THIRD PARTY REVIEW

Department of Central Management Services
Bureau of Communication and
Computer Services

July 2009

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, 2009

Release Date:
July 8, 2009

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 96 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 5, 2009 to May 26, 2009. 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	2009
Mainframes	4 Units Configured as 11 Production Systems and 6 Test Systems 1 Unit Configured as 5 Systems for Business Continuity
Services/Workload	Impact Printing – 7.2 Million Lines per Month Laser Printing – 14.5 Million Pages per Month
State Agency Users	96
Bureau Employees	2006 -- 777 2007 -- 748 2008 -- 708 2009 -- 679
Historical Growth Trend**	2006 -- 3,217 -- MIPS 2007 -- 3,962 -- MIPS 2008 -- 4,018 -- MIPS 2009 -- 4,035 -- 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: Acting Director: Maureen O'Donnell (7/1/2008 to 8/24/2008) Currently: Director: James Sledge (8/25/2008 to present) During Audit Period and Current Deputy Director/Bureau Manager: Doug Kasamis

REPORT SUMMARY

We identified one significant deficiency for which we could not obtain reasonable assurance over the controls.

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. (See page 6 for additional information)

The Department concurs with the Auditor's recommendations. We are working to improve our billing processes and the billing data we make available for rates that were introduced in the last two years as a result of the IT consolidations. We are also working on a comprehensive methodology document for all of our rates.

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.

Although a Recovery Methodology and Recovery Activation Plan existed, they had not been updated to reflect the current environment and referenced documentation which had not been fully developed.

A recovery test was performed in September 2008; 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 Recovery Activation Plan.

Reliance is being placed on the Department

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 and appropriately document comprehensive tests of the plans on an annual basis. (See pages 6-7 for additional information)

The Department partially concurs with the recommendations and is confident that the deficiencies found in Recovery Services do not impact the Departments capacity to recover the critical environment and applications of the State. This is evident in the results of the latest comprehensive exercise – environment and applications were recovered in 48 hours, with no major issues. Nevertheless, the Department will continue its current efforts to update Recovery Services documentation, enhance and improve Recovery exercises, and communicate Recovery requirements to supported Agencies.

AUDITORS' OPINION

With the exception of the one significant deficiency 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 26, 2009. Our examination started in July 2008 and primarily performed between January 5, 2009 and May 26, 2009, 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 26, 2009.

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.

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 5, 2009 through May 26, 2009. 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 assessments 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 5, 2009 through May 26, 2009. 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 26, 2009, and information about tests of the operating effectiveness of specified controls covers the period from January 5, 2009 through May 26, 2009. 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.

Willi J. Say

William J. Sampias, CISA
Director, Information Systems Audits

Mary K. Lovej

Mary Kathryn Lovejoy, CPA, CISA
Information Systems Audit Manager

June 22, 2009

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 96 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 41 through 177; in addition, we noted one significant deficiency for which we could not obtain reasonable assurance over the controls.

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.

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 51-55 for additional information)

Department Response

The Department concurs with the Auditor's recommendations. We are working to improve our billing processes and the billing data we make available for rates that were introduced in the last two years as a result of the IT consolidations. We are also working on a comprehensive methodology document for all of our rates.

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.

Although a Recovery Methodology and Recovery Activation Plan existed, they had not been updated to reflect the current environment and referenced documentation which had not been fully developed.

A recovery test was performed in September 2008; 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 Recovery Activation Plan.

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 and appropriately document comprehensive tests of the plans on an annual basis. (See pages 68-72 for additional information)

Department Response

The Department partially concurs with the recommendations and is confident that the deficiencies found in Recovery Services do not impact the Departments capacity to recover the critical environment and applications of the State. This is evident in the results of the latest comprehensive exercise – environment and applications were recovered in 48 hours, with no major issues. Nevertheless, the Department will continue its current efforts to update Recovery Services documentation, enhance and improve Recovery exercises, and communicate Recovery requirements to supported Agencies.

The Department responses were provided on June 22, 2009, 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 37) 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
    - Agency Relations
- Infrastructure Services
    - Lan Operations
    - End User Computing
    - Personal Information Management (PIM)
    - 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
- Security and Service Delivery
  - Service Delivery and Implementation
  - Security and Compliance Solutions
- Business Services
  - Revenue Management
  - CRF Expenditure and Invoice Verification
  - SSRF Invoice Verification
  - Appropriations Management
- Customer and Account Management
  - Field Operations
    - Communications Management Center
  - Customer Solution Center
  - Service Reporting
  - Network Services

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

The Enterprise Program Management Office (EPMO) utilizes project management to oversee the implementation of chartered projects and milestones within BCCS. The Enterprise Program Management (EPM) Portal is utilized to capture and coordinate the project lifecycle by facilitating the capture of pertinent data and artifacts for approved projects that BCCS undertakes on behalf of supported agencies. Enterprise Program Management (EPM) processes are documented via narrative descriptions and diagrams within the EPM Portal.

Proposed projects and initiatives are initiated via creation of a Portfolio Record in the EPM Portal and, as appropriate, subsequent submittal of a Project Charter. Chartered Projects are then evaluated by the Information Technology Governance (ITG) team and once approved through governance, are monitored by the EPM Project Management team in conjunction with responsible BCCS' Divisions and/or Supported Agency management.

Projects in the EPM Portal are categorized into Tiers to designate the applicable level of governance and management oversight. Project deliverables, assigned to BCCS, are documented as milestones, under the appropriate project in the EPM Portal. At the EPMO's discretion, SharePoint Team Sites may also be created for selected projects to serve as a project repository (SharePoint Team Sites are optional for Agency Projects).

Specific project management processes including planning, execution, and transition may vary based upon the specific needs of each project. To accommodate this, the EPMO provides a recommended set of artifacts, via a Project Checklist, which are appropriate for most projects. Project Status Report information is also captured within the EPM Portal.

The EPMO coordinates with BCCS Leadership, via the EPM Portal and associated reports, to identify and address project needs within each BCCS Division. Designated Project Managers and Work Coordinators publish periodic Project Status Reports and identify Project Constraints within the EPM Portal. In addition, the EPMO collaborates with BCCS Leadership in the review of priority projects, on a bi-weekly basis, to address exceptions, escalations, constraints, and other aspects of these projects.

IT Governance

Information Technology Governance (ITG) is the responsibility of the Enterprise Program Management (EPM) office in conjunction with Enterprise Architecture & Strategy (EA&S). The Information Technology Governance (ITG) team ensures that business initiatives are in alignment with the standards, guidelines, and overall IT direction of the Department, and manages the application of technology to business needs. There is no formal policy for IT Governance. In order to ensure that the ITG team operates in a consistent manner, a "swim lane" process flowchart is used which outlines what is required from both ITG and the requestor of the initiative.

Written governance information is available for persons requesting or considering IT-related initiatives. Entities proposing an initiative submit a project charter, (a high level definition of the initiative), business and technical requirement documents, and RFP specifications if available. These documents are entered / logged into the ITG module of the Enterprise Program Management (EPM) Portal.

If the specifications in a submitted RFP provide enough information to satisfy all of the areas of the business and technical requirement documents, the RFP may be used in lieu of these documents.

The ITG team is responsible for determining when an initiative moves forward. Determinations are based upon experience and best practices. Examples of information sources considered during this evaluation are the Taxonomy database, Technical Standards, Shared Services, and personal knowledge / experience. Once an initiative is advanced, the advancement is logged in the ITG module.

If for any reason an initiative is denied, an ITG Denial document is completed and attached to the corresponding entry in the ITG module. If the initiative is resubmitted, it will be resumed and marked as such in the ITG module.

d. Billing

The Department is statutorily authorized to provide information technology (IT) and telecommunications services for State agencies, boards and commissions (Agencies). The Department and Agencies share the costs of those services. The Agencies are billed for goods and services provided and remit payment to the Statistical Services Revolving Fund (SSRF) for IT and the Communications Revolving Fund (CRF) for telecommunications. General Revenue Funds (GRF) are also provided for telecommunications operations.

The Department's Accounting Division is responsible for pursuing outstanding SSRF and CRF accounts. Delinquency notices are sent out on a weekly basis and an Aging analysis is sent out monthly. Business Services pursues outstanding Network accounts.

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.

Data to support charges that are not available through the KOMAND IV system are supplied in various ways. These are primarily the Shared Services charges, detailed as follows:

Service	Metric for Billing	Data Source
End User Support	Number of PC's	Supplied by Agencies
Local Area Network	Number of PC's	Supplied by Agencies
Application Hosting	Number of Servers	TVD Database
Storage	Gigabytes	BCCS Storage Team

There is a verification process to ensure the data supplied matches what is billed.

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 services are billed to CMS by telecommunications carriers. CMS then bills users based on their consumption of these services. Billings for network bandwidth usage and/or other network services for constituents that are non-state entities are billed monthly through the Best 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.

e. Help Desk

Customer Management Center (CMC)

The CMC is the 24/7 network support center for the State of Illinois. The CMC uses ICN Remedy to support the backbone and customer access circuits for ICN constituents. Incidents tickets can be initiated either by a constituent call or discovered by a proactive monitoring system - Solar Winds. Incidents are managed in accordance with established procedures located on the CMC Sharepoint site.

CMC also provides backup monitoring of the IT infrastructure using Hobbit. Procedures exist for responding to alarms generated by Hobbit. After 5 p.m. and during non-business hours, weekends and holidays, the CMC provides help desk support for voice, wireless and data services. These tickets are tracked in CMS Remedy. Procedures exist on the CMC Sharepoint site.

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). Escalations are managed in accordance with established procedures located on the CMC Sharepoint site.

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 nonconsolidated 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.

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 MAC services require an ESR. The IT Service Desk has standardized on the ESR process and the intake of service requests in the Remedy system for all consolidated agencies. IT MAC documentation exists for the ESR process. Service requests are submitted to the IT Service Desk 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.

