, which required change manager and CAC approvals. Of the 23 change requests, 15 were missing one of the required approvals.

The CMS/ICN WAN Change Management Procedure, effective January 2, 2008 provided guidance in the event an ICN Remedy change ticket was required.

We reviewed 14 CMS Remedy and ICN Remedy change requests noting:

- Two CMS Remedy change requests did not have a corresponding ICN Remedy change requests.
- 12 change requests did not have the customer notification indicated.

- Acceptance and Post Test Plans were not completed for any of the change requests.
- One change request, with an impact of urgent, did not have proper approval.

The CMS Remedy change requests and the ICN Remedy change requests did not follow the applicable policy, procedures, or guidelines.

Department Description of Control: Regardless of platform, the below described path is followed for control of change:

- Changes are initiated by the Shared Services Technician or Manager as a result of an Enterprise Service Request (ESR), internal work assignment, or a configuration change.
- The Shared Services Technician or Manager identifies the changes to be made and generates a change request.
- Change requests are assessed for content and readiness.
- Changes are approved and appropriate parties are notified based on change impact.
- Changes are implemented.
- Changes are reviewed.

Tests Performed: Reviewed Remedy change requests, INFOMAN change requests and interviewed staff.

Test Results: The Department's Policy and INFOMAN Procedures did not correspond with the process described in the Description of Control. As a result, the change requests reviewed did not meet all the criteria listed in the Description of Control.

The change management process (Policy and INFOMAN Procedures) and actual practices did not correspond with the process described in the Description of Control.

OVERALL CONCLUSION

The Department had not implemented a consistent enterprise-wide process to control changes across all platforms. However, change requests generally complied with individual procedures and practices. To enhance the current process, the Department should ensure policies, procedures, and guidelines provide clear and consistent controls over change requests. Specifically, the Department should review current policies, procedures, guidelines and associated Description of Controls, and ensure all contain consistent and compatible information.

SECURITY ADMINISTRATION

EXISTING ENVIRONMENT

Background Provided by the Department: As outlined in the following controls, the Department's security posture is comprised of compliance and auditing functions that include corrective action planning, security assessments, security awareness promotion, policy development, and continuity of operation planning.

Department Description of Control: Corrective action plans that enhance the overall security posture of the Department are developed by Risk Management and are based on recommendations generated by external audit reviews and internal security assessments.

Tests Performed: Reviewed corrective action plans and interviewed staff.

Test Results: The Department developed a Corrective Action Status Report based on the recommendations from the 2007 BCCS Third Party Review. The 2007 BCCS Third Party Review included numerous recommendations, including 20 that were related to issues that were classified as significant deficiencies. We reviewed the Report to determine if the 20 recommendations were included, the inclusion of corrective action proposals, and the current status of each of the 20 recommendations.

The Department's plan did not include any reference to 9 of the 20 recommendations. The other 11 recommendations were included in the plan; however, corrective action proposals were generally missing, and no issues had been corrected.

The Risk Management Unit (Technical Safeguards) conducted 12 internal security assessments from November 2006 through January 2008, and completed an assessment report for each engagement. The assessment reports identified findings (weaknesses) and outlined general recommendations to correct the weaknesses.

During our audit work, we followed-up on the implementation status of the recommendations from seven internal security assessments that were performed in the audit period and found that, although some weaknesses had been corrected, a number of high priority weaknesses still needed to be addressed.

Although a framework to develop corrective action plans existed, there were deficiencies in the implementation.

By not addressing all the issues outlined in external audit reports and internal security assessments; the Department increased the risk of security exposures impacting the disclosure, integrity, and availability of information.

Department Description of Control: Security assessments are conducted and include vulnerability scans, penetration testing, and patch level review to identify weaknesses. The

Technical Safeguard Unit Security Audit Procedures Rules of Engagement document, located on a secure, shared network drive, outlines the steps to follow when conducting these assessments.

Tests Performed: Reviewed security assessments, Security Audit Procedures Rules of Engagement, and interviewed staff.

Test Results: The Technical Safeguards Unit conducted 12 security assessments that included discovery, enumeration, vulnerability assessment and penetration tests. Seven internal security assessments were performed from April 2007 through January 2008.

The Technical Safeguards Unit developed the Security Audit Procedures Rules of Engagement procedures. The Rules were available on a secured, shared network drive and per Technical Safeguards Unit staff, the procedures were being followed.

The procedures indicated a contract was to be developed and approved by the unit in which the assessment was being conducted. The contract was to outline the scope of testing, and the test plan. The procedures stated upon completion of the assessment, a report with recommendations would be developed and provided to the appropriate management.

During the audit period, the Technical Safeguards Unit conducted seven different security assessments. Our review indicated each assessment had an approved contract, which outlined the scope of testing and the testing plan. In addition each assessment had a report with recommendations provided to management.

No significant exception noted.

Department Description of Control: Security awareness is provided through the state's Enterprise web which includes a link to the IT Risk Management site (http://intra.state.il.us/it-risk/default.htm) that provides security-related news releases, tips, security posters, and other guidelines.

Tests Performed: Reviewed the IT Risk Management website and interviewed staff.

Test Results: On October 26, 2007, the Chief Security Office announced the creation of the IT Risk Management website. The announcement indicated the website contained "information on BCCS policy and corresponding security awareness", including "Computer Based Training, video presentations, and cyber-tips and guidelines."

During our review of the website, we noted it provided very high-level and general security information. In addition, the website provided links to federal and organizational security sites. However, the website did not contain information on BCCS policies, Computer Based Training, or video presentations.

On October 3, 2007, the Department announced the establishment of October as "National Cyber Security Awareness Month." As part of the announcement, the Department provided agency

CIOs with the “National Cyber Security Awareness Month” toolkit, which included calendars, posters, bookmarks, and CDs.

No significant exception noted.

Department Description of Control: Current approved security policies include Change Management, Data Breach, Laptop Data Encryption, Midrange Backup, and Resource Access. These policies have been developed based on information supplied at informal meetings with Bureau staff, from known operational practices, and from principles outlined in industry best practices. Prior to submission to the Deputy Director, policies are reviewed by the Bureau’s Chief Security Officer and the Bureau’s Deputy General Counsel. Policies are published by posting to the appropriate repository dependent upon the sensitivity of the material and the targeted audience. The Information Technology Security Policy, Chapter 4 Section 3 of the Department Policy Manual remains in effect.

Tests Performed: Reviewed policies and interviewed staff.

Test Results: The Department developed the Change Management, Data Breach, Laptop Data Encryption, Midrange Backup and Resource Access policies, which were dated December 1, 2007. Per Department staff, the policies were developed based on industry practices, operational practices and meetings with Department staff. The policies were reviewed and approved by the Department’s Chief Security Officer, Deputy General Counsel, and Deputy Director.

The policies outlined in the Department’s Description of Control as current and approved, were actually not in effect, and were not published by posting them to the appropriate repository. In addition, no documentation was provided to demonstrate that policies were distributed to appropriate audiences.

Per the Chief Security Officer, the Department was awaiting Union approval on the policies.

Our review of the Department’s Intranet and substantiated by interviews with the Department’s Chief Security Officer, indicated the following policies were actually in effect:

- Information Technology Security Policy, dated April 26, 2002,
- CMS Information Technology Security Policy, dated December 11, 2001,
- Statewide Internet Security Policy, dated December 11, 2001,
- Information Security Policy, LAN/OA, dated May 26, 1995, and
- Statewide Information Security Policy, BCCS/CCF (Internal), dated February 3, 2003.

As outlined in the last two BCCS Third Party Reviews, the above policies did not reflect the current technological environment or address security concerns.

Our review of the policies dated December 1, 2007, indicated they were targeted to a broad audience and at a general overview level. The policies did contain references to detailed procedures; however, the procedures had not been developed.

The policies currently published on the Intranet did not reflect the current technological environment or address security concerns. In addition, the policies dated December 1, 2007 were not effectively communicated or even placed on the Department's Intranet. Thus, a consistent and effective method to communicate current policies to users was not implemented.

The lack of adequate security policies increases the risk of security exposures impacting the disclosure, integrity, and availability of information.

Department Description of Control: Continuity of Operations Plan (COOP) information, based on a COOP checklist, has been collected and submitted to the Department's Emergency Management Coordinator in the ongoing development of the Department Continuity of Operations Plan (COOP).

Tests Performed: Reviewed COOP plan and interviewed staff.

Test Results: The Department worked with the Illinois Emergency Management Agency (IEMA), to develop the COOP plan. The COOP plan was developed for compliance with the federal Emergency Management Accreditation Program (EMAP) audit, which the State achieved EMAP accreditation. The COOP plan was updated semi-annually and maintained online by IEMA.

No significant exception noted.

Department Description of Control: The State of Illinois Public Key Infrastructure (PKI) is required to have a PKI compliance audit conducted on the Illinois Root certification authority on an annual basis. This is to validate the operational compliancy of the system. The most recent compliance audit is located at http://www.illinois.gov/pki/default.cfm.

Tests Performed: Reviewed audit report.

Test Results: A compliance audit was conducted for the period of June 1, 2006 to July 1, 2007. The audit provided an unqualified opinion with recommendations. The audit was posted on the PKI website.

No significant exception noted.

OVERALL CONCLUSION

The Department has the primary responsibility of providing IT services to State Government. Therefore, it is imperative the Department have in place a framework to promote and apply prudent, comprehensive, and effective security practices. Even though this deficiency was included in the last two Third Party Reviews, the Department had not taken comprehensive action to remedy the control weakness. To ensure the framework exists to promote and guide security practices, the Department should:

- Thoroughly review and update security policies to address the current technological environment, consolidation issues, and present-day risks. Once finalized, the policies (and associated procedures) should be implemented, formally communicated, and disseminated (along with being placed in the appropriate repository) to all affected parties.
- Enhance the process of developing proposals and implementing corrective plans to ensure all significant issues are adequately addressed, and corrected within a reasonable timeframe.
- Ensure the Risk Management Unit develops and implements comprehensive corrective action plans from internal security assessments. The plans will help ensure all significant issues are adequately addressed, and corrected within a reasonable timeframe.

PHYSICAL SECURITY

EXISTING ENVIRONMENT

Department Description of Control: The Department protects information system hardware and other assets through the use of access control and video surveillance. The H/V system, Access Cards, Badges, and video surveillance are used to limit or monitor physical entry into the Central Computer Facility, Communications Building, the Business Services Building, the BCCS Warehouse, and the Harris Facility.

Tests Performed: Toured facilities and interviewed staff.

Test Results: The Central Computer Facility (CCF), Communications Building, Business Services Building, BCCS Warehouse, and the Harris Facility were secured by an access control system (H/V system). The access control system was used to limit and monitor access into the facilities.

Additionally, the CCF, Communications Building, Business Services Building, BCCS Warehouse, and the Harris Facility utilized video surveillance to monitor the facilities.

No significant exception noted.

Department Description of Control: Access control includes limiting physical entry into buildings and/or locations within a building and uses Access Cards, Badges, and/or Pin Codes to control entry. Access Cards and PIN Codes are issued by the Physical Security Coordinator to Department personnel based on business need and job responsibility. Badges are issued by contracted Security Guards to visitors for temporary entry into a building. The Bureau Physical Security Coordinator processes emailed access requests from only designated authorities as identified in the Approval Authorization Matrix and Badge Production Matrix.

Tests Performed: Toured facilities, reviewed BCCS Facilities Access Policy, Badge Production Matrix, and Approval Authorization Matrix.

Test Results: Access controls (Access Cards, Badges, and/or Pin Codes) were used to limit physical entry into buildings and/or locations within buildings.

In addition, the CCF, Communications Building, and Harris Facility utilized Security Guards and a Building Admittance Register to document vendors, visitors, or employees who forget their ID badges.

The Physical Security Coordinator issued access cards and PIN Codes. The Department's "BCCS Facilities Access Policy" dated March 1, 2008 provided information on granting, assigning, and revoking user access to facilities. In addition, the Department had a Badge Production Matrix that detailed the procedure/process utilized to issue badges.

We noted the Badge Production Matrix and the BCCS Facilities Access Policy did not directly correspond to the Department's Policy Manual on Employee Separation. As a result, the Physical Security Coordinator did not always receive timely notification of employee separation. In addition, although it was practice to send badges from separated employees to the Physical Security Coordinator, it was not required by Policy.

The BCCS Facilities Access Policy was dated March 1, 2008. We noted there were no new hires or separations after March 1, 2008 to review for compliance with the policies. However, we noted the following:

- The Department did not maintain appropriate documentation to ensure individuals who requested access were properly authorized. This process was conducted via email and the Physical Security Coordinator did not maintain those emails.
- The Department did not have a process in place to ensure access rights were disabled in a timely manner. The system used to disable access rights did not maintain the appropriate information to determine when the rights were terminated. The system could only verify current status of individual's access rights.

We selected 20 individuals who had access to the CCF 3rd floor to determine the appropriateness of the access rights. We noted 3 of the 20 individuals no longer needed access but had not had their access rights removed. However, in all three cases, the access rights were automatically disabled after the absentee limit was reached. Even though the Department maintained an absentee limit, appropriate controls to ensure the timely deactivation of access rights did not exist.

Although a process existed to assign access cards; documentation supporting the approval of access rights was not maintained. In addition, the revocation rights of separated employees or contractors were not always immediately revoked.

<u>Department Description of Control:</u> The Hirsch/Velocity (H/V) system is used to create and track Access Cards. Creation of an Access Card requires identity authentication based on generally accepted identification sources such as a valid driver's license, State ID card, or U.S. passport. A picture of the individual is taken and stored in the H/V system along with credentialing source information. The H/V System Administrator's Manual contains instructions to create the physical card or badge.

<u>Tests Performed:</u> Reviewed Badge Production Matrix and H/V System Administrator's Manual.

<u>Test Results:</u> The H/V system was used to create and track Access Cards. A photo of the individual was taken and stored in the H/V system along with credentialing source information. We reviewed the system records for seven staff members and noted each record contained a picture and driver's license or ID number.

The H/V System Administrator's Manual contained instructions to create the physical card or badge.

No significant exception noted.

Department Description of Control: The H/V system records and logs the use of Access Cards. Reports can be produced to list who has access to what buildings and locations as well as which credential was used where and when. Reports are generated upon request by the Resource Custodian or by Personnel. In addition, application of employee pass-back functionality and absentee limits help control physical access to facilities.

Tests Performed: Reviewed H/V system logs and reports, and interviewed staff.

Test Results: The H/V system recorded and logged the use of Access cards. The H/V system produced several types of reports to assess facility security and activity.

We reviewed the transaction log report, noting it contained information regarding the date and time of access card was used, description of access (exit or entry), access granted or denied, door name, and user name and ID number.