Telecommunications Service Desk

The Telecommunications Service Desk consists of the Telecommunication Help Desk and Telecommunications Provisioning, and is responsible for maintenance (help desk) 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 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 received. 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 telecommunications managers and Quality Assurance staff attend a quarterly meeting with the vendor(s) to review achieved performance levels and other outstanding issues.

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 Provisioning unit is responsible for verifying that 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 assets, 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. The Provisioning unit utilizes EMS as an inventory, billing, and ordering system. When 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, create the vendor(s) order, and establish billing to the appropriate agency. The Provisioning unit validates paper invoices from the vendors for move, add, and change requests against contract pricing for equipment and associated labor charges if applicable. After validating the charges, the provisioning unit signs the invoice and routes to Business Services for processing payment.

New voice systems are sent directly to the appropriate site and are tagged by the Consulting and Procurement unit at the time of acceptance. A Property Control Form (PCF) is completed by the provisioning unit for newly tagged voice systems and attached to the original invoice before it is sent to Business Services for processing.

The Consulting and Procurement unit works closely with the agency Telecom 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. Procedures exist for the Consulting and Procurement unit tasks.

End User Computing (EUC)

CMS/BCCS is responsible for providing maintenance, support, and security of the Infrastructure and resources established to provide desktop and laptop services. The Enterprise Desktop Policy governs these services.

EUC provides personal computer, printer, software, and peripheral support to Consolidated Agencies and CMS Supported Non-Consolidated Agencies. Responsibilities of EUC include handling break-fix incidents as well as service requests for the move, add and change activities associated with the supported personal computer environments.

EUC receives break/fix incident assignments, service requests, and change requests via Remedy. The supervisor of the assigned EUC Unit or designee assigns the incident or request to an EUC technician and creates tasks (if required). The technician executes applicable diagnostic and repair or add/move/change actions, updates the Remedy work log, and resolves the Remedy incident, task and/or request.

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

The CMS DESKTOP/LAPTOP PERSONAL COMPUTER STANDARD document was established to record the new IT shared services standard for desktop and laptop personal computers. These standards are implemented as part of the conversion to the new illinois.gov environment.

f. Recovery Services

The Department provides recovery services for enterprise mainframe environments in order to minimize the risk of disrupted services or loss of resources using vendor contracted services. The following contingency plans and templates provide guidance and reference material to address restoration of various client environments:

1. Continuity Methodology
2. Recovery Activation Plan.

The Department, as defined in the Continuity Methodology, conducts scheduled annual regional and local mainframe recovery tests that exercise two levels of recovery:

1. Comprehensive – enterprise mainframe environment to exercise all qualified critical mainframe applications simultaneously recovered on a remote host.
2. Local – exclusive mainframe environments for individual applications recovered independently at a local recovery exercise host system.

The Department maintains a Critical Application Database built on information received from State agencies. State agencies are required to categorize, prioritize and define critical information as defined in the Continuity Methodology

The Department maintains scripts and/or procedures for the recovery of mainframe operating system and subsystem platforms. Recovery Services staff assist in updating and rehearsing these procedures during the comprehensive and local recovery exercises.

The Department utilizes an off-site storage facility for the storage of data tape backups and recovery information (Hotbox).

The Department stores critical recovery information that is defined in the Continuity

Methodology. The Hotbox provides hardcopy recovery data to be used in the event of an outage. The Hotbox is maintained at the off-site storage facility and is updated on a yearly basis.

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, Development and Logistics unit coordinates and facilitates internal personnel paperwork, workforce training, development and implementation, and workforce logistics for the Bureau. For HR related transactions the unit refers 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 and any policies or procedures initiated and enforced by Shared Services.

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 a repository for reference and monitoring purposes.

Documented procedures for reconciling desktop, mainframe and midrange software are outlined in the AIM/Vendor Management Guide. 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.

Warehouse and Inventory

The BCCS warehouse is responsible for the receipt, inventory, storage, security and limited distribution of EDP type equipment for CMS. The CMS Property Control Procedures are used as a baseline for managing equipment that is stored at the BCCS warehouse and managed in the CMS inventory. The BCCS inventory is broken down into three basic categories: EDP, Data and Voice related equipment. The inventory databases that manage these inventories include Monies Co 4, EMS11, Remedy and CIS.

j. Service Reporting and Agency Communication

<u>Service Reporting</u>
The current purpose and goal of Service Reporting is to lend insight, visibility and a basis for improvement of services.

Monthly and quarterly reporting currently includes Incidents, Service Requests, help desk calls, Mainframe, Email, WAN, and SSRF Invoicing. The Bureau prepares monthly and quarterly activity reports for each consolidated agency demonstrating volume, workload, and select cycle times allowing for interpretation of trends.

Incidents and service request reports represent data from the Remedy help desk system. During FY08, this reporting began with data extracts from Remedy, imported to Excel spreadsheets for processing to produce tables moved to Word documents. During FY08, training was gained and reporting migrated to Crystal Reports running a month of parallel reporting from the former Excel spreadsheets and Crystal Reports to ensure continuity. The monthly and quarterly Crystal Reports are configured to retain the “snap-shot” queried data as the Remedy system is a live and changing system subject to changes in criteria as tasks are worked and resolved. Review is performed at the time of processing, during document assembly and executive final review. Both verbal and electronic questions are addressed concerning any data issues observed during document assembly review, executive review or review by the shared service agencies. The SQL used is documented.

Calls received are reports generated by the Avaya phone system and forward for reporting. The Avaya reports are imported to an Access database. Reports are generated using Crystal Reports. Data review takes place during data import to Access.

Mainframe data is provided for processing as an extract from Tivoli Decision Support and Workload Manager. The extracts include spreadsheet data and work logs. The data goes through procedures requiring manual import, examination and interpretation to establish the final output. Mainframe reporting is undergoing revision targeted for October reporting in November, moving to a direct import to Access and generating reports via Crystal Reports.

E-mail represents a pass-through report from Ironmail perimeter filtering. This reporting is generated from the Ironmail system by the PIM unit.

WAN reporting is provided from manual compilation of data from outage notices and router and switch logs. The spreadsheet compilation is then forwarded by the network group for processing. The WAN data is updated to an Excel spreadsheet where the initial report spreadsheet is created and then moved to a Word table. The table is checked during processing for continuity but crosscheck verifications are not possible.

Invoice reporting is an extract provided from the PACES system used for the agency SSRF billing. The extract provided is imported to an Access database, generating reports using Crystal Reports. The reported totals are cross-checked against actual shared service agency invoicing totals.

Reports are posted to a SharePoint site available to agency CIO's and their designee.

Agency Communications:

The Department 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 were replaced as of 8/26/2008 by the new BCCS Service Site, cms.partner.illinois.gov/bccs/service/default.aspx, which allows agency CIOs to access their agency specific information from BCCS on a self-service basis.

Ad-hoc meeting requests are honored by the AR team. Periodically, the Bureau hosts topic specific meetings/forums with various customer interest groups. The customer-focused newsletter, the BCCS Pulse, provides 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. Note: As of 9/1/2008, the Agency Relations team reports to a new manager.

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. The ESB Guide helps 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, and ADRDSSU Restore. 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.

z/OS Backups are performed on the mainframe operating system data. System data is backed up daily and weekly with the weekly copies sent to the regional vault. Backups of non-operating system files 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 upon receipt of a Remedy ticket. ESB restores the data, updates the Remedy work log, and closes the record to reflect said actions.

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: Systems Operation Center, Input/Output (I/O) Control, Production Control, and Library Services.

System Operations Center

The Systems Operation 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 Systems Operation Center operates 24 hours a day, 7 days a week, 365 days a year. The Systems Operation Center utilizes the Remedy Change Management System to coordinate and oversee implementation of changes to the computing environment. Remedy is used to record and monitor incident resolution. The Systems Operation Center Data Processing Guide is utilized as a reference for operational tasks. The Focal application is used to assist Systems Operation Center in monitoring and maintaining system availability in an efficient and consistent manner. The Systems Operations Center provides input to the Daily Shift Report which is then distributed via an automated mechanism in the Focal application. The Daily Shift Report is used to document outages/issues. Shift Change Checklists are utilized by the Systems Operation Center to ensure consistent verification of system availability. SYSLOG is utilized as a tool to reference system activity.

Input/Output (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), Transportation (DOT), the Department of Revenue (REV) and the Environmental Protection Agency (EPA). Collectively, these can be referred to as I/O Managed agencies.

With the exception of REV, the processing for the I/O managed agencies is handled by staff at the Harris Building (100 South Grand Avenue East) and the processing for REV is conducted at the Willard Ice Building (101 West Jefferson).

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. 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 IO Managed agency except DCEO.

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 and for the Department of Commerce and Economic Opportunity (DCEO), Department of Agriculture (AGR), and other agencies utilizing the standard CMS printing services. 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 via the DHS Warehouse Control System (WCS). DCEO and DOT statistics are now included in the monthly reports, but it will be the last quarter of 2008 before EPA and DPH statistics are included in the reporting.

With the exception of the printing performed for REV at the Willard Ice Building, physical control over the distribution of printed material for the remaining I/O Managed Agencies (done at the Harris Building 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 for job acceptance are documented in each agency's standards manual if they exist; for DHS, DOT, and HFS these are located at the Agency Intranet.

Proc Acceptance - Any new or changed job or system that is presented for acceptance by CMS, DHS, DOT, DPH or EPA to be placed into the production environment must first pass through the Production Control area. The documentation for DHS, DOT, and HFS 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, DOT, 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 CMS, DHS, HFS, REV, DCEO, DOT, DPH, or EPA job abnormally terminates due to a cart problem or a problem with how the job was setup for processing and if problem can not be resolved by I/O Controls staff the production control staff are called upon to correct the problem and restart the job . When it is a problem with the job itself, the agency 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 (shift reports) 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 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. The Tape Library is responsible for all tape orders, initializing, labeling, degaussing, and destruction of media, as well as movement of media resources. The Tape Library utilizes the ISD Library Guide and the ISD Media Guide to ensure that duties are performed in a consistent manner. 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.