The Department set an absentee limit in the access card system to disable an access card after the predefined period of inactivity. In addition, the Department implemented pass-back technology to help prevent individuals from following ("piggy backing") others into the facility. We verified the absentee limit in the access card system, and observed the pass-back technology in place at the CCF and Communications Building.

No significant exception noted.

Department Description of Control: Access Cards are FIPS 201-1 compliant and contain text that outlines cardholder responsibilities as well as instructions on what to do if a lost badge is found. Access Cards contain the name and photo of the "owner", an anti-counterfeit feature, and expiration date. Once the Physical Security Coordinator is notified of employee separation or other circumstance for disabling access, card access is disabled by making the appropriate entry into the H/V system. Recovery of a separated employee's Access Card is the responsibility of the supervisor per Chapter 2, Section 13 of the Department's Policy Manual.

Tests Performed: Reviewed Access Card and the Department's Policy Manual.

Test Results: The access cards (badges) were FIPS 201-1 compliant as they contained the following:

- Photo.
- Name.
- Agency/company affiliation.
- Expiration dates.
- Agency Card Serial number.
- Issuer Identification.

The access cards also provided card holder responsibilities, and instructions for the postage free return to the Department if lost and found.

According to the Department's Policy Manual -- Employee Separation, Chapter 2; Section 13, dated September 1, 1998, all State owned items must be returned to the State when an employee separates service with the Department. Additionally, "the Supervisors are responsible for collecting a separated employee's telephone credit cards, door and desk keys, parking lot stickers, Data Center admittance cards, identification cards, vehicles, and special equipment."

We reviewed 10 separated individuals, noting two cases where the access card had not been returned as required by the Policy.

No significant exception noted, however, access cards were not always returned as required by Policy.

Department Description of Control: For those buildings staffed with 24/7 security guard protection, Badges are issued to visitors and to employees who forget their assigned Access Card. Those issued a Badge sign the Building Admittance Register recording their name and Badge ID. This is used as a log to track who is in the building. Security Guards have been instructed to inventory Badges at the start of each shift to ensure accountability.

Tests Performed: Reviewed Building Admittance Registers and Badge Inventory Sheets.

Test Results: An individual without an authorized access card was required by Security Guards to sign a Building Admittance Register to gain admittance. We reviewed a sample of two days of Building Admittance Registers for both the CCF and Communications Building. We found general compliance with the completion of the Registers; however, in several cases the time-out field was not completed.

Security Guards were required to inventory temporary badges at the start of each shift to ensure accountability. We reviewed a sample of temporary badge inventory sheets for several days for both the CCF and Communications Building. We noted no exceptions in the completion of the inventory sheets.

No significant exception noted.

Department Description of Control: For those buildings not staffed with 24/7 security guard protection, each entry door remains locked. Only a limited number of people from the inside may release the locked door. Audio and visual capabilities allow verification of the person entering.

Tests Performed: Toured Business Services Building and BCCS Warehouse.

Test Results: Entry into the Business Services Building was controlled by an access card reader and monitored by a digital video and audio surveillance camera. When someone without an authorized access card needed access to the building, staff viewed the video camera to allow entry into the building.

Entry into the BCCS Warehouse was controlled by an access card reader and monitored by a video surveillance camera. When someone without an authorized access card needed access to the Warehouse, staff identified individuals through glass doors to allow entry.

No significant exception noted.

Department Description of Control: Networked video cameras monitor exterior doors and sensitive interior entrances. Security Guards as well as the Bureau Physical Security Coordinator have remote view capability for all networked cameras.

Tests Performed: Toured facilities and reviewed monitoring capabilities.

Test Results: Video cameras were used to monitor the CCF, Communications Building, Business Services Building, BCCS Warehouse, and the Harris Facility.

The Physical Security Coordinator and the Security Guards at the Communications Building had remote view capability of all networked video surveillance cameras.

No significant exception noted.

Department Description of Control: In order to mitigate the risk of a power failure, the Central Computer Facility is supplied by two different sources and is equipped with an uninterruptible power supply (UPS). Within an allotted time the Department's generators will engage. The Department has in place a service contract for the UPS to provide routine preventive maintenance and remedial services as required.

Tests Performed: Reviewed contracts, maintenance reports, and interviewed staff.

Test Results: The electrical power for the CCF was from two different feeds from City Water Light and Power (CWLP). In the event of power failure the UPS was supposed to engage immediately and the generators were supposed to engage within 90 seconds.

During fieldwork the Department experienced a power interruption/failure at the CCF. Although some lighting and equipment was functioning, some critical systems, including the cooling and security systems experienced problems. As a result, service was impacted for approximately two hours and some equipment was damaged and data lost. The Department analyzed the event and developed a list of suggested actions, including the hiring of a vendor to perform an electrical/mechanical review of the CCF.

The Department had a service contract to provide routine preventative maintenance on the UPS components. We reviewed maintenance reports for the UPS from December 2007 and March 2008. The March report indicated the UPS batteries were in disrepair and needed to be replaced as soon as possible. Per Department staff, a procurement process for new batteries was initiated on October 29, 2007.

The Department had a service contract to provide routine preventative maintenance on the generators. We reviewed maintenance reports for the generators from July 2007. The reports indicated all generators were in good operating condition.

The UPS batteries were in disrepair and needed to be replaced and an electrical/mechanical review of the CCF was necessary.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should:

- Update the Department's Policy Manual (section on Employee Separation) and the BCCS Facilities Access Policy to ensure and document the timely revocation of access rights. Specifically, we recommend:
    - Supervisors be required to obtain and submit access cards to the Physical Security Coordinator within 24 hours of separation for employees. If a card is not received by the supervisor, the Physical Security Coordinator should be immediately notified to remove access rights.
    - Contract managers (or the staff member who authorized access rights) be required to obtain and submit access cards to the Physical Security Coordinator within 24 hours of separation for contractors. If a card is not received by the supervisor, the Physical Security Coordinator should be immediately notified to remove access rights.
- Maintain documentation to support the approval of access rights for all individuals.
- Ensure UPS batteries are replaced as soon as possible.
- Ensure the electrical/mechanical review of the CCF is performed and actions are taken as appropriate.

PHYSICAL SECURITY
Bureau of Property Management (BOPM)

EXISTING ENVIRONMENT

Department Description of Control: The Bureau of Property Management (BOPM) maintains fire suppression and detection systems on the third floor of the Central Computer Facility, at the Communications Building, and at the Business Services Building.

Tests Performed: Reviewed contracts and toured facilities.

Test Results: The CCF computer room had fire suppression and detection systems that were Underwriter Laboratory approved and utilized an environmentally friendly gaseous agent, FM-200. During our tour of the CCF, we noted the fire suppression and detection system was last inspected in April 2006.

The Communication Building and the Business Services Building contained fire detection and suppression systems and/or fire extinguishers. During our tour of the facilities, we noted the fire detection and suppression systems and fire extinguishers were inspected within the last year.

No significant exception noted; however, the fire suppression and detection system at the CCF had not been inspected since April 2006.

Department Description of Control: BOPM is also responsible for the issuing and maintenance of real property keys. Although the Bureau may provide information to BOPM regarding key provisioning, BOPM has the final authority and responsibility for real property keys.

Tests Performed: Reviewed Telecom Key Inventory Listing, CCF Key Card file, and interviewed staff.

Test Results: The Department's Bureau of Property Management was responsible for the management of real property keys for the CCF and Communications Building.

Per Department staff, BOPM was not responsible for the issuance or maintenance of real property keys for the Business Services Building.

During our testing, we identified some deficiencies in tracking and maintaining real property keys.

Although not a significant exception due to the card-key system, procedures to effectively track and maintain real property keys at all facilities had not been implemented.

Department Description of Control: BOPM also manages a contract for security guard services at select locations. Security guard services are based on contract documented requirements (general orders), post orders, and special instructions. These special instructions are communicated via email from the facility manager to the security guards and are then included in the Pass Down Book. Fundamental activities of security guards include but may not be limited to access control, incident reporting, and perimeter patrol.

Tests Performed: Reviewed security guard contract, security guard instructions, and interviewed staff.

Test Results: The Department had entered into a master contract, to provide security guards at State facilities. The activities of security guards for the CCF and Communications Building included access control, incident reporting, and perimeter patrol.

The master contract outlined (general orders) personnel, training, location of assignment, vendor records, uniforms and equipment, standards of conduct, hours of work, and duties of security guards.

A Post Order Manual was available to provide security guards with guidance to perform their duties at the Communications Building. The Post Order Manual for the CCF was not located by the security guard.

Pass Down Books were available to provide additional instructions to security guards at the Communications Building and CCF. The books were both last updated in August 2006.

We did not identify any significant deficiencies in the security guard's performance of duties.

We reviewed documentation to support the completion of basic and/or refresher training for 10 guards, noting no exceptions.

Although security guards existed to protect facilities, information to assist in the performance of duties was not always available or updated.

Department Description of Control: BOPM contracts with janitorial services to perform duties at these facilities on a daily, weekly, and/or monthly basis. The contracts outline duties and timeframes. BOPM is responsible for ensuring that background checks and training are conducted for each janitorial employee.

Tests Performed: Reviewed janitorial contracts and interviewed staff.

Test Results: The Department had contracted for janitorial services for the facilities. The contract outlined janitorial duties.

We did not identify any significant deficiencies in the janitor's performance of duties.

During the audit period, there were 20 individuals assigned to the CCF, Communications Building, and other facilities for janitorial services. Per Department staff, a background check was only performed on four individuals and no training was conducted.

The Department had not conducted background checks or provided training for janitorial employees.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should:

- Ensure the fire suppression and detection system at the CCF is tested at least annually.
- Ensure information to assist in the performance of security guard duties is available and updated.
- Develop and implement procedures to effectively track and maintain real property keys.
- Complete background checks and provide training for janitorial employees as outlined in the Description of Control.

PHYSICAL SECURITY
Harris Facility

EXISTING ENVIRONMENT

Background Provided by the Department: Physical security at the Harris Facility is a joint effort between the Department of Human Services (DHS) and the Department's Bureau of Property Management.

Department Description of Control: Physical security controls protecting the Department's assets housed at the Harris Facility include:

- Security guards in the front entry way.
- Video cameras strategically located inside and outside the building.
- Proximity card readers requiring an active Access Card to allow entry.
- Limited access, brightly colored badges for use by individuals entering the building to pick up printed output from the I/O Control area.

Tests Performed: Toured Harris Facility, reviewed card reader system, access cards, badges, video surveillance system, and interviewed staff.

Test Results: During our review, we found the following physical security controls were in place to protect the Harris Facility:

- Security guards were stationed in the front entry way 24 hours a day, 7 days a week.
- Video cameras were located inside and outside the building.
- Proximity card readers required an active access card for entry to restricted areas and were located throughout the Facility.
- Brightly colored badges providing limited access were used to permit access to the I/O Control area.

To supplement our audit work, we examined a detailed review of the implementation of physical security controls over the Harris Facility that was conducted in conjunction with the Compliance Attestation Examination of the Department of Human Services for the period ending June 30, 2007. Several weaknesses in physical security were identified and reported in the Examination (Finding – 07-29 Physical Security Weakness). The finding included weaknesses such as:

- Access to restricted areas was excessive.
- Adequate controls over the distribution/collection of facility keys were not established.
- Some surveillance monitors located at the Harris Facility's guards' desk did not effectively display surveillance images.

Although physical security controls existed, some weaknesses were identified.

OVERALL CONCLUSION

Although physical security controls existed, controls over the Harris facility should be enhanced. Since physical security of the Harris Facility is a shared responsibility between the Department and the Department of Human Services, we recommend the Department work with the DHS to reassess physical security of the Harris Facility and ensure established controls are adequately implemented, and regularly monitored and enforced.

SYSTEM SOFTWARE
Zero Downtime Operating System (z/OS)

EXISTING ENVIRONMENT

Background provided by the Department: The primary operating system at the Department's Central Computer Facility is Zero Downtime Operating System (z/OS). z/OS is a complex operating system used on mainframes and functions as the system software that controls the initiation and processing of work within the computer.

Department Description of Control: Some of the subsystems that run on z/OS are CICS, DB2, IMS, RACF, MQ series, NEON, SMS, HSM, TSM, JES, CA-scheduler, Mobius, HSC, TMS, etc.

Tests Performed: Reviewed documentation identifying established subsystems and interviewed staff.

Test Results: z/OS functioned as the system software that controlled the initiation and processing of work within the computer. The Department had defined multiple subsystems.

No significant exception noted.

Department Description of Control: The System Management Facility (SMF) records the activity within the operating system.

Tests Performed: Reviewed system recording options, security reports, and interviewed staff.

Test Results: The System Management Facility recorded operating system activities. In addition, the Department had ensured recorded activities were adequately backed-up.

No significant exception noted; however, the Department had not established its standard SMF recording options on the systems integrated from the Department of Revenue.

Department Description of Control: The agency security software administrator must submit a request to the CMS security software staff if a user ID needs to have TSO access on the mainframe.

Tests Performed: Reviewed process for requesting access and email notifications.

Test Results: Authorized user-agency representatives would send an electronic mail message to security software staff to request TSO access.

No significant exception noted.

Department Description of Control: Security software and system options are implemented to secure libraries, and to protect resources and data.

Tests Performed: Reviewed security profiles, system configurations, system options, and interviewed staff.

Test Results: Security software and system options were implemented to secure libraries, and protect resources and data.

No significant exception noted; however, the Department had not established its standard system options on the systems integrated from the Department of Revenue.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should ensure its standard system options are consistently established on all systems.

SYSTEM SOFTWARE
Zero Downtime Virtual Machine (z/VM)

EXISTING ENVIRONMENT

Background provided by the Department: The Department's secondary operating system utilized at the Central Computer Facility is Zero Downtime Virtual Machine (z/VM). z/VM is time-sharing, interactive, multi-programming operating system for IBM mainframes. The major subsystem that is supported in z/VM is NOMAD.

Department Description of Control: The agency RACF administrator must request and obtain a VM User ID from the z/VM staff. Agencies are assigned user IDs with the most restrictive security rights.

Tests Performed: Reviewed process for granting access rights.

Test Results: During our review, we noted the following nine agencies utilized z/VM:

- Department of Healthcare and Family Services.
- Department of Children and Family Services.
- Department of Transportation.
- Department of Public Health.
- Department of Central Management Services.
- Department of Employment Security.
- Department of Human Services.
- Department of Revenue.
- Illinois Racing Board.

Authorized user agency representatives would send an electronic mail message to z/VM staff to request a z/VM User ID.

z/VM user IDs were assigned the most restrictive access rights. Only z/VM staff and service machines had less restrictive access rights.

No significant exception noted.

Department Description of Control: The z/VM directory is restricted, which contains information regarding user IDs, mini-disk size and location, and operating functions.