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 DHS, HFS, DOT, and EBAS 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 , 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 modification 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/Quality Assurance

The Department's Change Management Unit is responsible for managing changes to the Department's environment (except for applications under EBAS control) that are initiated as the result of an ESR (Enterprise Service Request), a configuration change, or an internal work assignment. The Remedy Change Control System is used to create, review, approve and track change requests to Department systems. The Change Management Policy is used to govern these activities. The Remedy Change Guide is a procedural document which supports the Change Management Policy.

Change requests are visually reviewed for content and completeness by the Change Management Unit. A Change Advisory Committee (CAC) has been established which meets as needed to review submitted changes. While the Change Management Unit reviews all changes, this committee is responsible for reviewing the changes submitted as either a "medium" or "high" priority. Changes to be reviewed are made available to members of the CAC before the meeting, and the results of the meeting are made available after the meeting as meeting minutes.

If a major incident or problem is directly related to an implemented change, A Post Implementation Review (PIR) is completed. This information is then attached to the change request for documentation purposes. A spreadsheet is maintained by the Change Management Unit which tracks these PIRs.

Infrastructure Quality Assurance and Methods

The Infrastructure Quality Assurance and Methods group act as facilitators for organizing, planning and controlling work activities for the Infrastructure Services Division related to Agency IT projects.

Process and procedures that govern this process are located in the IQAM Guide.

4. Security Administration

The Department's security posture is comprised of compliance and auditing functions that include corrective action tracking, security assessments, security awareness promotion, security strategy development, security authorization list review, and policy development.

Corrective action tracking is achieved through collection of recommended improvements from sources such as audit recommendations and internally conducted vulnerability assessments. These recommended improvements are entered into a database. Reports generated from this database are discussed at BCCS Leadership meetings. Each appropriate BCCS Leadership member is responsible for developing detailed actions that address recommendations and for entering any updates into the database. The implementation of the corrective action is the responsibility of the appropriate area.

Security assessments are conducted by the Department's Technical Safeguards unit. Results of those assessments are made available to appropriate BCCS staff that has responsibility for remediation. The Technical Safeguard Unit Security Audit Procedures Rules of Engagement , located on a secure, shared network drive, outlines typical actions that Technical Safeguards staff follow when conducting assessments. Cyber security incident responses are also addressed by the team. Procedures for responding to these incidents exist.

Security awareness is promoted by placing relevant information on an enterprise accessible web site (http://bccs.illinois.gov) where security related news releases, tips, posters, and guidelines can be viewed by Department staff.

Security authorization list are continuously updated and reviewed every six months with the agencies. Process and procedures documentation guide these activities. The areas reviewed include; RACF coordinators, media pickup, IMS/DB2, CICS regions, Mobius, Web Services, and IDMS.

RACF violations for BCCS staff are reviewed every two weeks. Violation reports are provided to the individual responsible, requesting an explanation of the violation. These explanations are then reviewed for reasonableness. Procedures exist for this process.

Information collected from all the activities described above is used as the foundation to develop and maintain the Department's long-term security strategy – *Secure Illinois*. The strategy includes eight domains defined by; capabilities to implement, the projects to attain those capabilities, and high-level timelines for completion.

Policy development is a collaborative effort that crosses multiple organizational units. Results of this effort are approved policies published on the Department's web site (http://bccs.illinois.gov). Procedures to guide the development and approval process are documented for reference. Templates have been developed to ensure consistency in writing policy, procedures and standards. Policy update memos are distributed periodically to impacted users to announce updates to the policies.

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, locks, 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, security guards, and video surveillance are used to limit or monitor physical entry into the following buildings: the Central Computer Facility (201 W.Adams), and the Communications Building (120 W.Jefferson) in Springfield.

Physical security at 401 S.Clinton, Chicago is a joint effort between the Department of Human Services, Department of Health and Family Services and the CMS Bureau of Property Management. Security guards operate during business hours. CMS computing facilities are protected by Cipher locks.

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, and at the Communications 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.

The H/V system control panels have their own Uninterruptible Power Supply (UPS) to provide power to the control panels, and the access control devices they support. Separate UPS module supplies uninterruptible power to certain electric locks.

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.

Remote Monitoring Facility (RMF) reports are run weekly and monthly. These reports are stored on a secured drive and are available to management to monitor system resources and CPU utilization.

z/VM

z/VM (z/Virtual Machine) is a mainframe operating system utilized at the Central Computer Facility. z/VM is a time-sharing, interactive, multi-programming operating system for IBM mainframes. The major subsystem that is supported in z/VM is NOMAD which is business intelligence software for enterprise reporting and rapid application development. The client security software administrator must request and obtain a VM User ID from the z/VM staff. Clients are assigned user IDs with restrictive security rights. The z/VM directory is restricted to general access as it 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.

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 monitoring the security violations. The CMS Data Security Administrator reviews CCF staff violations and distributes to each CCF staff their violations, Staff must sign and return their report with an explanation to the CMS Data Security Administrator. The client security software administrators have the capability of producing the violation reports for their agency. System options and parameters are implemented to protect data and resources.

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 monitors these systems to confirm that devices and systems are properly, installed, configured, and maintained.

a. Network Services

Network Services manages the Illinois Century Network (ICN), the Illinois Wireless Information Network, and engineering responsibilities related to State of Illinois telecommunications services. The Division consists of two teams which includes Network Operations and Enterprise Network Support.

The ICN obtains public Internet services from multiple providers. 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. An additional and final pass through a centralized firewall system provides security for all agencies before reaching the 'Internet'.

Network Services - Network Operations

Network Operations develops standards and designs, installs, maintains and manages the ICN Backbone including backbone circuits, egress circuits, routers, firewalls, switches, fifteen Point of Presence (POP) sites, WAN monitoring tools and WAN services, including DNS, educational and state agency content filtering, and IP Video. . Network Operations maintains network diagrams associated with the ICN backbone connectivity and WAN services. Solarwinds Orion is used to manage and monitor the ICN Backbone. TACACS servers authenticate authorized individuals for device configuration and maintenance.

Network Services – Enterprise Network Support

Enterprise Network Support designs and supports 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. TACACS servers authenticate authorized individuals for device configuration and maintenance.

Enterprise Network Support has oversight of 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. Fiber records are maintained in a Microsoft Access database as well as within EMS 11. 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 team 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 and distribution routers.

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.

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 "Illinois Statewide Policy Manual," located on the CMS BCCS Catalog website at: http://bccs.illinois.gov/pdf/iwin/iwinpolicymanual.pdf 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.

The IWIN network infrastructure utilizes redundant routers which connect servers to the provider network. TACACS Servers 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. The RTCs are strategically placed to provide close proximity to the constituents they serve.

Field Operations is responsible for the provisioning of hardware and circuits for constituent connections to the ICN as well as providing technical help desk support as needed. Field Operations uses CMS Remedy, ICN Remedy and EMS11 for help desk and provisioning in accordance with established procedures posted to the team Sharepoint site. Service request forms used by constituents are available on Illinois.net and bccs.illinois.gov.

Field Operations is also responsible for maintaining ICN DNS records within the regional DNS servers in accordance with established procedures.

d. LAN Application Development / Web Services

LAN Application Development:
The LAN Application Development section is responsible for the development of custom application software, including but not limited to microcomputer, LAN, Internet/Intranet, and client server applications. The section follows the set standards and methodology for Rapid Application Development maintained by the EBAS Quality Assurance section. Tracking the status of requests is performed by using the Service Request Registration System (SRRS).

The Enterprise Remedy Change Management system is used for change control. The business owner can request changes to their applications via Remedy. User security to applications is determined and implemented based on the software tool used for development. Section personnel are responsible for maintaining security for applications, but the business owner is responsible for informing the section of user access requirements.

Web Services
The Bureau provides web services that enable 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 sites/applications. The "New Web Site Checklist" is used to ensure completeness of information for new static web sites. This checklist resides on the Web Services/Lan Application Development sharepoint site.

Web sites are reviewed by the Department's Illinois Office of Information and Communication for compliance with the IITAA Implementation Guidelines for Web-Based Information and Applications (based on the Illinois Information Technology Accessibility Act (IITAA). This information is located on the Illinois Depart of Human Services web site. Prior to being placed into production, updates and modifications are reviewed and approved by the owner. Once approval is obtained, the developer requests that their supervisor (or designee) move the changes into production. An Access database (which is used to track requests) is then updated with this information.

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. A standardized form is used for these requests. Domain naming conventions are outlined at http://www.illinois.gov/Tech/govpolicy.cfm.

e. PIM

The Personal Information Manager (PIM) section is responsible for providing a centralized and consolidated platform that facilitates a statewide common architecture for managing email. The General IT Policy is used to govern these activities. The Enterprise Shared Services Email Standards is a document that supports this policy. This document and other procedural documents are used by the PIM group to guide their actions, and are available on the BCCS central repository.

The PIM group has an Enterprise class virus filtering and SPAM solution in place called IRONMAIL that provides both anti-virus and spam filtering services.

PIM also provides Blackberry server and client services.

PIM is governed by Change Management Policy and Procedures.

f. LAN Services

The LAN 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 maintains configuration standards for LAN infrastructure devices. These standards are implemented on newly deployed equipment.

LAN Services is responsible for entering rules into the firewalls and monitoring security violations via firewall monitoring software. Security logs are processed for possible violations and reviewed for performance issues and/or intrusion prevention.

LAN Services is governed by Change Management Policy and Procedures.

Scheduled backups of critical device configurations are performed twice daily.

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, 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), 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; adds, deletes, and updates to the inventory data takes affect as soon as a transaction meets all the required criteria. CIS has the ability to utilize an optical scanner to read bar code labels during a physical inventory by using additional external software. 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 meets all the GASB-34 rules; it allows the user agencies the ability to accurately track depreciation on items that they specify.

The Department has developed an online CIS User Manual. 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 the previous day's 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.

This Page Intentionally Left Blank

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 41 through 152) and Application Controls (pages 153 through 177) sections of this report.