Tests Performed: Reviewed security reports and confirmed with Department staff.

Test Results: Access to the z/VM directory was limited to z/VM staff.

No significant exception noted.

Department Description of Control: Security software and system options are implemented to secure libraries, and to protect resources and data.

Tests Performed: Reviewed security software reports and confirmed with Department staff.

Test Results: System options and parameters were implemented to protect data and resources.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives.

SYSTEM SOFTWARE
Customer Information Control System (CICS)

EXISTING ENVIRONMENT

Background Provided by the Department: The Customer Information Control System (CICS) is a software product that enables online transaction processing. CICS allows numerous transaction types, entered from multiple terminals, to be processed concurrently by customer written application programs. CICS acts as an interface between the operating system and application programs.

Department Description of Control: The Department offers three different levels of CICS support for customers, described as follows:

- **Level One** – The Department supports only the CICS software. The customer is responsible for all security for the customer owned CICS regions.
- **Level Two** – The Department supports the CICS software, and maintains CICS System Definition File (CSD)/table definitions for the customer. The customer supplies the definitions to the Department and controls the application support. The Department and the customer owning agency share security responsibilities.
- **Level Three** – The Department supports the CICS software, maintains CSD/table definitions, and supports both CICS and the application software for the agency. The Department is also responsible for security for these regions.

Tests Performed: Reviewed CICS regions and interviewed staff.

Test Results: There were 36 CICS regions (13 production, 11 test, and 12 development).

The Department provided CICS support for user agencies as follows:

Level One Support

- Department of Human Services (6 regions)
- Department of Employment Security (2 regions)
- Department of Corrections (2 regions)

Level Two Support

- Department of Central Management Services (6 regions)
- Illinois Student Assistance Commission (2 regions)
- Department of Revenue (14 regions)

Level Three Support

- Department of Healthcare and Family Services (4 regions)

No significant exception noted.

Department Description of Control: Production regions are segregated from test and development regions to restrict access, based upon the various needs for each type of region. Restricted access to sensitive CICS transactions is established over production regions. Test regions have fewer access restrictions. Test regions allow programmers to test and debug against non-production files.

Tests Performed: Reviewed region listings, general resource classifications, and access rights to restricted commands.

Test Results: The production CICS regions were separated from the test and development/training CICS regions. Restricted access to sensitive CICS transactions was established over production regions. Non-production regions (test and development/training regions) had fewer access restrictions to allow programmers to develop and test applications.

No significant exception noted.

Department Description of Control: Security software and system options are implemented to secure libraries, and to protect resources and data.

Tests Performed: Reviewed system options, settings, definitions and security reports, and interviewed staff.

Test Results: Security software and system options were implemented to secure libraries and protect resources and data. In addition, restricted access to sensitive CICS transactions was established.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective.

SYSTEM SOFTWARE
Information Management System (IMS)

EXISTING ENVIRONMENT

Background Provided by the Department: Information Management System (IMS), which is an online database software subsystem, used as the control architecture under which online database system applications process. An IMS system is capable of running many different applications within a single definition of one or more “Message Processing Region” and one “Control Region”. The IMS applications can access IMS, DB2 and CICS data files.

Department Description of Control: Customers control their own TIMS and GIMS RACF definitions.

Tests Performed: Interviewed staff.

Test Results: Agency RACF Coordinators were responsible for permitting access to agency specific IMS resources. Access could be restricted to a specific IMS transaction (TIMS) or a group of IMS transactions (GIMS).

No significant exception noted.

Department Description of Control: Currently, there are four production IMS regions with 10+ testing regions.

Tests Performed: Reviewed region listing and interviewed staff.

Test Results: There were four primary production regions and over 10 testing regions.

No significant exception noted.

Department Description of Control: Security software and system options are implemented to secure libraries, and to protect resources and data.

Tests Performed: Reviewed system options, security reports and access screens, and interviewed staff.

Test Results: Security software and system options were implemented to secure libraries, and protect resources and data.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective.

SYSTEM SOFTWARE
DataBase 2 (DB2)

EXISTING ENVIRONMENT

Background Provided by the Department: DataBase 2 (DB2) is a relational database management system for z/OS environments, which the Department makes available to customers.

Department Description of Control: The Department has established ten+ subsystems at the Central Computer Facility.

Tests Performed: Reviewed subsystem report listing and interviewed staff.

Test Results: The Department had established over 10 subsystems at the Central Computer Facility.

No significant exception noted.

Department Description of Control: The Department has assigned staff to monitor the performance and problems of DB2. The DB2 staff is also responsible for software installation, maintenance and security.

Tests Performed: Interviewed staff.

Test Results: The DB2 Software Support Group, which consisted of one lead and three additional staff, was responsible for software installation, maintenance, security, performance monitoring, and database design.

No significant exception noted.

Department Description of Control: All customers who access DB2 are required to have a security software ID and password. The customer must authenticate to the security software first. If the customer authenticates, DB2 allows access. DB2 internal security verifies access rights to specific data.

Tests Performed: Reviewed security reports and interviewed staff.

Test Results: All users who accessed DB2 were required to have a security software ID and password. The user must authenticate to the security software first. If the user was authenticated, DB2 allowed access.

No significant exception noted.

Department Description of Control: The Department authorizes one user ID at each agency to coordinate the use of DB2 within the agency. This user ID allows each agency to create its own authority.

Tests Performed: Reviewed Agency DB2 Coordinator Listing and interviewed staff.

Test Results: Each user agency was required to assign a DB2 Coordinator for their agency, who in turn was responsible for assuring access privileges were adequately controlled within the user agency.

No significant exception noted.

Department Description of Control: The DB2 Software Support Group will monitor specific application problems when customers call. System performance is monitored on a continuous basis. The Department's Information Management System is utilized to report and document problems.

Tests Performed: Interviewed staff.

Test Results: When a user requested assistance, the DB2 Software Support Group monitored the application and reviewed the database design. Department staff used tools to monitor system performance.

The Department used the Information Management System, in addition to weekly status reports and email, to report and document problems to DB2 staff.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective.

SYSTEM SOFTWARE
Resource Access Control Facility (RACF)

EXISTING ENVIRONMENT

Department Description of Control: The Department utilizes security software to control access and protect resources. The security software is the primary tool for controlling and monitoring access to the Department's computer resources.

Tests Performed: Reviewed literature, security software reports, and interviewed staff.

Test Results: A security software package (RACF) existed and was used to control and monitor access to Department resources.

No significant exception noted.

Department Description of Control: Written procedures exist for the managing and maintenance of the security software.

Tests Performed: Reviewed procedures.

Test Results: The Department had a formal Mainframe Security Procedures Manual, which was updated in August 2006.

No significant exception noted.

Department Description of Control: The Department has appointed staff with primary responsibility for the implementation and administration of the security software

Tests Performed: Reviewed security software reports and interviewed staff.

Test Results: The Department assigned staff members with the primary responsibility to implement and administer security software. The access rights were appropriately assigned to these staff members.

No significant exception noted. However, we did note an excessive number of unused (revoked) IDs assigned to user agencies on the system.

Department Description of Control: A user ID is used to identify the client along with a password to verify the client's identity.

Tests Performed: Reviewed literature, security software reports, and interviewed staff.

Test Results: User IDs were used to identify a user's identity as a key control mechanism within RACF. RACF protected access and enforced 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.

No significant exception noted.

Department Description of Control: The Department maintains a log of all access attempts, which is used to monitor unauthorized access attempts and identify areas of weakness.

The Department has a procedure in place for the monitoring of security violations. The CMS Data Security Administrator reviews violations with CCF violation reports being distributed to staff for which they must be signed and returned with an explanation.

Tests Performed: Reviewed violation procedures and violation logs.

Test Results: The Department maintained the Resolution of RACF Violation Procedures, effective October 1, 2007. The CMS Data Security Administrator reviewed violations, and CCF violation reports were distributed to staff for explanation and signature.

No significant exception noted.

Department Description of Control: Clients are responsible for protecting their program and data files.

Tests Performed: Interviewed staff.

Test Results: User agencies were responsible for specifying the datasets to be protected and for properly utilizing the available security resources. When a user logged on to the Department's systems, a disclaimer was displayed, which informed users of their responsibilities, including protecting their program and data files.

No significant exception noted.

Department Description of Control: The agency RACF administrators have the capability of producing the reports for their agency.

Tests Performed: Interviewed staff and reviewed system menus.

Test Results: Utilities were available for RACF administrators for maintenance of user IDs, access rights, and reports for their agency.

No significant exception noted.

Department Description of Control: System options and parameters are implemented to protect data and resources. Written procedures exist for the managing and maintenance of the security software.

Tests Performed: Reviewed mainframe security procedures, security software reports, and associated options and parameters.

Test Results: The Department had a formal Mainframe Security Procedures Manual, which was updated in August 2006. System options and parameters were implemented to protect data and resources.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance the Department's controls, the Department should work with user agencies to decrease the number of unused (revoked) IDs.

TELECOMMUNICATIONS/NETWORK SERVICES

EXISTING ENVIRONMENT

Background Provided by the Department: The Bureau provides telecommunications/network services to a variety of agency, boards and commissions, educational institutions, and other governmental and non-profit entities. Bureau staff monitor these systems to confirm that devices and systems are properly, installed, configured, and maintained. Management reviews performance and capacity of the network services being provided.

Network Services

Background Provided by the Department: Network Services is responsible for management and oversight of the Illinois Century Network (ICN), Local Area Networking (LAN) for select agencies, the Illinois Wireless Information Network, and all engineering responsibilities related to State of Illinois telecommunications services.

Department Description of Control: The Division consists of three teams which includes Network Operations, LAN Services, and Enterprise Network Support.

Tests Performed: Reviewed organization chart and interviewed staff.

Tests Results: Network Operations, LAN Services, and Enterprise Network Support provided support for Network Services. An organizational change (effective January 16, 2008) modified the reporting structure for the three groups.

No significant exception noted.

Department Description of Control: The ICN obtains public Internet services from the following Internet providers: Sprint; Level 3; ATT; Qwest.

Tests Performed: Reviewed contracts.

Tests Results: The Department maintained contracts with Sprint, Level 3, ATT and Qwest for public Internet Services.

No significant exception noted.

Department Description of Control: Multi-point and redundant firewall hardware is maintained through Access Control Lists (ACL's) at the head ends of the MPLS VPN/VRF network to protect the agency networks. Additionally, firewall services are provided (both hardware and configuration) for each agency to protect their networks from each other.

Tests Performed: Reviewed network topologies and configurations for firewalls, routers and switches, and interviewed staff.

Tests Results: The Department maintained the State of Illinois Statewide Network. Firewall services were provided to protect agency networks.

No significant exception noted.

Network Services - Network Operations

Department Description of Control: Network Operations is responsible for installing, maintaining and managing the ICN Backbone including backbone circuits, egress circuits, routers, firewalls, switches, fifteen Point of Presence (POP) sites, WAN monitoring tools and WAN services. Solarwinds Orion is used to manage and monitor the ICN Backbone.

Network Operations staff are responsible for the backbone and POP site management and support. Support includes: delivery, removal and inventory of equipment; installation, maintenance and documentation of all POP site equipment; test and turn-up of all backbone and egress circuits; installation and management of POP sites. Network Operations staff are responsible for installing, customizing, maintaining and supporting WAN management and monitoring. Solarwinds Orion is used to manage and monitor the ICN Backbone. Additionally, Network Operations is responsible for WAN Services including DNS, registrar for the il.us domain, the educational content filtering solution, as well as the new state agency enterprise filtering solution, and IP Video. WAN services support includes installation, configuration, maintenance and support.

Tests Performed: Reviewed network topologies, device configurations, hardware and software, vendor websites, Department website, and interviewed staff.

Tests Results: Network Operations was responsible for installing, maintaining, managing and supporting the ICN Backbone utilizing its POP sites strategically placed throughout the State.

The ICN Backbone Network was divided logically into two layers: Core Network and Distribution Network. We reviewed the full configurations for a selection of devices as follows:

- 21 Core Routers.
- 22 Agency Distribution Routers.
- 16 Educational Institution Distribution Routers.

Upon review it appeared the configurations were, for the most part, appropriately configured; however, we did note instances where configurations could be enhanced.

In addition to the Core and Distribution routers, Network Operations maintained three firewalls. Upon review it appeared the firewall configurations were, for the most part, appropriately configured; however, we did note instances where configurations could be enhanced.

To document its network architecture, Network Operations maintained network topology maps for the backbone segment of the network it maintained. During our review of topologies and configurations we determined devices were placed in suitable logical positions.

Network Operations staff were responsible for installing, customizing, maintaining and supporting WAN management and monitoring tools. Solarwinds was utilized for monitoring and managing the ICN Backbone.

Additionally, Network Operations provided WAN services and support as outlined on its website (www.illinois.net).

No significant exception noted, however, we did note parameters which should be reviewed to ensure security issues are appropriately addressed.

Department Description of Control: Routers authenticate authorized individuals for device configuration and maintenance.

Tests Performed: Reviewed access rights, account parameters, software levels, vendor websites, device configurations, and interviewed staff.

Tests Results: The Department's Description of Control stated "Routers authenticate authorized individuals for device configuration and maintenance". However, we noted three authentication servers were utilized to provide authorized access to the firewalls, routers, and switches maintained by Network Operations, Enterprise Network Support and a few Field Operations routers. Per review of the vendor website, authentication software utilized appeared to be the current vendor recommended release. Upon review, accounts with powerful access rights appeared to be appropriately assigned and controlled.

No significant exception noted; however, authentication servers rather than routers authenticate access rights to devices.

Network Services - LAN Services

Department Description of Control: LAN Services is responsible for entering rules into the firewalls and monitoring security violations. Security logs are sent to the Mainframe and violations are reported by alarms and reports sent via the Mainframe. These reports are sent to members of LAN services and the mainframe group. They are reviewed for performance issues and/or intrusion prevention. Additionally, the LAN Networking Services group is responsible for installation, configuration and support of the Department's LAN networking infrastructure including: switches, routers, hubs, firewalls, wireless switches and inside cabling.

Tests Performed: Reviewed network topologies, device configurations, hardware and software, vendor websites, authentication servers, and interviewed staff.

Tests Results: LAN Services provided the LAN network architecture (including firewalls, routers, and switches) for the Department and consolidated agencies.

We reviewed the full configurations for a selection of devices as follows:

- 23 Firewalls.
- 25 Routers.
- 48 Switches.

Upon review it appeared the configurations were, for the most part, appropriately configured; however, we did note instances where configurations could be enhanced.

LAN Services device configurations were not routinely backed up for all devices. LAN Services had implemented a tool to backup select devices maintained by LAN Services; however, a timeframe for enterprise deployment had not been established.

To document its network architecture, LAN Services maintained individual network topology maps for each of the agency network segments it maintained. During our review of topologies and configurations we determined devices were placed in suitable logical positions.

Although intrusion detection/preventions systems had not been deployed for the agency network segments maintained by LAN Services, firewalls maintained by LAN Services were monitored for security violations via the mainframe. Reports, detailing denied traffic, were generated daily and distributed to appropriate staff.

LAN Services also maintained wireless networks and associated equipment to extend/supplement wired networks. We noted limited deployment of wireless technologies.

No significant exception noted; however, we noted some security parameters which should be reviewed to ensure security issues are appropriately addressed.

<u>Department Description of Control:</u> LAN Services maintain these configuration standards for LAN infrastructure devices. These standards are implemented on newly deployed equipment.

<u>Tests Performed:</u> Reviewed templates and configurations for devices.

<u>Tests Results:</u> LAN Services maintained the CMS/BCCS LAN Services Standards for Hardware Configuration and Development document to assist in configuration of firewalls, routers and switches. Upon review of the standards we noted they, for the most part, provided for appropriate baseline settings; however, we did note instances where configurations could be improved. Additionally, upon review of configurations, we noted instances where the configurations deviated from the standards.

No significant exception noted; however, we noted some security parameters which should be reviewed to ensure security issues are appropriately addressed.

Network Services – Enterprise Network Support

Department Description of Control: Enterprise Network Support is responsible for design and support of State agency network access. Responsibilities include installation and support of access routers, WAN switches, VOIP, video conferencing, fiber, DNS, and Internet. Enterprise Network Support also performs Tier 3 technical support for the CMC as well as for state agencies. Enterprise Network Support provides customer consultation, access and distribution router configuration, ongoing maintenance, head-end router installations/troubleshooting, making equipment and connectivity recommendations, performing equipment installation/recovery at state agency sites in Springfield and surrounding area, and the provisioning for new circuits, moves and changes. ENS utilizes established architectural and methodologies standards such as the Basic MPLS Connectivity Model to serve as a foundation for design and support of State Agency network access.

Tests Performed: Reviewed network topologies, device configurations, hardware and software, vendor websites, and interviewed staff.

Tests Results: Enterprise Network Support utilized established standards and methodologies to design and support State Agency network access. Access devices connected each of the respective agencies' and non-state agencies' networks to the ICN Backbone Network via distribution routers. We reviewed the full configurations for a selection of devices as follows:

- 134 Agency Access Routers.
- 8 Agency Access Switches.
- 2 Agency Shared Services Firewalls.

Upon review it appeared the configurations were, for the most part, appropriately configured; however, we did note instances where configurations could be enhanced.

During our review of topologies and configurations we determined devices were placed in suitable logical positions.

Enterprise Network Support also provided technical support for the CMC as well as State agencies.

No significant exception noted; however, we noted some parameters which should be reviewed to ensure security issues are appropriately addressed.

Department Description of Control: Routers authenticate authorized individuals for device configuration and maintenance.

Tests Performed: Reviewed access rights, account parameters, software levels, vendor websites, device configurations, and interviewed staff.

Tests Results: The Department's Description of Control stated "Routers authenticate authorized individuals for device configuration and maintenance". However, we noted three authentication servers were utilized to provide authorized access to the firewalls, routers, and switches maintained by Network Operations, Enterprise Network Support and a few Field Operations routers. Per review of the vendor website, authentication software utilized appeared to be the current vendor recommended release. Upon review, accounts with powerful access rights appeared to be appropriately assigned and controlled.

No significant exception noted; however, authentication servers rather than routers authenticate access rights to devices.

Department Description of Control: Enterprise Network Support is responsible for the installation, maintenance, and protection of the MAN fiber Network. Responsibilities include overseeing installation of fiber facilities and outside plant construction projects, fiber plant locating services, and maintenance of accurate fiber records. ENS is a member of the Monitor Illinois One Call (J.U.L.I.E.) dig notification system in order to protect fiber assets. The Monitor Illinois One Call (J.U.L.I.E.) group forwards dig notifications to a Department email distribution list. ENS screens the notifications for those requiring a dispatch. The Customer Solutions Center (CSC) opens a CMS Remedy Helpdesk ticket for each dispatch.

Tests Performed: Reviewed procedures, dig notices, and interviewed staff.

Tests Results: Enterprise Network Support utilized vendors to perform installation, maintenance, and locate services for the MAN fiber network. Two individuals were assigned primary and backup responsibility for managing these vendors.

As a member of the J.U.L.I.E dig notification system, Enterprise Network Support monitored the J.U.L.I.E dig notification email system during normal working hours. If they determined a notification required dispatch, the notification was forwarded onto the CSC for creation of a Remedy help desk ticket. During non-working hours the CMC monitored the email system. If the CMC identified an emergency notification during non-working hours, they would notify Enterprise Network Support for their review.

During the period of August to December 2007, 16 J.U.L.I.E dig notifications required dispatch for locate and marking services. According to procedures, Enterprise Network Support had 48 hours to respond and locate facilities for non-emergency (normal) notifications and 2 hours for emergency notifications. Upon review of the Remedy tickets for each of the 16 dig notifications, we noted notifications appeared to be dispatched to the vendor in a timely manner.

No significant exception noted.

Backup and Recovery

Department Description of Control: Network Operations and Enterprise Network Support backup firewall, router, and switch configurations via two servers. The servers are backed up to tape weekly and when a major change occurs. Tapes are then rotated off-site.

Tests Performed: Interviewed staff.

Tests Results: Two servers were utilized by Network Operations and Enterprise Network Support to backup firewall, router, and switch configurations for backbone and State agency access devices.

Configurations were automatically backed up and stored off-site.

No significant exception noted.

Configuration Standards

Department Description of Control: Network Services has established standard network configuration templates for core, distribution, access routers, and LAN routers and switches.

Tests Performed: Reviewed templates and configurations for devices.

Tests Results: Configuration templates were maintained for Core, Distribution, and Agency Access routers maintained by Network Operations and Enterprise Network Support; however, templates were not maintained for firewalls and switches maintained by each group. Upon review of the templates we noted they, for the most part, provided for appropriate baseline settings; however, we did note instances where configurations could be improved. Additionally, upon review of configurations, we noted instances where configurations deviated from the templates.

No significant exception noted; however, we noted some parameters which should be reviewed to ensure security issues are appropriately addressed.

Architectural Standards and Methodologies

Department Description of Control: Established standards currently include: POP Site Power Strategy, Basic MPLS Connectivity Model, and Common Connection Methodology for LAN, and Quality of Service. Network Services staff conducts, coordinates, and serves as lead(s) on feasibility studies and projects involving wide-area network systems.

Tests Performed: Reviewed documentation and interviewed staff.

Tests Results: Although project specific standards were developed, as needed, as the result of individual projects, a common/overarching set of standards and methodologies had not been developed and implemented to provide guidance for all projects and associated developments.

In our review of projects, we found a lack of consistent and repeatable practices for system development and project management.

No significant exception noted; however, consistent and repeatable practices for system development and project management did not exist.

Illinois Wireless Information Network (IWIN)

Background Provided by the Department: The Department and Illinois State Police (ISP) have coordinated efforts to provide the Illinois Wireless Information Network (IWIN), a wireless wide area data network using Code Division Multiple Access (CDMA). The Department administrates the IWIN network and ISP provides the connection to the Law Enforcement Agencies Data System (LEADS), National Crime Information Center (NCIC), Secretary of State, National Law Enforcement Telecommunications System (NLETS), and Criminal History Record Information (CHRI) that the network utilizes to provide information to IWIN users.

Transmissions are sent from the users' Mobile Data Computer (MDC), equipped with the client software Premier MDC, to the nearest cellular tower equipped with CDMA equipment. Once the cellular tower has received the transmission from the user's MDC, the transmission is then forwarded to a Verizon -owned and -operated messaging switch. From the messaging switch, the transmission is forwarded to one of the Department's redundant Premier MDC Servers and then to the Department's network for access to the appropriate data.

Department Description of Control: The "Illinois Statewide Policy Manual," located on the Internet, outlines the responsibilities for the Department, ISP, local agency IWIN coordinator and the IWIN user, as well as appropriate usage, necessary certifications to obtain IWIN access and Motorola client functions.

Tests Performed: Reviewed policies.

Test Results: The IWIN Policy Manual (Manual), dated December 19, 2005, outlined the responsibilities for DCMS – IWIN Support Center, Illinois State Police, Local Agency IWIN Coordinators, and IWIN users. The Manual posted on the Internet had not been updated since December 2005 and did not depict the current environment.

No significant exception noted; however, the Manual had not been updated to depict the current environment.

Department Description of Control: The Department has a contract with Verizon Wireless (Verizon) to provide data connectivity throughout the State, as well as with Motorola to provide the software utilized by the IWIN network.

Tests Performed: Reviewed contracts.

Test Results: The Department had established contracts with Verizon and Motorola to provide software and data connectivity for the State's IWIN network.

No significant exception noted.

Department Description of Control: Redundant routers, maintained by the Department, connect Premier MDC Servers to the Verizon Network. The IWIN network infrastructure utilizes redundant routers which connect servers to the provider network. Routers authenticate authorized individuals for device configuration and maintenance.

Tests Performed: Interviewed staff.

Tests Results: Redundant IWIN routers were maintained by Enterprise Network Support. (See the Enterprise Network Support section for additional information on routers and authentication.)

No significant exception noted.

Department Description of Control: The IWIN infrastructure is comprised of a multi-layer security approach. This approach secures access to the infrastructure from the IWIN user community by utilizing strong authentication such as user IDs, passwords, and unit IDs.

Tests Performed: Interviewed staff.

Test Results: The IWIN infrastructure was comprised of a multi-layer security approach consisting of application and network layer firewalls as well as software to control user access to IWIN infrastructure.

No significant exception noted.

Field Operations

Department Description of Control: Field Operations, within the Bureau's Customer and Account Management unit, consists of a decentralized staff operating out of nine statewide Regional Technology Center (RTC) offices (see http://www.illinois.net/rtc/default.htm for a listing of site staff and office locations). The RTCs are strategically placed to provide close proximity to the constituents they serve. Field Operations staff includes a Regional Manager, four Supervisors, twenty-one Network Engineers, and four Administrative Assistants.

Field Operations serves two primary constituent groups- 1) Legacy Illinois Century Network (ICN) constituents of K12 schools, community colleges, universities, museums, libraries, municipalities, and other not-for-profit groups, and 2) State agencies.

Tests Performed: Reviewed website, constituent listings, and interviewed staff.

Test Results: Field Operations staff were located throughout nine RTCs, representing 15 Market Service Areas. The RTCs have been strategically located throughout the State to provide services to State agencies and non-State agencies.

No significant exception noted.

Department Description of Control: Field Operations utilizes two versions of Remedy for constituent connectivity provisioning. Agency provisioning utilizes a Bureau version of Remedy. Other constituent and non-agency provisioning and trouble ticketing utilizes ICN Remedy.

Tests Performed: Interviewed staff.

Test Results: Field Operations utilized two versions of Remedy for provisioning. (See the Help Desk section for details regarding testing of Remedy.)

No significant exceptions noted.

Department Description of Control: Field Operations is responsible for the following:

- Services (www.illinois.net/services/default.htm#tech contains a listing of services)
  - Consultation – help constituents design efficient and cost effective network connectivity, identify circuit options, and identify appropriate equipment.
  - Filtering – perform sales and ongoing support for content filtering software designed to allow constituents to restrict access to inappropriate content on the Internet. Support includes router configurations, setting up user accounts, adding IP addresses, providing end user training, and troubleshooting problems. Primary constituents using this product include municipalities and K12 education sites.
  - IP Video – consultation, installation and troubleshooting IP based video conferencing systems.
  - Monitoring/Analysis – monitor constituent connections for up/down status and provide constituent access to utilization data for their circuits.
  - Configuration services – multicast and quality of service (QoS) configurations for specific applications including video streaming, IP voice and video, and preference cueing.
  - Technical Support – support and dispatch for circuits, equipment, and services.
  - IP Addressing – maintain and assign Internet Protocol (IP) addresses.
  - DNS – configure and maintain Domain Name Service (DNS) for domain name resolution services.
- Provisioning
  - Circuit orders – place orders for circuits with telecommunication companies (telcos) and maintain a database (ICN Remedy of all circuits connected to the ICN for both legacy ICN constituent connections and State Agency connections. Track installation dates and keep constituents notified of status via email and phone. Process Moves/Adds and Changes (MAC) to existing services. CMS Remedy is used by Field Operations staff for processing work orders initiated by the Customer Service Center (CSC).
  - Installations – visit constituent sites, install and configure equipment, connect and test circuits. Track and record inventory.
- Support
  - Technical Support – Provide Tier 2 and 3 level support for constituent connections, equipment and services. Perform or arrange for repairs, replacements, upgrades,

configuration changes and provide information. Work is documented and tracked using the trouble ticketing module of ICN Remedy and via Email.

- Maintenance – Provide on site emergency repair and regular maintenance and equipment installation at network backbone points of presence (POP sites).
- Cost Recovery – Provide quotes, bandwidth allocations and adjustments, vendor pricing verifications and invoicing support.

Field Operations is responsible for Policies, Procedures and Documentation, including:

- Network Services' SharePoint is used for housing internal policy and procedural documentation as well as white papers, project outlines and progress reports, contact lists and technical resources.
- Shared servers are used to store non-agency constituent documents including telco and equipment quotes, completed applications, and participation agreements.
- Illinois.net (www.illinois.net) is used to house all non-agency forms and information distributed to constituents, announcements of new services, conferences and policy meetings, costs and bandwidth allocations, instructions on how to access services, and historical data about the network and associated committees. Agency customer information is housed at http://www.cms.il.gov/telecom/default.htm.

Tests Performed: Reviewed websites, SharePoint site, methods and procedures, and interviewed staff.

Test Results: Field Operations maintained various methods and procedure documents to assist and guide staff when performing work associated with Service, Support and Provisioning. In addition, Field Operations utilized websites to provide necessary information to user entities.

No significant exception noted.

To support our evaluation and testing of Field Operations we performed the following additional tests.

Control: Management should ensure that firewall and router rules are sufficient and current, to protect against unauthorized access to resources and denial of services.

Tests Performed: Reviewed network topologies, device configurations, templates, hardware and software, vendor websites, and interviewed staff.

Tests Results: Access devices connected each of the respective State agencies and non-State agencies to the ICN Backbone Network via distribution routers. We reviewed the full configurations for a selection of devices as follows:

- 134 Agency Access Routers.
- 46 Non-State Agency Access Routers.

Upon review it appeared the router configurations were, for the most part, appropriately configured; however, we did note instances where configurations could be enhanced.