This Page Intentionally Left Blank

BUREAU ORGANIZATION

EXISTING ENVIRONMENT

Background Provided by the Department: 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)

Department Description of Control: 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
    - Agency Relations
- Infrastructure Services
    - Lan Operations
    - End User Computing
    - Personal Information Management (PIM)
    - 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
- Security and Service Delivery
    - Service Delivery and Implementation
    - Security and Compliance Solutions
- Business Services
    - Revenue Management
    - CRF Expenditure and Invoice Verification
    - SSRF Invoice Verification
    - Appropriations Management

- Customer and Account Management
    - Field Operations
        - Communications Management Center
    - Customer Solution Center
    - Service Reporting
    - Network Services

<u>Tests Performed:</u> Reviewed organizational chart and interviewed staff.

<u>Test Results:</u> 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

Background Provided by the Department: The Bureau monitors technological trends through strategic and business planning.

Department Description of Control: 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 ARB meeting summaries and interviewed staff.

Test Results: A Strategic Plan for FY09 was not developed.

For FY08, the Bureau's Leadership Team assisted the Deputy Director in the development of the "FY08 Information Technology and Network Strategic Plan", dated January 22, 2008.

A cross-agency subcommittee of the Architecture Rationalization Board (ARB) is expected to develop and publish a new State IT Strategy in FY10.

No significant exception noted; however, a current Strategic Plan had not been developed.

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, Consolidated Project Portfolio database, and interviewed staff.

Test Results: On October 31, 2008 the Chief Information Office – Office of the Governor sent a memorandum to Consolidated Agencies, Illinois State Police, Department of Corrections, and Department of Children and Family Services requesting FY09 and FY10 business and resource needs. Information received from the agencies was incorporated into individual and combined budget and forecast spreadsheets, BCCS Strategic portfolio, and the Consolidated Project Portfolio database.

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 ARB meeting summaries, Product Standardization Requests, and interviewed staff.

Test Results: The Enterprise Architecture Taxonomy Database Management System contained 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

We obtained and reviewed three Product Standardization Requests that were finalized during the audit period.

The ARB held several meetings during the audit period and addressed issues including guidelines, bylaws, guiding principles, initiatives, and standards. The ARB developed the State of Illinois – IT Guiding Principles (August 2008) to guide IT decisions and support strategic direction.

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. Although strategic planning activities were being conducted, the Department should enhance its process to ensure Strategic Plans are current, updated at least annually, and address at least three years.

ADMINISTRATION
Project Management

EXISTING ENVIRONMENT

Department Description of Control: The Enterprise Program Management Office (EPMO) utilizes project management to oversee the implementation of chartered projects and milestones within BCCS. The Enterprise Program Management (EPM) Portal is utilized to capture and coordinate the project lifecycle by facilitating the capture of pertinent data and artifacts for approved projects that BCCS undertakes on behalf of supported agencies. Enterprise Program Management (EPM) processes are documented via narrative descriptions and diagrams within the EPM Portal.

Tests Performed: Reviewed the EPM portal and interviewed staff.

Test Results: We reviewed the EPM Portal, noting the portal captured the project lifecycle and defined the project lifecycle in descriptive narratives and diagrams. In addition, Department staff performed a walkthrough of a project in the EPM Portal to identify and illustrate the different phases of the project lifecycle.

No significant exception noted.

Department Description of Control: Proposed projects and initiatives are initiated via creation of a Portfolio Record in the EPM Portal and, as appropriate, subsequent submittal of a Project Charter. Chartered Projects are then evaluated by the Information Technology Governance (ITG) team and once approved through governance, are monitored by the EPM Project Management team in conjunction with responsible BCCS' Divisions and/or Supported Agency management.

Tests Performed: Interviewed staff.

Test Results: Department staff stated Chartered Projects were evaluated by IT Governance prior to being submitted to the EPM Project Management team. Once the Project Management team received the project from IT Governance, a project manager was assigned. The project manager was either Department staff and/or supported agency management.

No significant exception noted.

Department Description of Control: Projects in the EPM Portal are categorized into Tiers to designate the applicable level of governance and management oversight. Project deliverables, assigned to BCCS, are documented as milestones, under the appropriate project in the EPM Portal. At the EPMO's discretion, SharePoint Team Sites may also be created for selected projects to serve as a project repository (SharePoint Team Sites are optional for Agency Projects).

Tests Performed: Reviewed EPM Portal and interviewed staff.

Test Results: The EPM Portal used Tiers as a method to categorize projects to provide applicable level of governance and management oversight. The three primary Tiers were:

- Tier 1: Governance Exempt – Projects that did not meet the criteria for IT Governance.
- Tier 2: Governance Required – Projects that met the criteria for IT Governance.
- Tier 3: Enterprise/Multi-Agency – Projects that met the criteria for IT Governance and were enterprise level and/or multi-agency projects.

Project milestones were documented in the status reports.

No significant exception noted.

Department Description of Control: Specific project management processes including planning, execution, and transition may vary based upon the specific needs of each project. To accommodate this, the EPMO provides a recommended set of artifacts, via a Project Checklist, which are appropriate for most projects. Project Status Report information is also captured within the EPM Portal.

Tests Performed: Reviewed EPM Portal and interviewed staff.

Test Results: The Department did not maintain official project management policies and procedures. However, the Department did publish a recommended set of artifacts via a Project Checklist which was located within the EPM Portal. In addition, Project Status Reports were maintained within the EPM Portal.

No significant exception noted.

Department Description of Control: The EPMO coordinates with BCCS Leadership, via the EPM Portal and associated reports, to identify and address project needs within each BCCS Division. Designated Project Managers and Work Coordinators publish periodic Project Status Reports and identify Project Constraints within the EPM Portal. In addition, the EPMO collaborates with BCCS Leadership in the review of priority projects, on a bi-weekly basis, to address exceptions, escalations, constraints, and other aspects of these projects.

Tests Performed: Reviewed the EPM Portal and interviewed staff.

Test Results: The EPM Portal had the capability to produce the following standard reports:

- Project Status Report
- Current Deliverables Report
- BCCS Priority Report
- Programs Report
- BCCS Constraints Report

In addition, the EPM portal had the capability to produce ad hoc reports based on specified criteria.

EPMO communicated the status of projects via the reports on a bi-weekly basis during the ARB meetings.

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
IT Governance

EXISTING ENVIRONMENT

Background Provided by the Department: Information Technology Governance (ITG) is the responsibility of the Enterprise Program Management (EPM) office in conjunction with Enterprise Architecture & Strategy (EA&S).

Department Description of Control: The Information Technology Governance (ITG) team ensures that business initiatives are in alignment with the standards, guidelines, and overall IT direction of the Department, and manages the application of technology to business needs. There is no formal policy for IT Governance. In order to ensure that the ITG team operates in a consistent manner, a "swim lane" process flowchart is used which outlines what is required from both ITG and the requestor of the initiative.

Tests Performed: Reviewed the IT Governance Policy, swim lane process, and interviewed staff.

Test Results: After the submission of the Description of Control, the Department developed an IT Governance Policy, dated December 15, 2008. The purpose of the IT Governance Policy was to "define the ITG scope, roles and responsibilities." The policy stated that each user agency should also establish procedures and assign responsibility to specific agency personnel to achieve compliance with this policy.

IT Governance was defined as the process for agency submitted initiatives as projects by ensuring alignment with the enterprise architecture and registering compliance requirements.

IT Governance applied to IT projects within the following criteria:

a. New business functionality was being added.
b. A move to a new or updated platform was being made.
c. An old system was being replaced (lifecycle).
d. A system was being in-sourced or outsourced either partially or completely.
e. The work had enterprise implications.

During the governance process, IT Governance staff determined if the project initiatives were compliant with the enterprise architecture. Agencies were required to submit procurement specifications that involved third parties in an IT solution, ensure compliance with all applicable requirements for the defined initiative, and collaborate with the Department to establish a deployment package. The IT Governance staff reserved the right to deny initiatives with compliance issues or unresolved exceptions during the swim lane process.

Agencies were able to contact the State CIO for a waiver on any denials.

A flowchart outlined the swim lane process and it consisted of three gates and a resumption process. Each flowchart identified the Business Agency and IT Governance roles and responsibilities during the process.

No significant exception noted.

Department Description of Control: Written governance information is available for persons requesting or considering IT-related initiatives. Entities proposing an initiative submit a project charter, (a high level definition of the initiative), business and technical requirement documents, and RFP specifications if available. These documents are entered / logged into the ITG module of the Enterprise Program Management (EPM) Portal.

If the specifications in a submitted RFP provide enough information to satisfy all of the areas of the business and technical requirement documents, the RFP may be used in lieu of these documents.

Tests Performed: Reviewed the EPM Portal and interviewed staff.

Test Results: Written governance information included the forms for documenting the project charter and business and technical requirements, swim lane process flow chart, the IT Governance Policy dated December 15, 2008, and State of Illinois IT Guiding Principles. In addition, documentation from an IT Governance Update presentation at the July 23, 2008 Architecture Rationalization Board meeting was provided.

We reviewed the EPM Portal, noting project charters, business and technical requirements, and RFPs (if required) were maintained in the portal.

No significant exception noted.

Department Description of Control: The ITG team is responsible for determining when an initiative moves forward. Determinations are based upon experience and best practices. Examples of information sources considered during this evaluation are the Taxonomy database, Technical Standards, Shared Services, and personal knowledge / experience. Once an initiative is advanced, the advancement is logged in the ITG module.

Tests Performed: Reviewed the ITG module (EPM Portal) and interviewed staff.

Test Results: IT Governance staff utilized the technical reference model, research on solutions, utilized previous knowledge over the existing environment, and detailed discussions to make decisions regarding initiatives.

We reviewed the EPM Portal, noting the module documented approvals for the IT Governance process for proposed initiatives.

No significant exception noted.

Department Description of Control: If for any reason an initiative is denied, an ITG Denial document is completed and attached to the corresponding entry in the ITG module. If the initiative is resubmitted, it will be resumed and marked as such in the ITG module.