Configuration templates were maintained for Non-State Agency Access routers maintained by Field Operations. Field Operations also utilized a configuration template, maintained by Enterprise Network Support, for Agency Access routers it maintained. Upon review of the templates we noted they, for the most part, provided for appropriate baseline settings; however, we did note instances where configurations could be improved. Additionally, upon review of configurations, we noted instances where the configurations deviated from the templates.

During our review of topologies and configurations we determined devices were placed in suitable logical positions.

No significant exception noted; however, we noted some parameters which should be reviewed to ensure security issues are appropriately addressed.

Control: Management should ensure adequate procedures are in place for backup and recovery of Internet resources.

Tests Performed: Interviewed staff.

Tests Results: Configuration files for access routers maintained by Field Operations were automatically backed up and stored off-site.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. However, the complexity of the statewide network necessitates continual review and analysis to ensure security controls meet the Department's standards. To enhance the controls, the Department should:

- Continually review security parameters to ensure security issues are adequately addressed.
- Update the IWIN Policy Manual to reflect the current environment.
- Develop and implement consistent and repeatable practices for system development and project management.

TELECOMMUNICATIONS/NETWORK SERVICES
LAN Application Development

EXISTING ENVIRONMENT

Department Description of Control: Responsibilities of LAN Development include the development of custom application software on microcomputers, local area networks (LANs), Internet, Intranet, and mainframe client server environments.

Tests Performed: Reviewed Application System Development Methodology (Methodology) and interviewed staff.

Test Results: The LAN Application Development Unit was responsible for the development of applications which resided on microcomputers, LANs, Internet, Intranet and mainframe client server environments.

No significant exception noted.

Department Description of Control: The section follows the set standards and methodology for rapid application development maintained by the EBAS Quality Assurance Section. Access to the data for both the users and support staff follows the Active Directory/Novell login process required by each platform or tool. Tracking the status of requests is performed using a local Access database and/or the Service Request Registration System (SRRS). For projects that are classified as enhancements or new development, QA requires a checklist of deliverables to be created and delivered. QA reviews the required documents and time-stamp approves each required task as complete on their checklist tracking system.

Tests Performed: Reviewed Application System Development Methodology, access policies and procedures, SRRS, service requests, and interviewed staff.

Test Results: The LAN Application Development Unit utilized the Methodology. New developments and enhancements followed the rapid application development standards, while maintenance and ad hoc changes only required a completed service request.

The LAN Application Development Unit utilized the SRRS for tracking requests.

Department staff stated the Access database was not used to track requests in the LAN Application Development Unit.

During the audit period, there were two maintenance service requests. We reviewed the service requests for compliance with the Methodology. Although the requests generally complied with the Methodology, formal user and management approval was not indicated on the requests.

There were no new developments or enhancements during the audit period, which were required to follow the rapid application development standards and the QA review requirements.

Service requests did not contain user and management approvals and the Access database was not used to track requests in the LAN Application Development Unit.

Department Description of Control: Prior to being placed into production, all updates and modifications are reviewed and approved via email by the owner. Once approval is obtained, the developer requests the supervisor to move the changes into production. The supervisor copies the application onto the production drive and then re-tests the application to verify that the application works in the production environment.

Tests Performed: Reviewed service requests and interviewed staff.

Test Results: During the audit period, LAN Application Development had two maintenance service requests. We reviewed the two service requests, noting owner approval via email was received prior to the move to production.

The moves to production for both requests were performed by the application programmer, not the supervisor. According to the LAN Application Development Manager, the application programmer routinely moved changes to production.

After the move to production, the change was reviewed and verified by the programmer and user; however, documentation was not maintained.

Moves to production were not performed independently; thus, not appropriately segregated.

OVERALL CONCLUSION

The LAN Development Unit had not implemented procedures to ensure it met control objectives.

To ensure an appropriate segregation of duties, moves to production should be performed by an independent person.

In addition, the Department should ensure:

- Service requests contain user and management approvals.
- Appropriate documentation of the review and verification of application changes moved to production is maintained.

TELECOMMUNICATIONS/NETWORK SERVICES
Web Services

EXISTING ENVIRONMENT

Department Description of Control: The Bureau provides web services that enable more than thirty state agencies to communicate their specific and broadly related information to both public and private sectors. This is accomplished through development and continued support of a variety of internal and external web applications and high profile websites as well as enterprise-wide standardization and guidance to the agencies.

Tests Performed: Reviewed templates and interviewed staff.

Test Results: The Department provided web services that enabled State agencies to communicate their specific information via the Internet.

The Department developed enterprise-wide standardization and guidance called the Official State Web Templates. These templates were available to State agencies to provide guidance on the development of standard websites.

No significant exception noted.

Department Description of Control: Web Services supports (which includes creation, implementation, and on-going update and maintenance) both static and dynamic websites. Static websites consist of agency specific documentation, offerings, programs, etc., and applicable linking to other supporting information (including internal, external, and other public arenas). Dynamic websites consist of interactive, data-driven web-based applications, which allow staff members from state agencies to perform various functions and reporting efficiently and securely (i.e. using public key infrastructure, PKI) via the Internet.

Tests Performed: Reviewed policies and procedures, templates, and interviewed staff.

Test Results: The Department used the Official State Web Templates and additional informal procedures to create websites.

The Department utilized a database to track work and change requests for the websites supported by Web Services. The work/change requests would include creation, implementation, and update and maintenance of static and dynamic websites. Static websites consisted of agency specific information and links to supporting information. Dynamic websites consisted of interactive web-based applications used to collect information. Dynamic websites were often secured using the State’s public key infrastructure (PKI) software.

In addition, the Department developed the Web Services Content Change Procedures, revised January 30, 2008, to assist with work/change requests.

No significant exception noted.

Department Description of Control: Websites and web applications provide anywhere, anytime access. Web Services also takes direct responsibility for website maintenance if an agency requests. Websites maintained by Web Services utilize the Official State Web Templates developed and administered by Web Services. Websites are reviewed by the Department's Illinois Office of Information and Communication for compliance with the Illinois Web Accessibility Standards (IWAS), which are based on the Federal "Section 508" and World Wide Web Consortium accessibility guidelines. Additionally, in an effort to address the needs of all users, prior to implementation, web applications are thoroughly reviewed for IWAS compliance.

Tests Performed: Reviewed website reviews and interviewed staff.

Test Results: Websites maintained by Web Services were developed utilizing the Official State Web Templates.

We requested a list of the websites that were reviewed by the Department's Illinois Office of Information and Communication for compliance with the Illinois Web Accessibility Standards. Information was provided to support the review of 65 web pages (primarily specialized pages related to CMS-specific or specialized services). However, information was not provided to support the review of other State agency websites for IWAS compliance.

Additionally, Department management stated they were in the process of incorporating the Information Technology Accessibility Act (PA 95-307) requirements into their review of websites.

Although the Department used the State's Web Templates to support websites, it did not maintain documentation to verify its review of specific State agency websites for IWAS compliance.

Department Description of Control: Prior to being placed into production, all updates and modifications are reviewed and approved by the owner. Once approval is obtained, the developer requests that their supervisor move the changes into production. This is accomplished by an email sent by the Web Services supervisor to the developer to tell them the content owner has approved the final content change. The web developer then replies back to one of the Web Services supervisors requesting that it be moved into production.

Tests Performed: Reviewed procedures, change requests, and interviewed staff.

Test Results: The Department developed the Web Services Content Change Procedures, revised January 30, 2008, which provided guidance for content changes.

We reviewed 10 content change requests, noting none had documentation indicating the supervisor moved the changes into production. According to Department management, the developer verbally requested their supervisor to move the change to production.

The Department did not maintain documentation indicating the supervisor moved changes into production.

Department Description of Control: Web Services Third Level Domain Registration application (Domain Name Service/Server (DNS) /Universal Resource Locator (URL)) provides both a user interface for agencies, counties, municipalities and other authorized organizations to request an illinois.gov domain as well as an administrative component for Web Services staff to review and approve these requests.

Tests Performed: Reviewed policies, procedures and interviewed staff.

Test Results: The Department developed the Illinois.gov Policy Statement (Policy) which was published on its website (www.illinois.gov/Tech/govpolicy.cfm). The State of Illinois, via the Department as the administrator and technical contact, registered the Illinois.gov domain for use by state and local government and related interests in Illinois.

A Domain Name Service Request form, which was included in the Policy, was to be completed by the requestor and submitted to Web Services. We reviewed 15 Request forms, noting none had the CMS authorization signature.

The Domain Name Service Request forms were not properly completed.

OVERALL CONCLUSION

Web Services had not implemented procedures to ensure it met control objectives.

To enhance controls, the Department should ensure:

- Moves to production are performed independently and appropriate documentation of the review and verification of application changes moved to production is maintained.
- Documentation to support the review of State agency websites for compliance with standards is maintained.
- Request forms are properly completed and authorized.

EXISTING ENVIRONMENT

Department Description of Control: PIM provides a centralized and consolidated platform that facilitates a statewide common architecture for managing email.

Tests Performed: Reviewed consolidation efforts and interviewed staff.

Test Results: The Department had been consolidating various agencies' email systems into a centralized and consolidated platform. As of January 2008, the Department had consolidated 34 agencies to the common platform. The Department anticipated consolidating the remaining 18 agencies by January 2010.

No significant exception noted.

Department Description of Control: Services include account provisioning, calendaring, supporting user interaction with messaging application, monitoring/reporting service levels, technical support and problem resolution.

Tests Performed: Reviewed policies and procedures, monitoring reports, and interviewed staff.

Test Results: The PIM Group provided various services and support to users. These services included account provisioning, calendaring, supporting user interaction with messaging application, monitoring/reporting service levels, technical support and problem resolution.

No significant exceptions noted.

Department Description of Control: PIM applications include limited FAX Service, Mobile Messaging, Anti-Virus, Anti-Spam and Content Filtering and directory support for State of Illinois email.

Tests Performed: Reviewed policies and interviewed staff.

Test Results: The Department provided FAX services, mobile messaging, anti-virus, anti-spam, content filtering and directory support for the centralized email platform.

Additionally, mail features such as email caching and archiving, and distribution lists were available to the authorized users.

No significant exception noted.

Department Description of Control: A secure, limited access SharePoint site is established that contains instructions for PIM staff on how to manage email accounts. The following procedural documents are stored on this site; a migration PowerPoint presentation (Towards a Common Standard-Email Migration for the State of Illinois) outlining the migration approach, migration responsibility schedules for agencies converted, and a migration instruction template. Meeting minutes and status reports from completed migrations are also available on this site.

Tests Performed: Reviewed meeting minutes and interviewed staff.

Test Results: According to the PIM Manager, the SharePoint site was under construction and the procedural documentation had not been placed on the site. However, the procedural documentation was available to appropriate staff members.

The PIM Group held weekly meeting with the migration committee in order to discuss the agency migration taking place at that time. We reviewed meeting minutes for the month of January 2008, noting they met once a week.

No significant exception note; however, the Department had not established the SharePoint site as outlined in the Description of Control.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives.

This Page Intentionally Left Blank

APPLICATION CONTROLS

Application controls are the methods, policies, and procedures adopted by an organization to ensure all transactions are entered, processed, and reported correctly. Application controls ensure data being entered, processed, and stored are complete and accurate. They ensure 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 the data entered into the system are authorized and accurate. These controls include both manual and computerized techniques. Processing controls are those that are coded into the software program. Manual procedures often supplement the programmed controls to verify that all processing has taken place as intended. Output controls govern the printing and distribution of reports.

The Department has developed several applications for use by State agencies. As part of the Third Party Review, we reviewed four of the applications used by multiple State agencies.

The applications reviewed were:

- Accounting Information System;
- Central Payroll System;
- Central Inventory System; and
- Central Time and Attendance System.

This Page Intentionally Left Blank

COMMON SYSTEMS
ACCOUNTING INFORMATION SYSTEM

EXISTING ENVIRONMENT

The Accounting Information System (AIS) was implemented in 1995. AIS was utilized by 51 entities. (See page 167 for the list of user agencies).

Department Description of Control: AIS functions as an automated expenditure control and invoice/voucher processing system. AIS, in processing invoices, allocates invoice amounts into sub accounts; groups invoices, according to the Comptroller's Statewide Accounting Management System (SAMS) procedures, for the preparation of vouchers; and allows users to track cost centers. AIS interfaces with the Illinois Governmental Purchasing System (IGPS), the Accounts Receivable Posting System (ARPS), the Central Inventory System (CIS) and the Central Payroll System (CPS).

Tests Performed: Reviewed AIS application, AIS Online User Manual, and interviewed staff.

Test Results: AIS was an online, menu-driven, mainframe application that provided an automated expenditure control and invoice/voucher processing system. Invoice processing allocated invoice amounts by cost centers and sub-accounts and groups common invoices for payment according to SAMS procedures. In addition, AIS interfaced with the Illinois Governmental Purchasing System (IGPS), the Accounts Receivable Posting System (ARPS) and the Central Payroll System (CPS).

Department staff stated the Central Inventory System did not interface with AIS at this time.

No significant exception noted.

Department Description of Control: AIS is secured using security software, in addition to internal security requirements. Users must have an authorized ID and password to gain access. Assignment and authorization of access rights is the responsibility of the user agency. Once access has been gained to the operating system, users must have a separate application user ID and password to gain access.

Tests Performed: Reviewed AIS application, list of authorized users, process of granting rights, and appropriateness of access for those authorized users.

Test Results: Access to AIS was controlled through security software (Resource Access Control Facility (RACF)), in addition to AIS' internal security. Users must have a properly authorized security software user ID and password to gain access to the operating environment. Once access to the operating environment was allowed, users must use a separate application user ID and password to gain access to AIS.

Assignment, authorization, and maintenance of access rights were the responsibility of each agency's security administrator.

The Department required Departmental employees to complete a RACF Mainframe Request, obtain approval, and forward the request to Technical Support staff to obtain access rights. We reviewed access rights of 25 Department staff member to AIS, noting several disparities between RACF access and internal security access.

No significant exception noted; however, access rights were not always appropriately aligned with current staff responsibilities.

Department Description of Control: Changes to AIS are controlled through the Application System Development (now referred to Enterprise Business Applications) Methodology. Changes are initiated through the use of a Service Request Form. The changes are approved and tested before implementation into the production environment. The Library Control Group will then move the change into production.

Tests Performed: Reviewed the Application Systems Development (ASD) Methodology Manual, the IMS Standards and Documentation Requirements Manual (Manual), Service Requests (SR's), Program Library Procedures, and Electronic Move Production Forms.

Test Results: During the audit period, AIS had one service request which was classified as an enhancement. We reviewed the service request, noting the SR complied with the Methodology.

Additionally, we noted there were no major changes to AIS in the past year.

No significant issues were identified with the contents or utilization of the Manual, SR, Program Library Procedures, or Electronic Move Production Form.

No significant exception noted.

Department Description of Control: Project Administration includes requirements gathering, drafting charters, facilitating and organizing project management activities, tracking and documenting issues and action items, project status reporting, maintaining task and resource plans, documenting work processes, etc.

Tests Performed: Reviewed the ASD Methodology, the IMS Standards and Documentation Requirements Manual, and interviewed staff.

Test Results: Project administration was accomplished through the use of the ASD Methodology and the Manual.

No significant exception noted.

Department Description of Control: AIS is backed up daily, weekly, and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.

Tests Performed: Reviewed AIS backup schedule and backups maintained at the CCF and at the off-site storage location, and interviewed staff.

Test Results: We reviewed the list of backup tapes and identified daily, weekly, and monthly backup tapes. We selected a sample of backup tapes and located all tapes at the CCF or the off-site storage location.

No significant exception noted.

Department Description of Control: EBAS Quality Assurance applies to AIS.

Tests Performed: Reviewed EBAS Quality Assurance (QA) procedures and changes to AIS.

Test Results: The QA procedures were included in Appendix D of the Application System Development Methodology Manual. The procedures outlined the process for the design, development, and implementation of new developments and enhancements. The procedures required a checklist to be completed for enhancements.

We reviewed the one enhancement completed during the audit period, noting a completed checklist.

No significant exception noted.

Department Description of Control: The AIS User Manual, which is located on the State's Enterprise Web Server (Intranet), provides guidance on the use of the Accounting Information System.

Tests Performed: Reviewed the AIS Online User Manual.

Test Results: The Department had a User Manual, which provided users with guidance on logging into AIS, security screen functions, producing and processing invoices, edit checks, and producing reports.

No significant exception noted.

Department Description of Control: AIS transactions are entered online in a real-time environment, with the ability to batch transactions for processing at a later date. AIS was developed with edits that force correction of errors and completion of critical fields before a transaction is accepted. All data entry is performed by user agencies and is the responsibility of user agencies.

Tests Performed: Reviewed AIS edits, AIS Online User Manual, and agency data.

Test Results: The AIS transactions were entered online in real time environment with the ability to batch transactions for processing at a later date. Additionally, the AIS Online User Manual provided information regarding AIS built in edit checks which required specific fields to be completed before AIS transactions can be completed.

The accuracy and reconciliation of data was the responsibility of the user agency.

During our review, we selected two agencies' AIS data and tested the accounting records for proper input, edits, and compliance with date standards. We determined that the 297,239 data records tested were entered properly and complied with date composition standards. During our testing of AIS data, we did not identify any significant weaknesses.

No significant exception noted.

Department Description of Control: A disaster recovery plan for AIS provides guidelines for restoration.

Tests Performed: Reviewed AIS disaster recovery plan.

Test Results: The Financial Applications Disaster Recovery Plan provided for disaster recovery of financial systems in accordance with the Department’s overall recovery plan. The Plan was last updated and tested on September 11, 2007.

No significant exception noted.

Department Description of Control: AIS provides various online and batch reports to assist in the balance of transactions. A complete listing of the various reports is maintained in the AIS Users Manual. Retention of the various reports is the responsibility of the user agency.

Tests Performed: Reviewed the AIS Online User Manual.

Test Results: The AIS Online User Manual provided a complete listing of various online and batch reports used for the balancing of transactions. Also, retention of the various reports was the responsibility of the user agency.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should periodically review access rights to AIS and ensure access is appropriate.

Department records listed the following entities as users of the Accounting Information System.

1. Board of Higher Education
2. Capital Development Board
3. Department of Agriculture
4. Department of Central Management Services
5. Department of Corrections
6. Department of Financial and Professional Regulation
7. Department of Human Rights
8. Department of Labor
9. Department of Juvenile Justice
10. Department of Military Affairs
11. Department of Natural Resources
12. Department of Public Health
13. Department of Veterans’ Affairs
14. Department on Aging
15. Environmental Protection Agency
16. General Assembly Retirement System
17. Guardianship and Advocacy Commission
18. Historic Preservation Agency
19. Human Rights Commission
20. Illinois Arts Council
21. Illinois Civil Service Commission
22. Illinois Commerce Commission
23. Illinois Community College Board
24. Illinois Council on Developmental Disabilities
25. Illinois Criminal Justice Information Authority
26. Illinois Deaf and Hard of Hearing Commission
27. Illinois Educational Labor Relations Board
28. Illinois Labor Relations Board
29. Illinois Law Enforcement Training and Standards Board
30. Illinois Office of the State’s Attorneys Appellate Prosecutor
31. Illinois Prisoner Review Board
32. Illinois Procurement Policy Board
33. Illinois Student Assistance Commission
34. Illinois Violence Prevention Authority
35. Illinois Workers’ Compensation Commission
36. Judges’ Retirement System
37. Judicial Inquiry Board
38. Office of Management and Budget
39. Office of the Attorney General
40. Office of the Auditor General
41. Office of the Executive Inspector General
42. Office of the Governor
43. Office of the Lieutenant Governor
44. Office of the State Appellate Defender
45. Office of the State Fire Marshal
46. Property Tax Appeal Board
47. State Board of Elections
48. State Employees’ Retirement System
49. State Police Merit Board
50. State Universities Civil Service System
51. Supreme Court of Illinois

COMMON SYSTEMS
CENTRAL PAYROLL SYSTEM

EXISTING ENVIRONMENT

The Central Payroll System (CPS) was implemented in 1972. CPS was utilized by 75 entities. (see page 173 for the list of user agencies).

Department Description of Control: CPS was designed to provide assistance in preparing payrolls for state agencies. The system will accommodate agencies which are governed by the Rules of the Personnel Code and agencies that are exempt from the Personnel Code (Non-Code Agencies). The payroll system is a tool to be used by qualified personnel with SAMS and payroll procedure knowledge. CPS enables state agencies to maintain automated pay records and provide a file that is submitted to the Comptroller's Office for the production of payroll warrants. CPS has an interface with Central Time and Attendance System (CTAS) and Accounting Information System (AIS).

Tests Performed: Reviewed CPS User Manual and interviewed staff.

Test Results: According to the User Manual, the system was designed to provide assistance in preparing payrolls for agencies within the State of Illinois. The system would accommodate agencies which were governed by the Rules of the Personnel Code and agencies that were exempt from the Personnel Code, (Non-Code Agencies). Guidelines for payrolls were set forth in the current version of the Statewide Accounting Management System (SAMS), and the Illinois Compiled Statues

CPS interfaced with Central Time and Attendance System and the Accounting Information System.

No significant exception noted.

Department Description of Control: CPS is secured using security software, in addition to internal security requirements. Users must have an authorized ID and password to gain access. Assignment and authorization of access rights is the responsibility of the user agency. Once access has been gained to the operating system, users must have a separate application user ID and password to gain access.

Tests Performed: Reviewed the Mainframe Security Procedures, appropriateness of individuals with access to CPS, and interviewed staff.

Test Results: Access to CPS was controlled through security software (Resource Access Control Facility (RACF)), in addition to CPS' internal security. Users must have a properly authorized security software user ID and password to gain access to the operating environment. Once access to the operating environment was, users must use a separate application user ID and password to gain access to CPS.

Assignment and authorization of access rights were the responsibility of each agency's security administrator.

The Department required Departmental employees to complete a RACF Mainframe Request, obtain approval and forward to the Technical Support staff for completion of access rights. We reviewed seven Department staff with access rights to CPS, noting two no longer required access.

No significant exception noted; however, access rights were not always appropriately aligned with current staff responsibilities.

Department Description of Control: Changes to CPS are controlled through the Application System Development (now referred to Enterprise Business Applications) Methodology. Changes are initiated through the use of a Service Request Form. The changes are approved and tested before implementation into the production environment. The Library Control Group will then move the change into production.

Tests Performed: Reviewed the Application System Development Methodology (Methodology), Program Library Procedures, Service Requests (SR), and interviewed staff.

Test Results: During the audit period, CPS had nine service requests (eight maintenance and one ad hoc). We reviewed the service requests, noting they complied with the Methodology.

Additionally, we noted there were no major changes to CPS in the past year.

No issues were identified with the contents or utilization of the Methodology, SR's, or the Program Library Procedures.

No significant exception noted.

Department Description of Control: EBAS Quality Assurance applies to CPS.

Tests Performed: Reviewed EBAS Quality Assurance (QA) procedures and interviewed staff.

Test Results: The QA procedures were included in Appendix D of the Application System Development Methodology. The procedures outlined the monitoring process for the design, development, and implementation of new developments and enhancements.

No changes during the audit period were required to follow the QA procedures.

No significant exception noted.

Department Description of Control: Project Administration includes requirements gathering, drafting charters, facilitating and organizing project management activities, tracking and documenting issues and action items, project status reporting, maintaining task and resource plans, documenting work processes, etc.

Tests Performed: Interviewed staff.

Test Results: Project administration was accomplished through the use the Methodology and the IT Governance Process.

No significant exception noted.

Department Description of Control: CPS is backed up daily, weekly, and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.

Tests Performed: Reviewed backup schedules, backups maintained at the CCF and at the off-site storage location, and interviewed staff.

Test Results: According to Department staff, CPS backups were performed twice daily, once before batch processing and once after the batch process. In addition, every week a backup was performed, which was rotated to the off-site location. Specific monthly backups were not performed.

We selected a sample of backup tapes and located all the tapes at the CCF or the off-site storage location.

No significant exception noted.

Department Description of Control: The User Manual is a guideline for using the payroll system and is not intended to provide SAMS or payroll rules and regulations. Guidelines for payrolls are set forth in the current version of SAMS and the Illinois Compiled Statutes.

Tests Performed: Reviewed CPS User Manual and interviewed staff.

Test Results: The Department had a User Manual, which provided users with guidance on logging into the application, recovery in the event of a disaster, backup cycle, adding/deleting employees, and the processing and completion of payroll.

No significant exception noted.

Department Description of Control: CPS has an edit feature designed to reject invalid information entered into the system. When invalid data has been entered into the system, an error message will appear at the top of the screen and the field that is in error will be highlighted. The system will not accept the entry until the error has been corrected or deleted. The Department has procedures in place to handle errors that occur during processing.

Tests Performed: Reviewed edits of CPS, agency data, and interviewed staff.

Test Results: Data entered into the system was the responsibility of the user agency. The CPS contained online edit checks to help prevent a user from entering a transaction with invalid data.

If an error occurred during data entry, users were not allowed to continue until the error had been corrected.

During our review, we selected two agencies' CPS data and tested employee identification numbers, voucher numbers, warrant amounts and date fields for proper input, edits, and compliance with date standards. We determined that the 62,152 data records tested were entered properly and complied with date composition standards. During our testing of CPS data, we did not identify any significant weaknesses.

No significant exception noted.

Department Description of Control: Disaster Recovery guidance is included in the User Manual.

Tests Performed: Reviewed CPS User Manual.

Test Results: Disaster recovery guidance was communicated to user agencies through the CPS User Manual. In the event of an emergency, Central Payroll would submit to the Comptroller the last correct version of the payroll file for payment. User agencies were responsible for supplying the last correct version of the hardcopy voucher to allow the Comptroller's Office to produce a warrant for that agency. User agencies were responsible for retaining the hardcopy payroll voucher for the three most current pay periods.

No significant exception noted.

Department Description of Control: The payroll vouchers/reports that are produced from the batch process are printed by the Department's Production Operations Services and delivered to Central Payroll. Central Payroll separates the vouchers/reports for each agency to pickup or to be delivered by Mail Messenger, UPS, or Fed Ex. Each agency must fill out an informational sheet provided by Central Payroll that contains the list of individuals that are approved to pick up payroll related materials. This list is reviewed periodically by the user agencies. The retention of these payroll vouchers/reports is the responsibility of the user agency.

Tests Performed: Reviewed the reports/vouchers, CPS User Manual and interviewed CPS staff.

Test Results: Each pay period, the following standard payroll reports were provided to agencies:

- Personal Services Expenditure Report.
- Expenditure Report with Insurance Reimbursement.
- Employer Pickup of Employee Retirement Contributions.
- Translog Report.
- Alpha Change Listing.
- Warning Report from Payroll Calculations.

Reports were printed by I/O Control and then delivered to the CPS staff for distribution. Security guards are provided with the both the Payroll Pickup Procedures and a list of individuals authorized to pick up payroll reports. User agency staff obtained payroll reports from the lobby of the Communications Building after providing security guards with a valid ID for comparison to the authorization list and signing the Payroll Release Log.

We reviewed one Payroll Release Log, noting no significant exception.

Twice a year the CPS staff request the agency staff review/update the authorization listing. The last review was conducted in October 2007.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should periodically review access rights to CPS and ensure access is appropriate.

Department records listed the following entities as users of the Central Payroll System.

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

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

COMMON SYSTEMS
CENTRAL INVENTORY SYSTEM

EXISTING ENVIRONMENT

The Central Inventory System (CIS) was implemented in 1998. CIS was utilized by 24 entities. (see page 178 for the list of user agencies).

Department Description of Control: CIS is an online real time system; therefore, inventory data is updated immediately to reflect the transactions entered. CIS allows user agencies to maintain records of inventory and to comply with the Department's Property Control Division's rules of reporting and processing. CIS has an interface with AIS.

Tests Performed: Reviewed the Department's Property Control Division's rules, list of user agencies, the CIS application, and interviewed staff.

Test Results: CIS was an online real time system that allowed agencies to maintain records of inventory to comply with the Department's Property Control Division's rules of reporting and processing (44 Ill. Adm. Code 5010).

Department staff stated the Central Inventory System did not interface with AIS at this time.

No significant exception noted.

Department Description of Control: CIS is secured using security software, in addition to internal security requirements. Users must have an authorized ID and password to gain access. Assignment and authorization of access rights is the responsibility of the user agency. Once access has been gained to the operating system, users must have a separate application user ID and password to gain access.

Tests Performed: Reviewed CIS application, list of authorized users, process of granting rights, and appropriateness of access for authorized users.

Test Results: Access to CIS was controlled through security software (Resource Access Control Facility (RACF)), in addition to CIS' internal security. Users must have a properly authorized security software user ID and password to gain access to the operating environment. Once access to the operating environment was allowed, users must use a separate application user ID and password to gain access to CIS.

Assignment and authorization of access rights is the responsibility of each agency's security administrator.

The Department required Departmental employees to complete a RACF Mainframe Request, obtain approval, and forward the request to Technical Support staff to obtain access rights. We reviewed access rights of 25 staff members to CIS, noting several disparities between RACF access and internal security access.

No significant exception noted; however, access rights were not always appropriately aligned with current staff responsibilities.