Tests Performed: Reviewed EPM Portal, denial documentation, and interviewed staff.

Test Results: During the audit period, there was one project initiative denied. The EPM Portal maintained the appropriate denial documentation.

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.

BILLING
Statistical Service Revolving Fund (SSRF)
and
Communications Revolving Fund (CRF)

EXISTING ENVIRONMENT

Background Provided by the Department: The Department is statutorily authorized to provide information technology (IT) and telecommunications services for State agencies, boards and commissions (Agencies). The Department and Agencies share the costs of those services. The Agencies are billed for goods and services provided and remit payment to the Statistical Services Revolving Fund (SSRF) for IT and the Communications Revolving Fund (CRF) for telecommunications. General Revenue Funds (GRF) are also provided for telecommunications operations

Department Description of Control: The Department's Accounting Division is responsible for pursuing outstanding SSRF and CRF accounts. Delinquency notices are sent out on a weekly basis and an Aging analysis is sent out monthly. Business Services pursues outstanding Network accounts.

Tests Performed: Reviewed Fiscal Operation Policy, delinquency notices, and interviewed staff.

Test Results: The Department's Fiscal Operations Policy required the "collection of unpaid agency receivables, referral of unpaid receivables to alternative collection efforts and write-off of accounts receivable as uncollectible."

The Department sent out delinquency notices at various times during the billing period. We reviewed 17 delinquency letters, noting no exceptions.

According Business Service staff, one account had been turned over to the Comptroller's off-set system.

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, 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.

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 February 2009, the Department billed user agencies approximately $85.4 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.

Data to support charges that are not available through the KOMAND IV system are supplied in various ways. These are primarily the Shared Services charges, detailed as follows:

Service	Metric for Billing	Data Source
End User Support	Number of PC's	Supplied by Agencies
Local Area Network	Number of PC's	Supplied by Agencies
Application Hosting	Number of Servers	TVD Database
Storage	Gigabytes	BCCS Storage Team

There is a verification process to ensure the data supplied matches what is billed.

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 (updated monthly to include data from current bills), 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 and system data for the months of November and December 2008 and found the Department:

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

For example, during our review we found the source data for the number of email accounts, PCs, and servers did not support or match agency billing statements.

Although we identified problems with the supporting information that populated the billing system, we were able to reconcile the information in the various billing system reports to the two agencies' billings for the months of November and December 2008.

In the event the Department and agency determined an inappropriate charge had been assessed, the agency may request a credit. We reviewed documentation associated with 21 issued credits, noting no exceptions.

As a result of the consolidation, the Department developed three new rates for consolidated services. However, our review indicated a lack of a consistent methodology for rate calculations.

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.

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.

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 FY08 Allocation Plan in March 2009. We did not perform a detailed review of the Plan as it is routinely reviewed in the Department's annual Financial and Compliance Examinations, which are available on our website at http://www.auditor.illinois.gov.

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

No significant exception noted.

Communications Revolving Fund (CRF)

Department Description of Control: 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 services are billed to CMS by telecommunications carriers. CMS then bills users based on their consumption of these services.

Billings for network bandwidth usage and/or other network services for constituents that are non-state entities are billed monthly through the Best MAS90 system.

Tests Performed: Reviewed CRF billing procedures, MAS90 billing procedures, and interviewed staff.

Test Results: According to the CRF billing overview, approximately 95% of the CRF billings were generated through the EMS system; the remaining 5% were generated through AIS. The EMS billing system and AIS allowed for re-rated charges as well as pass-thru charges.

The Department billed network services and bandwidth usage through the MAS90 system.

No significant exception noted.

Department Description of Control: 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 November and December 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 four issued credits, noting no exceptions.

For July through February 2009, the Department billed user agencies approximately $63.7 million.

No significant exception noted.

Department Description of Control: 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.

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 FY08 Allocation Plan in March 2009. We did not perform a detailed review of the Plan as it is routinely reviewed in the Department's annual Financial and Compliance Examinations, which are available on our website at http://www.auditor.illinois.gov.

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

No significant exception noted.

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.

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.

Tests Performed: Reviewed procedures.

Test Results: According to the CSC Service Desk Guide, dated January 2008, "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."

No significant exception noted.

Department Description of Control: 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, tested Remedy tickets, and interviewed staff.

Test Results: The Department developed the CSC Service Desk Guide, dated January 2008, "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."

Additionally, the CSC Service Desk Guide provided information regarding enterprise-wide management, escalation and notifications, and other operational needs.

We reviewed 25 Remedy tickets, noting the work logs were completed and captured information regarding the problem and resolution. Additionally, we noted it took an average of 4.5 days for a ticket to be closed.

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 nonconsolidated 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.

Tests Performed: 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 staff.

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, tested 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 25 Remedy tickets, noting the tickets were completed appropriately. Additionally, we noted the average closure time was 4.5 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 MAC services require an ESR. The IT Service Desk has standardized on the ESR process and the intake of service requests in the Remedy system for all consolidated agencies. IT MAC documentation exists for the ESR process. Service requests are submitted to the IT Service Desk via email.

Tests Performed: Reviewed instructions and procedures, IT Coordinator lists, tested ESRs, and interviewed staff.

Test Results: The Department developed the Enterprise Service Request (ESR) Instructions, dated June 27, 2008. The Instructions provided guidance to the agency and the IT Service Desk staff on the completion of an ESR.

An ESR provided "the end user a means to request standard or routine software or hardware related additions, moves or changes to their desktop system." An ESR was required for IT changes. After the receipt of the ESR, IT Service Desk staff were to create a Remedy ticket, assign it to the appropriate team, and attach the ESR.

According to the Remedy User Guide, IT Service Desk staff were charged with reviewing ESRs for completeness and accuracy. In addition, the Department developed several procedures to assist staff in the completion of Remedy tickets, ESRs and Addendums.

We reviewed 25 Service Requests from the Remedy Change Management Module, noting the IT changes had an ESR attached.

No significant exception noted.

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 Web site (www.bccs.illinois.gov/downloads.htm) and are provided guidance by the IT staff when necessary.

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 ESRs noting they had been 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.

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 uses ICN Remedy to support the backbone and customer access circuits for ICN constituents. Incidents tickets can be initiated either by a constituent call or discovered by a proactive monitoring system - Solar Winds. Incidents are managed in accordance with established procedures located on the CMC Sharepoint site.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: The CMC provided (24 hours a day, 7 days a week, and 365 days a year) support to various State agencies and entities.

Incident Tickets were created in ICN Remedy by the CMC staff as a result of either a phone call or an alarm within the Solar Winds monitoring system.

The CMC Sharepoint site contained the following methods and procedures to assist CMC staff with incidents; CMC: Remedy Ticket Procedures and the CMC: M&P After Hours Server Support. We reviewed the procedures, noting the Remedy Ticket Procedures did not include a process to ensure sensitive transactions generated from incident tickets, such as those involving security settings, were approved by authorized staff.

No significant exception noted; however, the Remedy Ticket Procedures did not include a process to ensure sensitive transactions generated from incident tickets were approved by authorized staff.

Department Description of Control: CMC also provides backup monitoring of the IT infrastructure using Hobbit. Procedures exist for responding to alarms generated by Hobbit. After 5 p.m. and during non-business hours, weekends and holidays, the CMC provides help desk support for voice, wireless and data services. These tickets are tracked in CMS Remedy. Procedures located on the CMC Sharepoint site.

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

Test Results: The CMC, along with the Systems Operations Center utilized Hobbit to monitor the IT infrastructure. However, the Department was in the process of replacing Hobbit with the "What's Up Gold" monitoring system. The Department expected to have the new monitoring system in production by March 2009.

The CMC Sharepoint site contained the CMC: M&P After Hours Server Support procedure to assist in responding to Hobbit alarms.

Upon notification of a Hobbit alarm, a Remedy Help Desk ticket was opened. We reviewed 25 CMS Remedy Help Desk tickets, noting they had been completed appropriately.

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.

No significant exception noted.

Department Description of Control: 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). Escalations are managed in accordance with established procedures located on the CMC Sharepoint site.

Tests Performed: Reviewed policies, tested Remedy tickets, and interviewed staff.

Test Results: The CMC Sharepoint site contained the CMC M&P: Managing Escalation and Carrier vendor management procedures (last revised August 8, 2008). The procedures identified general escalation information along with guidance on escalating issues to vendors.

The Department had obtained listings from vendors regarding management contact information. Our review indicated the listings had been last updated in August and September 2008.

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

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 include a process in the Remedy Ticket Procedures to ensure sensitive transactions generated from incident tickets are approved by authorized staff.

ADMINISTRATION
Help Desk
End User Computing (EUC)

EXISTING ENVIRONMENT

Department Description of Control: CMS/BCCS is responsible for providing maintenance, support, and security of the Infrastructure and resources established to provide desktop and laptop services. The Enterprise Desktop Policy governs these services.

Tests Performed: Reviewed policy and interviewed staff.

Test Results: The Department developed the Enterprise Desktop/Laptop Policy, effective December 15, 2008, to assist staff with the "proper administration of enterprise desktop/laptop services and assets."

See Security Administration control for additional information.

No significant exception noted.

Department Description of Control: EUC provides personal computer, printer, software, and peripheral support to Consolidated Agencies and CMS Supported Non-Consolidated Agencies. Responsibilities of EUC include handling break-fix incidents as well as service requests for the move, add and change activities associated with the supported personal computer environments.

Tests Performed: Reviewed service request tickets and interviewed staff.

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

The move, add and change requests were handled through the Enterprise Service Request (ESR) process. The ESR process in Remedy was documented in the Change Management module of Remedy.

During our review, we reviewed 25 service request tickets noting they were properly completed and each had a properly authorized ESR.

No significant exception noted.