Department Description of Control: Changes to CIS are controlled through the Application System Development (now referred to Enterprise Business Applications) Methodology. Changes are initiated through the use of a Service Request Form. The changes are approved and tested before implementation into the production environment. The Library Control Group will then move the change into production.

Tests Performed: Reviewed the Application Systems Development (ASD) Methodology Manual (Methodology), the IMS Standards and Documentation Requirements Manual (Manual), Service Requests (SR's), Program Library Procedures, and Electronic Move Production Forms.

Test Results: During the audit period, CIS had eight service requests (one maintenance and seven ad hoc requests). We reviewed the service requests, noting they complied with the Methodology.

Additionally, we noted there were no major changes to CIS in the past year.

No significant issues were identified with the contents or utilization of the Manual, SR's, Program Library Procedures, or Electronic Move Production Forms.

No significant exception noted.

Department Description of Control: Project Administration includes requirements gathering, drafting charters, facilitating and organizing project management activities, tracking and documenting issues and action items, project status reporting, maintaining task and resource plans, documenting work processes, etc.

Tests Performed: Reviewed the ASD Methodology, the IMS Standards and Documentation Requirements Manual, and interviewed staff.

Test Results: Project administration was accomplished through the use the ASD Methodology and the Manual.

No significant exception noted.

Department Description of Control: CIS is backed up daily, weekly, and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.

Tests Performed: Reviewed backup schedules and backups maintained at the CCF and at the off-site storage location, and interviewed staff.

Test Results: We reviewed the list of backup tapes and identified daily, weekly, and monthly backup tapes. We selected a sample of backup tapes and located all the tapes at the CCF or the off-site storage location.

The Department had not developed a formal disaster recovery plan; however, procedures were in place which would be utilized to recover CIS in the event of a disaster.

No significant exception noted.

Department Description of Control: EBAS Quality Assurance applies to CIS.

Tests Performed: Reviewed EBAS Quality Assurance (QA) procedures and interviewed staff.

Test Results: The QA procedures were included in Appendix D of the Methodology. The procedures outlined the process for the design, development, and implementation of new developments and enhancements.

No changes during the audit period were required to follow the QA procedures.

No significant exception noted.

Department Description of Control: The Department has developed a user manual, the CIS User Manual, which is available from the Department. The manual provides guidance to the user when utilizing the various functions.

Tests Performed: Reviewed the CIS Online User Manual.

Test Results: The Department had a User Manual, which provided users with guidance on logging into application, adding/deleting transactions and various reports which were available.

No significant exception noted.

Department Description of Control: Data is entered online by user agencies. CIS has several edit checks to alert users of errors. Errors must be corrected before the transaction is accepted. CIS has the ability to utilize an optical scanner to read bar code labels during a physical inventory.

Tests Performed: Reviewed CIS edits, CIS User Manual, and agency data.

Test Results: CIS contained online edit checks to help prevent a user from entering a transaction with invalid data. If an error occurred during data entry, the online edit would display a message and prompt the user for correct data. Data was entered online by user agencies and errors must be corrected before the transaction was accepted.

The CIS User Manual contained information on the use of bar code technology for conducting a physical inventory.

During our review, we selected two agencies' CIS data and tested the inventory records for proper input, edits, and compliance with date standards. We determined that the 145,452 data records tested were entered properly and complied with date composition standards. During our testing of CIS data, we did not identify any significant weaknesses.

No significant exception noted.

Department Description of Control: The Department generates a Location Balance Report nightly to determine whether transactions processed correctly. Additional reports are available to users. The accuracy and reconciliation of data is the responsibility of the user agency.

Tests Performed: Reviewed Location Balance Report, CIS User Manual, and interviewed staff.

Test Results: The Location Balance Report provided information on inventory locations, number of items with value less than $100, number of items with value greater than $100, and items that were capitalized and owned.

Data entered into the system was the responsibility of the user agency. The CIS User Manual provided information on various reports available to user agencies to assist them in ensuring the accuracy and reconciliation of CIS data.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should periodically review access rights to CIS and ensure access is appropriate.

Department records listed the following entities as users of the Central Inventory System.

1. Capital Development Board
2. Department of Agriculture
3. Department of Central Management Services
4. Department of Employment Security
5. Department of Human Rights
6. Department of Military Affairs
7. Department of Natural Resources
8. Department of Public Health
9. Department of Transportation
10. Department of Veterans' Affairs
11. Department on Aging
12. Environmental Protection Agency
13. Historic Preservation Agency
14. Illinois Deaf and Hard of Hearing Commission
15. Illinois Educational Labor Relations Board
16. Illinois Law Enforcement Training and Standards Board
17. Illinois Office of the State's Attorneys Appellate Prosecutor
18. Illinois Procurement Policy Board
19. Illinois Violence Prevention Authority
20. Illinois Workers' Compensation Commission
21. Office of Management and Budget
22. Office of the Attorney General
23. Office of the Governor
24. Office of the Lieutenant Governor

COMMON SYSTEMS
CENTRAL TIME AND ATTENDANCE SYSTEM

EXISTING ENVIRONMENT

The Central Time and Attendance System (CTAS) was implemented in 1992. CTAS was utilized by 31 entities. (see page 183 for the list of user agencies).

Department Description of Control: CTAS is an online system used to maintain "available benefit time". Additionally, CTAS allows user agencies to monitor whether usage of time is in accordance with state rules. CTAS provides for attendance information to be recorded using either the positive or exception methods. CTAS interfaces with the Central Payroll System.

Tests Performed: Reviewed CTAS User Manual and interviewed staff.

Test Results: CTAS was an online system which maintained current available benefit time balances and monitored the usage of time. CTAS recorded information using the positive or exception methods.

CTAS interfaced with the Central Payroll System.

No significant exception noted.

Department Description of Control: CTAS is secured using security software, in addition to internal security requirements. Users must have an authorized ID and password to gain access. Assignment and authorization of access rights is the responsibility of the user agency. Once access has been gained to the operating system, users must have a separate application user ID and password to gain access.

Tests Performed: Reviewed the Mainframe Security Procedures, appropriateness of individuals with access to CTAS, and interviewed staff.

Test Results: Access to CTAS is controlled through security software (Resource Access Control Facility (RACF)), in addition to CTAS' internal security. Users must have a properly authorized security software user ID and password to gain access to the operating environment. Once access to the operating environment was allowed, users must use a separate application user ID and password to gain access to CTAS.

Assignment and authorization of access rights were the responsibility of each agency's security administrator.

The Department required Departmental employees to complete a RACF Mainframe Request, obtain approval and forward to the Technical Support staff for completion of access rights. We reviewed access rights of 25 Department staff members to CTAS, noting five staff members no longer required access.

No significant exception noted; however, access rights were not always appropriately aligned with current staff responsibilities.

Department Description of Control: Changes to CTAS are controlled through the Application System Development (now referred to Enterprise Business Applications) Methodology. Changes are initiated through the use of a Service Request Form. The changes are approved and tested before implementation into the production environment. The Library Control Group will then move the change into production.

Tests Performed: Reviewed the Application System Development Methodology (Methodology), Program Library Procedures, Service Requests (SR), and interviewed staff.

Test Results: During the audit period, CTAS had four maintenance service requests. We reviewed the service requests noting they complied with the Methodology.

Additionally, we noted there were no major changes to CTAS in the past year.

No issues were identified with the contents or utilization of the Methodology, SR's, or the Program Library Procedures.

No significant exception noted.

Department Description of Control: EBAS Quality Assurance applies to CTAS.

Tests Performed: Reviewed EBAS Quality Assurance (QA) procedures and interviewed staff.

Test Results: The QA procedures were included in Appendix D of the Application System Development Methodology. The procedures outlined the monitoring process for the design, development, and implementation of new developments and enhancements.

No changes during the audit period were required to follow the QA procedures.

No significant exception noted.

Department Description of Control: Project Administration includes requirements gathering, drafting charters, facilitating and organizing project management activities, tracking and documenting issues and action items, project status reporting, maintaining task and resource plans, documenting work processes, etc.

Tests Performed: Interviewed staff.

Test Results: Project administration was accomplished through the use the Methodology and the IT Governance Process.

No significant exception noted.

Department Description of Control: CTAS is backed up daily, weekly, and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.

Tests Performed: Reviewed backup schedules, backups maintained at the CCF, and at the off-site storage location, and interviewed staff.

Test Results: According to Department staff, CTAS backups were performed twice daily, once before and once after batch processing. In addition, every week at the end of the batch process, a backup was performed. Specific monthly backups were not performed.

We selected a sample of backup tapes and located all the tapes at the CCF or the off-site storage location.

No significant exception noted.

Department Description of Control: The CTAS User Manual provides guidance to the user when utilizing the various functions.

Tests Performed: Reviewed CTAS User Manual and interviewed staff.

Test Results: The Department had a User Manual, which provided users with guidance on logging into the application, adding/deleting employees, and the processing and completion of transactions.

No significant exception noted.

Department Description of Control: Data is entered online by user agencies. CTAS has edit checks to alert users of errors. Transactions with errors will be rejected

Tests Performed: Reviewed edits of CTAS, agency data, and interviewed staff.

Test Results: Data entered into the system was the responsibility of the user agency. CTAS contained hundreds of edit checks built into the system to notify the user of any exceptions. The system performed an online edit check and would reject all transactions that did not meet the edit criteria.

During our review, we selected two agencies' CTAS data and tested date fields, vacation balances, and the employee identification number for proper input, edits, and compliance with date standards. We determined that the 6,630 data records tested were entered properly and complied with date composition standards. During our testing of CTAS data, we did not identify any significant weaknesses.

No significant exception noted.

Department Description of Control: CTAS provides online and batch reports that user agencies may use for reconciliation purposes. During the “close” process, CTAS generates error reports, reconciliation reports, and file maintenance activity reports. All transactions must be reconciled before the “close” process can be finalized. The accuracy and reconciliation of data is the responsibility of the user agency.

Tests Performed: Reviewed CTAS User Manual and interviewed staff.

Test Results: During the “close” process, CTAS generated an error report, a reconciliation report, and a file maintenance activity report. All discrepancies were to be reconciled before a “close” could be finalized.

No significant exception noted.

Department Description of Control: Recovery procedures for CTAS provide guidelines for restoration.

Tests Performed: Reviewed the CTAS Recovery Report and the Business Continuity Plan.

Test Results: The Department developed the CTAS Recovery Report, not dated, and the Business Continuity Plan, dated December 2006.

The Report provided steps necessary to recover the CTAS database in the event of a disaster. The Plan identified the Technical Support staff who was responsible for the recovery of CTAS.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should periodically review access rights to CTAS and ensure access is appropriate.

Department records listed the following entities as users of the Central Time and Attendance System.

1. Capital Development Board
2. Department of Agriculture
3. Department of Central Management Services
4. Department of Commerce and Economic Opportunity
5. Department of Financial and Professional Regulation
6. Department of Human Rights
7. Department of Labor
8. Department of Natural Resources (Division of Mines and Minerals)
9. Department of Public Health
10. Department of Revenue
11. Department of Veterans' Affairs
12. Department on Aging
13. Environmental Protection Agency
14. Guardianship and Advocacy Commission
15. Human Rights Commission
16. Illinois Civil Service Commission
17. Illinois Comprehensive Health Insurance Plans
18. Illinois Criminal Justice Information Authority
19. Illinois Deaf and Hard of Hearing Commission
20. Illinois Educational Labor Relations Board
21. Illinois Law Enforcement Training and Standards Board
22. Illinois Planning Council on Developmental Disabilities
23. Illinois Procurement Policy Board
24. Illinois Workers' Compensation Commission
25. Office of Management and Budget
26. Office of the Attorney General
27. Office of the Executive Inspector General
28. Office of the Governor
29. Office of the State Fire Marshal
30. Property Tax Appeal Board
31. State Board of Elections

This Page Intentionally Left Blank

APPENDIX A

COMPLEMENTARY USER ORGANIZATION CONTROLS

Users of the State's Central Computer Facility are responsible for complying with prescribed requirements and for using available security mechanisms to protect the security and integrity of their data. During the course of our review, we identified several areas of user agency responsibility that should be reviewed by user agencies and their internal and external auditors.

Disaster contingency plans are needed.
Due to the fact agencies rely on the Department for computing services, they should take steps to reduce the risks associated with disruption or loss. Agencies should:

- Submit a listing of critical applications with all pertinent information to the Department, at least annually.
- Submit detailed recovery requirements to the Department.
- Submit formal disaster recovery plans to the Department.
- Ensure all data is backed up and stored appropriately off-site.
- Ensure all critical applications are tested at least annually. Additionally, agencies should submit detailed goals and results of the test to the Department.

Available security mechanism should be utilized.
To ensure that controls are functional at the agency level, agencies should:

- Effectively utilize security software features and perform periodic reviews of existing profiles to ensure that access rights are appropriate.
- Formally encourage users to include both alphabetic and non-alphabetic characters in their passwords, to protect the security of their account.
- Examine revoked IDs and delete IDs that are no longer necessary.
- Utilize the Department's password reset utilities for users who are required to have the ability to reset passwords. Powerful attributes should only be assigned to users who need administrative capabilities.
- Provide timely notification to the Department's DB2 Application Support Administrator if the agency DB2 Coordinator changes and assign the DB2 Coordinator ID to a specific person to promote accountability for the use of the ID.
- Review the use of security permissions that permit multi-write capabilities on z/VM (which may cause data to be corrupted or lost) and have it eliminated from all minidisks where it is not absolutely essential.
- Coordinate with the Department to assure that automatic time-out settings for their CICS regions provide reasonable protection of the information resources for the agency, while considering their operational needs.
- Utilize available encryption technology to protect confidential data, including data on backup media.

Bills for computer services should be reviewed.
User agencies should monitor the monthly billing to ensure charges are correct. Additionally, all user agencies should submit payment in a timely manner.

Security and Controls over the Internet should be reviewed.
To enhance security, agencies should:

- Regulate and monitor Internet web-based content by utilizing resources such as Internet content filtering and access logging.
- Develop and implement policies and procedures regarding appropriate Internet usage.
- Utilize available encryption technology to secure transmission of confidential or sensitive information across the Internet.
- Ensure the Department is notified of IWIN accounts that need to be deactivated in a timely manner.
- Monitor content transmitted through the IWIN network.

Accounting Information Systems (AIS) use should be reviewed.
We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, agencies using AIS should:

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

Central Payroll System (CPS) use should be reviewed.
We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, agencies using CPS should:

- Verify only accurate and authorized data are entered into CPS. It is the agency's responsibility to ensure only properly authorized transactions are entered into the system.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the users and user groups with access to CPS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up payroll reports, and inform appropriate CPS personnel of changes timely.
- Retain hardcopy payroll vouchers for at least the three most current pay periods, as specified by the CPS User Manual.