Department Description of Control: EUC receives break/fix incident assignments, service requests, and change requests via Remedy. The supervisor of the assigned EUC Unit or designee assigns the incident or request to an EUC technician and creates tasks (if required). The technician executes applicable diagnostic and repair or add/move/change actions, updates the Remedy work log, and resolves the Remedy incident, task and/or request.

Tests Performed: Reviewed Remedy 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 were updated.

We reviewed 25 Remedy Help Desk tickets and 25 Remedy Help Desk ticket work logs for completeness, 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 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 18,013 Help Desk tickets, ESRs, and tasks for the period of June 27, 2008 through December 16, 2008.

No significant exception noted.

Department Description of Control: The CMS DESKTOP/LAPTOP PERSONAL COMPUTER STANDARD document was established to record the new IT shared services standard for desktop and laptop personal computers. These standards are implemented as part of the conversion to the new illinois.gov environment.

Tests Performed: Reviewed policy and interviewed staff.

Test Results: The Department developed the CMS Desktop/Laptop Personal Computer Standard, effective May 19, 2008. The purpose of the Standard was to “record the shared services standard for desktop and personal laptop computers.”

EUC, along with sections of the Midrange Group ensured the equipment was configured properly and continuously updated as needed.

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
Help Desk
Telecommunications Service Desk

EXISTING ENVIRONMENT

Department Description of Control: The Telecommunications Service Desk consists of the Telecommunication Help Desk and Telecommunications Provisioning, and is responsible for maintenance (help desk) 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 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: Interviewed staff.

Test Results: The Telecommunications Service Desk was responsible for telecommunication calls during regular business hours. The 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 received. Procedures exist for the Help Desk task.

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

Test Results: The Department developed the Remedy User Guide, dated June 2007 and the Telecomm Service Desk-Remedy 6.3 Work Flow, dated July 31, 2007 to assist help desk staff in the creation of a Remedy ticket. We reviewed the Telecom Service Desk-Remedy Work Flow, noting it did not include a process to ensure sensitive transactions generated from incident tickets, such as those involving security settings, were approved by authorized staff.

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

We reviewed 25 Remedy tickets, noting the tickets were completed appropriately and work logs captured information regarding the problem and resolution.

No significant exception noted; however, the Telecom Service Desk-Remedy Work Flow did not include a process to ensure sensitive transactions generated from incident tickets were approved by authorized staff.

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 telecommunications managers and Quality Assurance staff attend a quarterly meeting with the vendor(s) to review achieved performance levels and other outstanding issues.

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 2008, noting response times were reported based on the severity of tickets.

In addition, the CSC manager and the Quality Assurance staff met with the vendors 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.

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 Provisioning unit is responsible for verifying that 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.

Tests Performed: Reviewed telecommunication change request forms, procedures, website, and interviewed staff.

Test Results: The Department developed the Procedures for Provisioning Tasks to assist TSD staff with provisioning tasks. Additionally, the Department maintained various telecommunication forms and instructions on the Telecom website.

The Department maintained a database of Telecom Coordinators who were authorized to expend funds.

We reviewed 25 telecommunication change requests, noting all had been appropriately completed and were 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 assets, 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. The Provisioning unit utilizes EMS as an inventory, billing, and ordering system. When 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, create the vendor(s) order, and establish billing to the appropriate agency. The Provisioning unit validates paper invoices from the vendors for move, add, and change requests against contract pricing for equipment and associated labor charges if applicable. After validating the charges, the provisioning unit signs the invoice and routes to Business Services for processing payment.

Tests Performed: Reviewed EMS, invoices, 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.

We reviewed EMS noting the information maintained for each asset was dependent on the type of asset.

We reviewed 25 invoices, noting all were appropriately authorized.

No significant exception noted.

Department Description of Control: New voice systems are sent directly to the appropriate site and are tagged by the Consulting and Procurement unit at the time of acceptance. A Property Control Form (PCF) is completed by the provisioning unit for newly tagged voice systems and attached to the original invoice before it is sent to Business Services for processing.

Tests Performed: Interviewed staff.

Test Results: Property Control Forms were completed for new voice systems, attached to invoices, then sent to Business Services for processing.

No significant exception noted.

Department Description of Control: The Consulting and Procurement unit works closely with the agency Telecom 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. Procedures exist for the Consulting and Procurement unit tasks.

Tests Performed: Reviewed procedures, provisioning tickets and interviewed staff.

Test Results: The Consulting and Procurement unit worked with agency coordinators to analyze telecommunication needs.

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

We reviewed 25 provisioning tickets, noting appropriate approvals were maintained and the tickets generally complied with procedures.

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 include a process in the Telecom Service Desk-Remedy Work Flow to ensure sensitive transactions generated from incident tickets are approved by authorized staff.

ADMINISTRATION
Recovery Services

EXISTING ENVIRONMENT

Department Description of Control: The Department provides recovery services for enterprise mainframe environments in order to minimize the risk of disrupted services or loss of resources using vendor contracted services.

Tests Performed: Reviewed recovery service provider contract.

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.

According to the contract, in the event of a disruption, the State would 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 a maximum cost of $4,750,000, with expenditures through April 2009 of $216,324.

No significant exception noted.

Department Description of Control: The following contingency plans and templates provide guidance and reference material to address restoration of various client environments:

- Continuity Methodology
- Recovery Activation Plan.

Tests Performed: Reviewed plans and interviewed staff.

Test Results: The Department developed the following guidance and reference materials for recovery services:

- State of Illinois, DCMS, BCCS Infrastructure Services, Recovery Methodology (revision date - December 11, 2008)
- State of Illinois, DCMS, BCCS, Infrastructure Services, Recovery Activation Plan (revision date - December 31, 2008).

Per Department staff, the Continuity Methodology referenced in the Description of Control is the Recovery Methodology.

The Recovery Methodology and the Recovery Activation Plan provided high-level guidance in the event the Department's computing facilities and services were required to be recovered. The Recovery Methodology and the Recovery Activation Plan made reference to documentation for the recovery of the mainframe environment.

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

The Recovery 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: The Department, as defined in the Continuity Methodology, conducts scheduled annual regional and local mainframe recovery tests that exercise two levels of recovery:

- Comprehensive – enterprise mainframe environment to exercise all qualified critical mainframe applications simultaneously recovered on a remote host.
- Local – exclusive mainframe environments for individual applications recovered independently at a local recovery exercise host system.

Tests Performed: Reviewed plans, exercise documentation, critical application listing, and interviewed staff.

Test Results: The Department conducted regional and local recovery tests as defined in the Recovery Activation Plan, not the Continuity Methodology.

According to the Recovery Activation Plan, "Stage 0, Category One applications/functions recovery plan must be exercised annually."

Additionally, according to the Recovery Activation Plan, documentation of the exercise was to be filed with Recovery Services and maintained in the Statewide Recovery File. The exercise documentation was to include the "outcome results, recommendation for change, problems encountered, lessons learned and cost associated with transportation, off-site retrieval, hotel, per-diem, over time, etc."

The Department conducted testing of its computing facility and services at the recovery service provider's site in September 2008.

Our review of the exercise documentation indicated four out of six agencies, including the Department, with Stage 0, Category One applications participated in the exercise. A comprehensive exercise would include all six agencies and all Stage 0, Category One applications.

The exercise documentation lacked detailed information regarding applications tested and the results of the test. In addition, exercise documentation indicated problems were encountered during testing; however, information regarding the resolution of the problems was not included in the exercise documentation. In addition, the exercise documentation did not document the results, recommendations, lessons learned, cost and off-site retrieval information as required by the Recovery Activation Plan.

Additionally, exercise documentation lacked detail to determine if all qualified mainframe applications were simultaneously recovered as outlined in the Department's Description of Control.

From July through November 2008, five agencies conducted five separate exercises at a local recovery site. However, exercise documentation lacked detailed information regarding applications tested and resolution of problems encountered.

A recovery test was performed in September 2008; 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 Recovery Activation Plan. Local recovery tests were performed; however, exercise documentation lacked detailed information.

Department Description of Control: The Department maintains a Critical Application Database built on information received from State agencies. State agencies are required to categorize, prioritize and define critical information as defined in the Continuity Methodology.

Tests Performed: Reviewed Critical Application Database report, Recovery Methodology, and interviewed staff.

Test Results: The Department maintained a Critical Application Database, which was populated by user agencies.

The Recovery Methodology stated "recovery priority values are comprised of a sequence of ranking based on resource type, human service impact and agency mission relevance." However, per review of the Critical Application Database, we noted ranking based on resource type was not indicated.

The Critical Application Database was maintained; however, it did not provide for resource type rankings.

Department Description of Control: The Department maintains scripts and/or procedures for the recovery of mainframe operating system and subsystem platforms. Recovery Services staff assist in updating and rehearsing these procedures during the comprehensive and local recovery exercises.

Tests Performed: Reviewed Recovery Activation Plan and interviewed staff.

Test Results: As part of the Recovery Activation Plan, the Department developed the Recovery Exercise Script to assist in the recovery of the mainframe operating system.

According to Recovery Services 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.

No significant exception noted; however, Recovery Services staff did not assist in updating and rehearsing procedures for recovery exercises.

Department Description of Control: The Department utilizes an off-site storage facility for the storage of data tape backups and recovery information (Hotbox).

Tests Performed: Reviewed off-site storage facility and interviewed staff.

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

No significant exception noted.

Department Description of Control: The Department stores critical recovery information that is defined in the Continuity Methodology. The Hotbox provides hardcopy recovery data to be used in the event of an outage. The Hotbox is maintained at the off-site storage facility and is updated on a yearly basis.

Tests Performed: Reviewed Recovery Activation Plan, Hotbox, and interviewed staff.

Test Results: The Recovery Activation Plan documented the critical information which was to be maintained in the Hotbox at the regional off-site storage facility. We reviewed the contents of the Hotbox noting several items, which were expected to be located in the box, were not, and some items were outdated.

In addition, we noted the contents of the Hotbox were last reviewed by the Department on February 11, 2009.

Although the Hotbox was maintained at the regional off-site storage facility, critical information to assist in recovery efforts was missing or outdated.

OVERALL CONCLUSION

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

- The Hotbox is routinely reviewed to ensure it contains current versions of all critical documents. Since the Hotbox is an essential component of recovery efforts, it is imperative it contains comprehensive and current information.
- The Recovery Methodology and Recovery Activation Plan are updated to reflect the current recovery environment.
- Documents referenced in the Recovery Methodology and Recovery Activation Plan are fully developed and current.
- All agencies with Stage 0, Category One applications participate in the recovery exercises.

- The capability to simultaneously recover all qualified mainframe applications is tested and documented in recovery exercises.
- Documentation supporting recovery exercises contains detailed information regarding test objectives, problems, resolutions, results, and all other requirements outlined in the Recovery Activation Plan.

In addition, the Department should ensure the Description of Controls is an accurate description of the current recovery services environment.

From a broad overview perspective, 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.
- Conduct comprehensive tests of the plans on an annual basis.

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 and interviewed staff.

Test Results: We reviewed the FY08 annual report, noting 105 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

Background Provided by the Department: The Workforce, Development and Logistics unit coordinates and facilitates internal personnel paperwork, workforce training, development and implementation, and workforce logistics for the Bureau.

Department Description of Control: For HR related transactions the unit refers 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 and any policies or procedures initiated and enforced by Shared Services.

Tests Performed: Interviewed staff.

Test Results: The Unit utilized policies/procedures established by other entities, such as the Bureau of Personnel, the Department, the Governor, or Legislature.

The Unit did not establish its own policies/procedures.

Per Department management, the Shared Services division at the Department of Revenue had not been established yet; thus, policies and procedures had not been developed.

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 training memorandum, training forms, and interviewed staff.

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

We reviewed 10 training request forms and found general compliance with the process; however, we did identify minor issues on 5 out of 10 forms.

No significant exception noted.

To support our evaluation and testing of this control objective we performed the following additional tests.

Tests Performed: Reviewed organization chart and interviewed staff.

Test Results: Per Department management, as of January 9, 2009, the Bureau had 82 staffing vacancies.

During the course of our review, we identified several areas (Infrastructure Services, Enterprise Applications and Architecture, LAN Application Development, and Systems Software) that had potential staffing issues due to vacancies and/or loss of institutional or technical knowledge.

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 perform an assessment of current staffing levels (including the availability of staff to fill voids due to the loss of institutional or technical knowledge) to ensure it can effectively support its operations.

ADMINISTRATION
Vendor Management

EXISTING ENVIRONMENT

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

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

Tests Performed: Reviewed repository and interviewed staff.

Test Results: The repository 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 repository were utilized to assist in renewing contracts and services for the next fiscal year.

No significant exception noted.

Department Description of Control: Documented procedures for reconciling desktop, mainframe and midrange software are outlined in the AIM/Vendor Management Guide. 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.

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

Test Results: The Department maintained the AIM/Vendor Management Guide (Guide), with each section of the Guide dated separately. The Guide provided step-by-step instructions for issues concerning Service-Information Request Management, Contract Management, Contract Administration, Database Management, Procurement Management, Maintenance Renewals, Software Maintenance, Invoice Processing, and Software License Compliance.

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

Our review of the Guide 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.

Although software inventory problems were identified in prior year reviews and audits, the Department had not conducted a reconciliation of software, identifying the actual number of licenses in use versus the number of licenses purchased from each vendor. In addition, we noted the software inventory list did not accurately record all software.

We also found the controls over physical access to the software library lacking.

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

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 inventory list properly records all software and its location.
- Ensure all software is properly secured and maintained in the software library.

ADMINISTRATION
Warehouse and Inventory

EXISTING ENVIRONMENT

Background provided by the Department: The BCCS warehouse is responsible for the receipt, inventory, storage, security and limited distribution of EDP type equipment for CMS.

Department Description of Control: The CMS Property Control Procedures are used as a baseline for managing equipment that is stored at the BCCS warehouse and managed in the CMS inventory.

Tests Performed: Reviewed the CMS Property Control Procedure and interviewed staff.

Test Results: The Department developed the CMS Property Control Procedures, not dated, to assist in maintaining inventory.

The purpose of the CMS Property Control Procedures (Procedures) was to create a uniform set of standards for identification, maintenance, and disposition of equipment for the Department. The Procedures applied to all equipment acquired by the Department in accordance with the Property Control Rules.

The Procedures outlined the responsibilities of the Director, Bureau Managers, the Property Control Officer, Property Control Coordinators, Bureau Fiscal Staff, and employees.

The Property Control Officer was responsible for maintaining the property control system including:

- Inventory and assignment of property control tags.
- Annual inventory certification.
- Timely preparation and distribution of all required and requested reports.
- Maintenance of all property control records in the Common Systems Inventory.
- Physical inventory of equipment.

The Procedures stated the Department utilized three inventory systems for maintaining and tracking inventory; Common Systems Inventory (CIS), Management of Network Income, Expense, and Services (MONIES), and Vehicles Database System. However, according to Warehouse Inventory staff, EMS11 (data and voice provisioning) and Remedy (PC-Lease program) were also used to maintain and track inventory.

No significant exception noted; however, the Procedures did not reflect the current process and addressed the use of EMS11 and Remedy in maintaining and tracking inventory.

Department Description of Control: The BCCS inventory is broken down into three basic categories: EDP, Data and Voice related equipment. The inventory databases that manage these inventories include Monies Co 4, EMS11, Remedy and CIS.

Tests Performed: Interviewed staff.

Test Results: The BCCS inventory was classified the following categories:

- EDP – EDP assets included: PCs, laptops, printers, servers, mainframe, storage, and miscellaneous personal computing equipment.
- Data – Data assets included routers, switches, modems, nodal systems, and other miscellaneous network or data communications equipment.
- Voice Related Equipment – Voice Related assets included all telephones and telephone systems.

In addition, the following databases were utilized for inventory purposes:

Monies Co 4 – Monies Co 4 was used as an order module to manage and track Department owned EDP equipment.

EMS 11 – EMS 11 was an updated, web based version of Monies that was used to support voice and data order processing, management, inventory, billing and engineering activities for the Department.

Remedy – Remedy was used to track leased assets (personal computing equipment and laptops) for the Department and consolidated Agencies.

CIS – CIS was the inventory system of record for the Department and was used to track all tagged assets.

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 Department's controls, the Department should update the CMS Property Control Procedures to reflect the current process to maintain and track inventory.

ADMINISTRATION
Service Reporting

EXISTING ENVIRONMENT

Background Provided by the Department: The current purpose and goal of Service Reporting is to lend insight, visibility and a basis for improvement of services.

Department Description of Control: Monthly and quarterly reporting currently includes Incidents, Service Requests, help desk calls, Mainframe, Email, WAN, and SSRF Invoicing. The Bureau prepares monthly and quarterly activity reports for each consolidated agency demonstrating volume, workload, and select cycle times allowing for interpretation of trends.

Tests Performed: Reviewed reports and interviewed staff.

Test Results: Service level reports were provided to consolidated agencies to furnish information on services. The monthly and quarterly reports included information on Incidents, Service Requests, Help Desk Calls, Mainframe, Email, WAN, SSRF Invoicing, volume, workload, and select cycle times.

We reviewed monthly reports for the consolidated agencies from July to November 2008, noting no exceptions.

We reviewed the quarterly report for the period of July 1 to September 30, 2009, noting no exceptions.

No significant exception noted.

Department Description of Control: Incidents and service request reports represent data from the Remedy help desk system. During FY08, this reporting began with data extracts from Remedy, imported to Excel spreadsheets for processing to produce tables moved to Word documents. During FY08, training was gained and reporting migrated to Crystal Reports running a month of parallel reporting from the former Excel spreadsheets and Crystal Reports to ensure continuity. The monthly and quarterly Crystal Reports are configured to retain the "snap-shot" queried data as the Remedy system is a live and changing system subject to changes in criteria as tasks are worked and resolved. Review is performed at the time of processing, during document assembly and executive final review. Both verbal and electronic questions are addressed concerning any data issues observed during document assembly review, executive review or review by the shared service agencies. The SQL used is documented.

Tests Performed: Reviewed reports and interviewed staff.

Test Results: During the transition to Crystal Reporting at the end of fiscal year 2008, the Department conducted parallel reporting with the old processes to ensure the accuracy of the new reporting process. The executive final review was completed by Bureau management.

SQL documentation was maintained and was provided to user agencies by request.

No significant exception noted.

Department Description of Control: Calls received are reports generated by the Avaya phone system and forward for reporting. The Avaya reports are imported to an Access database. Reports are generated using Crystal Reports. Data review takes place during data import to Access.

Mainframe data is provided for processing as an extract from Tivoli Decision Support and Workload Manager. The extracts include spreadsheet data and work logs. The data goes through procedures requiring manual import, examination and interpretation to establish the final output. Mainframe reporting is undergoing revision targeted for October reporting in November, moving to a direct import to Access and generating reports via Crystal Reports.

E-mail represents a pass-through report from Ironmail perimeter filtering. This reporting is generated from the Ironmail system by the PIM unit.

WAN reporting is provided from manual compilation of data from outage notices and router and switch logs. The spreadsheet compilation is then forwarded by the network group for processing. The WAN data is updated to an Excel spreadsheet where the initial report spreadsheet is created and then moved to a Word table. The table is checked during processing for continuity but crosscheck verifications are not possible.

Invoice reporting is an extract provided from the PACES system used for the agency SSRF billing. The extract provided is imported to an Access database, generating reports using Crystal Reports. The reported totals are cross-checked against actual shared service agency invoicing totals. Reports are posted to a SharePoint site available to agency CIO's and their designee.

Tests Performed: Reviewed reports and interviewed staff.

Test Results: We reviewed the reporting processes for invoice reporting, WAN reporting, e-mail, mainframe, and calls, 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.

ADMINISTRATION
Agency Communications

EXISTING ENVIRONMENT

Department Description of Control: The Department 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 were replaced as of 8/26/2008 by the new BCCS Service Site, cms.partner.illinois.gov/bccs/service/default.aspx, which allows agency CIOs to access their agency specific information from BCCS on a self-service basis.