Central Inventory System (CIS) use should be reviewed.
We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, agencies using CIS should:

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

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

Central Time and Attendance System (CTAS) use should be reviewed.
We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, agencies using CTAS should:

- Verify only accurate and authorized data are entered into CTAS. It is the agency's responsibility to ensure only properly authorized transactions are entered into the system.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the users and user groups with access to CTAS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up timekeeping reports, and inform appropriate CTAS personnel of changes timely.

Note: Additional information is available to assist user agencies and their internal and external auditors in the review of these complementary controls or other pertinent controls. Please feel free to contact the Office at 217-782-6046 or auditor@mail.state.il.us.

This Page Intentionally Left Blank

APPENDIX B

LIST OF USER AGENCIES

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

49. Illinois Office of the State's Attorneys Appellate Prosecutor
50. Illinois Prisoner Review Board
51. Illinois Procurement Policy Board
52. Illinois State Board of Investment
53. Illinois State Police
54. Illinois State Toll Highway Authority
55. Illinois State University
56. Illinois Student Assistance Commission
57. Illinois Violence Prevention Authority
58. Illinois Workers' Compensation Commission
59. Joint Committee on Administrative Rules
60. Judges' Retirement System
61. Judicial Inquiry Board
62. Legislative Audit Commission
63. Legislative Ethics Commission
64. Legislative Information System
65. Legislative Printing Unit
66. Legislative Reference Bureau
67. Legislative Research Unit
68. Medical District Commission
69. Northeastern Illinois University
70. Northern Illinois University
71. Office of Management and Budget
72. Office of the Architect of the Capitol
73. Office of the Attorney General
74. Office of the Auditor General
75. Office of the Comptroller
76. Office of the Executive Inspector General
77. Office of the Governor
78. Office of the Lieutenant Governor
79. Office of the Secretary of State
80. Office of the State Appellate Defender
81. Office of the State Fire Marshal
82. Office of the Treasurer
83. Property Tax Appeal Board
84. Senate Operations
85. Sex Offender Management Board
86. Southern Illinois University
87. State Board of Education
88. State Board of Elections
89. State Employees' Retirement System
90. State of Illinois Comprehensive Health Insurance Board
91. State Police Merit Board
92. State Universities Civil Service System
93. State Universities Retirement System
94. Supreme Court of Illinois
95. Teachers' Retirement System of the State of Illinois
96. University of Illinois
97. Western Illinois University

APPENDIX C

IDENTIFIED DESCRIPTION OF CONTROL DEFICIENCIES

The Department's Description of Control identified several controls that were not accurate based on test work performed.

The following table is a summary of specific deficiencies noted in the Department's Description of Controls (pages 9 to 40).

Department's Description of Control	Test Results	Report Page(s)
Help Desk-Telecommunications Service Desk		
Monthly reports are generated from the EMS system based on a fiscal year to track and monitor vendor performance levels for completion of voice orders in the Springfield and Chicago dedicated areas, the non-dedicated areas, non-routine orders and the overall vendor performance levels.	Monthly reports were not generated and the associated tracking and monitoring of vendor performance levels was not performed.	74
Recovery Services		
The Bureau has developed scripts and/or procedures for the recovery of operating system platforms. Recovery Services staff assist in updating and rehearsing these procedures when building the operating systems for customer recovery exercises.	The Department had not developed scripts and/or procedures for the recovery of operating system platforms. In addition, according to Department staff, they did not assist in the updating and rehearsing the various procedures during recovery exercises. This was the responsibility of the staff responsible for the operating system.	78-79
Vendor Management		
Duties performed to manage Bureau contracts included: ▪ Entering product/service and terms and conditions information into an Access database for monitoring and tracking purposes.	The Access database contained some contract information; however, the terms and conditions of the contracts were not maintained in the database.	85-86
Duties performed to manage Bureau contracts included: ▪ Performing periodic cost benefit analyses when appropriate.	Vendor Management stated cost benefit analyses were not conducted.	85-86
All software media or documentation is filed in the software library, in a secured cabinet, by call name.	Software media was not maintained in a secured cabinet or by call name.	86-87
Enterprise Production Operation Services-Production Control		
Proc Acceptance - Any new or changed job or system that is presented for acceptance by CMS, DHS, HFS, DPH or EPA to be placed into the production environment must first pass through the Production Control area.	According to Department staff, Production Control was not responsible for management of Proc Acceptance functions for HFS, DPH and EPA. These functions remained the responsibility of the individual agency. In addition, Production Control had limited responsibility for the management of Proc Acceptance functions for CMS.	98

Job setup and processing - All jobs that are processed in the production environment, for CMS, DHS, DCEO, HFS, DPH, or EPA whether they run through CA-Scheduler or are manually submitted must be setup and processed by Production Control.	According to Department staff, Production Control was not responsible for management of job setup and processing for HFS, DPH and EPA. These functions remained the responsibility of the individual agency. In addition, Production Control had limited responsibility for the management of job setup and processing for CMS.	99
Abend Resolution - When a job abnormally terminates due to a cart problem or a problem with how the job was setup for processing, production control staff correct the problem and restart the job. When it is a problem with the job itself, the application staff corrects the problem. After the application staff fixes the problem, production control is notified and they resubmit the job. All production abends are recorded listing the cause, who was contacted, and when the job was corrected. This documentation is provided daily to all Production Control, I/O, and Library Services staff, as well as to each legacy agency being monitored.	According to Department staff, Production Control was responsible for monitoring HFS, DHS, CMS and DOT abends.	99-100
Enterprise Production Operation Services-I/O Control		
The Input side monitors all production jobs the departments of Central Management Services (CMS), Human Services (DHS), Health and Family Services (HFS), Public Health (DPH), Commerce and Economic Opportunity (DCEO), Transportation (DOT), and the Environmental Protection Agency (EPA). Collectively, these can be referred to as I/O-managed agencies.	The Input side monitored production jobs for CMS, DHS, HFS, DCEO, and DOT. The Department was not responsible for DPH and EPA Input processes and procedures. These functions remained the responsibility of the individual agency.	101
I/O daily shift reports that contain abends, restores, and corrections to production jobs are created and emailed to each legacy agency.	I/O daily shift reports were created for CMS, HFS, DOT, and DHS (IDOT is included in DHS). I/O daily shift reports were not created for DCEO, DPH and EPA.	102
The Output section is responsible for printing and distribution of all documents and reports generated as a result of processing jobs for the departments mentioned above	The Output section was responsible for printing and distribution of all user agencies and not just these seven consolidated agencies (CMS, DHS, HFS, DCEO, DPH, DOT and EPA).	102-103
Monthly job performance reports are produced and submitted to management.	Performance reports were not created for DOT, DCEO, DPH and EPA.	102-103
Enterprise Production Operation Services-Library Services		
Library Support staff are responsible for migrating test environments to production libraries.	The Department was responsible for production libraries for four agencies: Department of Human Services (DHS), Department of Healthcare and Family Services (HFS), Department of Central Management Services (CMS), and Department of Transportation (DOT). The Department was not responsible for other agency moves to production.	107-108

Change Control		
Regardless of platform, the below described path is followed for control of change: ▪ Changes are initiated by the Shared Services Technician or Manager as a result of an Enterprise Service Request (ESR), internal work assignment, or a configuration change. ▪ The Shared Services Technician or Manager identifies the changes to be made and generates a change request. ▪ Change requests are assessed for content and readiness. ▪ Changes are approved and appropriate parties are notified based on change impact. ▪ Changes are implemented. ▪ Changes are reviewed.	The Department's Policy and INFOMAN Procedures did not correspond with the process described in the Description of Control. As a result, the change requests reviewed did not meet all the criteria listed in the Description of Control.	111
Security Administration		
Current approved security policies include Change Management, Data Breach, Laptop Data Encryption, Midrange Backup, and Resource Access. Policies are published by posting to the appropriate repository dependent upon the sensitivity of the material and the targeted audience.	The policies outlined as current and approved, were actually not in effect, and were not published by posting them to the appropriate repository.	114-115
Network Services		
Network Operations staff are responsible for the backbone and POP site management and support. Support includes: delivery, removal and inventory of equipment; installation, maintenance and documentation of all POP site equipment; test and turn-up of all backbone and egress circuits; installation and management of POP sites.	Network Operations did not actually inventory equipment; however, they did have responsibility for ensuring appropriate individuals were notified of such needs prior to installation and upon removal of equipment.	142-143
Routers authenticate authorized individuals for device configuration and maintenance.	Servers were utilized to provide authorized access to the firewalls, routers, and switches maintained by Network Operations, Enterprise Network Support and a few Field Operations routers.	143
Network Services-LAN Application Development		
Tracking the status of requests is performed using a local Access database and/or the Service Request Registration System (SRRS).	Department staff stated the Access database was not used to track requests in the LAN Development Unit.	153-154
Prior to being placed into production, all updates and modifications are reviewed and approved via email by the owner. Once approval is obtained, the developer requests the supervisor to move the changes into production. The supervisor copies the application onto the production drive and then re-tests the application to verify that the application works in the production environment.	The moves to production for both requests were performed by the application programmer, not the supervisor. According to the LAN Application Development Manager, the application programmer routinely moved changes to production.	154
Network Services-PIM		
A secure, limited access SharePoint site is established that contains instructions for PIM staff on how to manage email accounts.	According to the PIM Manager, the SharePoint site was under construction and the procedural documentation had not been placed on the site.	159

Common Systems-Accounting Information System		
AIS interfaces with the Illinois Governmental Purchasing System (IGPS), the Accounts Receivable Posting System (ARPS), the Central Inventory System (CIS) and the Central Payroll System (CPS).	Department staff stated the Central Inventory System did not interface with AIS at this time.	163
Common Systems-Central Inventory System		
CIS has an interface with AIS.	Department staff stated the Central Inventory System did not interface with AIS at this time.	174

APPENDIX D

ACRONYM GLOSSARY

ACL – Access Control List

ACS – Automated Cartridge System

AGR – Department of Agriculture

AIM – Acquisition and Inventory Management

AIS – Accounting Information System

ARB – Architecture Rationalization Board

ARPS – Accounts Receivable Posting System

ASD – Application System Development

BAS – Billing Allocation System

BCCS – Bureau of Communication and Computer Services

BOPM – Bureau of Property Management

BRM – Business Reference Model

Bureau – Bureau of Communication and Computer Services

CAC – Change Advisory Council

CCF – Central Computer Facility

CDMA – Code Division Multiple Access

CFO – Chief Financial Officer

CICS – Customer Information Control System

CIO – Chief Information Officer

CIS – Central Inventory System

CMC – Customer Management Center

CMS – Central Management Services

COOP – Department's Continuity of Operations Plan

CPO – Chief Procurement Officer

CPU – Central Processing Unit

CPS – Central Payroll System

CRF – Communication Revolving Fund

CSC – Customer Solution Center

CSD – CICS System Definition File

CSS2 – Communication Systems Specialist 2

CTAS – Central Time and Attendance System

CTI – Category, Type and Item

DASD – Direct Access Storage Device

DB2 – DataBase 2

DCEO – Department of Commerce and Economic Opportunity

DCMS – Department of Central Management Services

Department – Department of Central Management Services

DFPR – Department of Financial and Professional Regulation

DES – Department of Employment Security

DHS – Department of Human Services

DNR – Department of Natural Resources

DNS – Domain Name Service

DOT – Illinois Department of Transportation

DP – Data Processing

DPH – Department of Public Health

EA&S – Enterprise Architecture and Strategy

EBAS – Enterprise Business Application Services

EMAP – Emergency Management Accreditation program

EMS – Expense Management System

ENS – Enterprise Network Services

EPA – Illinois Environmental Protection Agency

EPMO – Enterprise Program Management Office

EPOS – Enterprise Production Operation Services

ESB – Enterprise Storage Backup

ESR – Enterprise Service Request

EUC – End User Computing

FCIAA – Fiscal Control and Internal Auditing Act

FIPS – Federal Information Processing Standards

FY – Fiscal Year

GIMS – Transaction Type for the Information Management System

GRF – General Revenue Fund

HFS – Department of Health and Family Services

HR – Human Resources

HSM – Hierarchical Storage Management

H/V – Hirsch Velocity

IBiS – Internet Billing System

IBM – International Business Machines

ICN – Illinois Century Network

ID – Identification

IEMA – Illinois Emergency Management Agency

IFB – Invitation for Bid

IGPS – Illinois Governmental Purchasing System

ILCS – Illinois Compiled Statutes

IMS – Information Management System

INFOMAN – Information Management System

I/O – Input/Output

IOC – Illinois Office of the Comptroller

IOIA – Illinois Office of Internal Audit

ISD – Information Services Division

ISP – Illinois State Police

IT – Information Technology

IWAS – Illinois Web Accessibility Standards

IWIN – Illinois Wireless Information Network

JCL – Job Control Language

LAN – Local Area Network

M&P – Methods and Procedures

MAC – Moves/Adds and Changes

MAS90 – Name of application utilized by Business Services

MDC – Mobile Data Computer

MPLS – MultiProtocol Label Switching

NOMAD – Name of application utilized on VM

OA – Office Automation

PAR – Project Assessment Requirements

PCF – Property Control Form

PIM – Program Information Management

PKI – Public Key Infrastructure

PM – Project Management

POP – Point Of Presence

PSR – Paging Service Request or Product Standardization Request

QA – Quality Assurance

RACF – Resource Access Control Facility

RAD – Rapid Application Development

RFC – Request for Change

RFI – Request for Information

RFP – Request for Proposal

RM – Risk Management

RMF – Resource Monitoring Facility

RTC – Regional Technology Center

RTO – Recovery Time Objective

SAMS – Statewide Accounting Management System

SCAS – Service Center Allocation System

SMF – System Management Facility

SMS – System Management Storage

SNA – Systems Network Architecture

SPOC – Single Point of Contact

SPO – State Procurement Officer

SQL – Structured Query Language

SR – Service Request

SRRS – Service Request Registration System

SSL – Secure Socket Level

SSRF – Statistical Services Revolving Fund

SYSLOG – System Generated Log

TCP/IP – Transmission Control Protocol/Internet Protocol

TDR – Telecommunications Data/Intercity Service Request

TGR – Terminal Generation Request

TGS – Tape Generating System

TIMS – Transaction type for the Information Management System

TMS – Tape Management System

TRM – Technical Reference Model

TSO – Time Sharing Option

TSR – Telecommunications Service Request

TTS – Transient Tape System

UPS – Uninterruptible Power Supply

URL – Universal Resource Locator

VOIP – Voice Over Internet Protocol

VOTS – Voice Teleconferencing Services

WAN – Wide Area Network

WSR – Wireless Service Request

z/OS – Zero Downtime Operating System

z/VM – Zero Downtime Virtual Machine