Tests Performed: Interviewed staff and reviewed the website.

Test Results: The Department utilized the BCCS Service Site, the Bureau website - www.bccs.illinois.gov, and the BCCS Pulse newsletter to communicate to user agencies.

The Department's service catalog, contact information, forms and guides for requesting services, and announcements/bulletins were available on the website.

No significant exception noted.

Department Description of Control: Ad-hoc meeting requests are honored by the AR team. Periodically, the Bureau hosts topic specific meetings/forums with various customer interest groups. The customer-focused newsletter, the BCCS Pulse, provides 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. Note: As of 9/1/2008, the Agency Relations team reports to a new manager.

Tests Performed: Reviewed newsletters and interviewed staff.

Test Results: Meetings/forums with various interest groups were held during the audit period.

The BCCS Pulse Newsletter was distributed via e-mail and was also available on the Bureau website.

We reviewed the September 2008 and January 2009 newsletters, noting the newsletters contained information on:

- Green computing
- Enterprise Program Management
- IT Rationalization
- New Services
- Alternate Data Center
- Electronic Pay Stub System

- Email Archive Solution
- ICN Regional Meeting
- Cyber Security Awareness

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 (ESB) 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: The ESB Guide helps 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, and ADRDSSU Restore. 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: Reviewed procedures and interviewed staff.

Test Results: The Department had an ESB Guide (Guide) located on the Department's SharePoint site, which contained procedures followed by the ESB technicians responsible for storage and backup. The Guide contained procedures utilized by ESB technicians to help ensure z/OS cleanup, restores, and DASD additions and deletions were completed successfully. Among the procedures included within the Guide were: the Daily/Weekly Cleanups, DASD Addition Checklist, DASD Removal Checklist, DASD Return to Spare, DASD additions, Daily RMF, Weekly RFM, RMF Special, and ADRDSSU.

ESB technicians managed both SMS Pools and Private Pools for the Department's mainframe systems.

Department staff stated SMS was used to manage Public (shared) and Private (agency-dedicated) Pools. System Automation monitored threshold limits and notified ESB technicians via automated email message when SMS (shared) storage fell below pre-determined threshold limits.

Department staff stated ESB technicians were responsible for migrating data, deleting disk packs, and adding additional disk space when required.

No significant exception noted.

Department Description of Control: z/OS Backups are performed on the mainframe operating system data. System data is backed up daily and weekly with the weekly copies sent to the regional vault. Backups of non-operating system files 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 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 would be kept.

Department staff stated user agencies were responsible for assuring their data was backed up. ESB technicians were only responsible for backing up user agency data residing on SMS. Backups were performed by HSM (Hierarchal Storage Management). These backups were controlled by SMS routines and were set by the customer at allocations time. When the customer allocated a new file, a management class was assigned which determined how long the data would be kept.

No significant exception noted.

Department Description of Control: z/OS Restores are performed upon receipt of a Remedy ticket. 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: ESB technicians were responsible for performing restores on z/OS, which were documented in Remedy. Department staff stated requests coming from user-agencies go through the Helpdesk, which entered the request ticket into Remedy. Also, Department staff stated ESB technicians restored data, updated the Remedy work log, and closed the record.

At the time of our review, Department staff stated there had been only one restore performed within the past three months. We obtained and reviewed the Remedy work log ticket for the restore and noted the Remedy ticket was completed within a reasonable timeframe.

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
Enterprise Production Operations Services
Systems Operation Center

EXISTING ENVIRONMENT

Department Description of Control: The Systems Operation 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 Systems Operation Center operates 24 hours a day, 7 days a week, 365 days a year.

Tests Performed: Interviewed staff.

Test Results: The Systems Operation Center monitored the operation of the Bureau’s computing resources and operated 24 hours a day, 7 days a week, 365 days a year. Staff monitored the operation of the Bureau's computing resources to ensure availability, performance, and response necessary to sustain customer business demands. During our review, we noted the System Operation Center averaged 200 hours of overtime per month.

No significant exception noted.

Department Description of Control: The Systems Operations Center utilizes the Remedy Change Management System to coordinate and oversee implementation of changes to the computing environment. Remedy is used to record and monitor incident resolution.

Tests Performed: Reviewed the Remedy tracking system and interviewed staff.

Test Results: The Remedy Help Desk module was utilized to record and monitor incident resolution. The Remedy Change Management module was utilized to record changes to the system.

We reviewed 25 problem tickets and noted all had been entered in the Remedy Help Desk Module.

No significant exception noted.

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

Tests Performed: Reviewed Data Processing Guide (Guide).

Test Results: The Guide maintained information for commands, problems, troubleshooting, changes, and a description on how to take the mainframe systems down and bring them back up.

In reviewing the Guide, we noted the Guide appeared to document in detail, specific information on commands to monitor and operate the computing resources to ensure availability and performance of the systems. The Guide was routinely updated during the audit period.

No significant exception noted.

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

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

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

The Guide contained a section on Focal Point Operations Procedures, which provided guidance on responding to Focal Point messages. The Focal Point Application supported various functional areas.

No significant exception noted.

Department Description of Control: The Systems Operation Center provides input to the Daily Shift Report which is then distributed via an automated mechanism in the Focal application. The Daily Shift Report is used to document outages/issues.

Tests Performed: Reviewed Daily Shift Reports 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 Daily Shift Reports for November 10 to 16, 2008, noting 25 problems identified in the reports had a corresponding Remedy ticket.

No significant exception noted.

Department Description of Control: Shift Change Checklists are utilized by the Systems Operation Center to ensure consistent verification of system availability. SYSLOG is utilized as a tool to reference system activity.

Tests Performed: Reviewed Shift Change Checklists and interviewed staff.

Test Results: 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 Shift Change Checklists for November 10 to November 16, 2008, noting all had supervisory review and appeared to be appropriately completed.

The SYSLOG recorded all messages written to, and all commands entered into the system console. The main use of the system generated log 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 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 formally review staffing levels in the System Operations 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 for job acceptance are documented in each agency's standards manual if they exist; for DHS, DOT, and HFS these are located at the Agency Intranet.

Tests Performed: Reviewed Intranet and interviewed staff.

Test Results: Production Control monitored processing activities for the Department and the following agencies: DHS, HFS, REV, DCEO, DOT, DPH, and EPA.

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

Standards manuals existed on the respective agency intranet site for DHS, IDOT and HFS.

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

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

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

Tests Performed: Reviewed Proc documentation and interviewed staff.

Test Results: Production Control was responsible for the Proc Acceptance for CMS, DHS, DOT, DPH and EPA.

Production Control also maintained Proc Acceptance documentation for DHS, DOT and HFS. We reviewed the documentation, noting the documentation appeared to maintain sufficient information to ensure compliance with standards. The documentation outlined production standards, naming conventions, and run procedures.

No significant exception noted.

Department Description of Control: Job setup and processing - All jobs that are processed in the production environment for CMS, DHS, DCEO, DOT, 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: CMS, DHS, DCEO, DOT, DPH and EPA 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.

Department Description of Control: Abend Resolution - When a CMS, DHS, HFS, REV, DCEO, DOT, DPH, or EPA job abnormally terminates due to a cart problem or a problem with how the job was setup for processing and if problem can not be resolved by I/O Controls staff the production control staff are called upon to correct the problem and restart the job . When it is a problem with the job itself, the agency 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 (shift reports) is provided daily to all Production Control, I/O, and Library Services staff, as well as to each legacy agency being monitored.

Tests Performed: Interviewed staff and reviewed daily shift reports.

Test Results: CMS, DHS, HFS, REV, DCEO, DOT, DPH, or EPA generally had the procedures to fix abends 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 was recorded in the daily shift reports, which contained information on agency contacts, when the job was corrected, and the cause of the abend.

During our review, we noted the daily shift reports for December 2008 appeared to be properly completed and were provided to Production Control, I/O, and Library Services staff, as well as to each legacy agency being monitored, except DCEO.

No significant exception noted.

Department Description of Control: 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.

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. 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

Background provided by the Department: 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), Transportation (DOT), the Department of Revenue (REV) and the Environmental Protection Agency (EPA). Collectively, these can be referred to as I/O Managed agencies.

With the exception of REV, the processing for the I/O managed agencies is handled by staff at the Harris Building (100 South Grand Avenue East) and the processing for REV is conducted at the Willard Ice Building (101 West Jefferson).

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. 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: Interviewed staff.

Test Results: 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. However, staff had been (and continued to be) cross trained in the legacy processes.

For production jobs that did not complete successfully (abends), the information to correct the abend was the responsibility of the I/O Managed agencies (CMS, DHS, HFS, DPH, DOT, REV, and EPA). I/O Control staff reviewed the abends and determined if there was enough information in the abend documentation to correct the problem. If the problem could not be corrected, Production Control staff contacted the associated agency to help resolve the problem. A Job Call List was maintained to provide agency contact information. Abends were tracked in the daily shift reports.

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. 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 IO Managed agency except DCEO.

Tests Performed: Reviewed daily shift reports and interviewed staff.

Test Results: I/O instructions were imbedded 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. Hardcopy flows were maintained for two years.

During our review, we noted the daily shift reports appeared to be complete and were emailed to each IO Managed agency, except DCEO.

No significant exception noted.

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 and for the Department of Commerce and Economic Opportunity (DCEO), Department of Agriculture (AGR), and other agencies utilizing the standard CMS printing services. 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 via the DHS Warehouse Control System (WCS). DCEO and DOT statistics are now included in the monthly reports, but it will be the last quarter of 2008 before EPA and DPH statistics are included in the reporting.

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

Test Results: 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.

The Output section was responsible for printing and distribution of all documents and reports generated as a result of processing jobs for I/O managed agencies, DCEO, AGR, and other agencies utilizing the standard CMS printing services.

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 were posted by the printers and maintained by Department staff.

The printer meter readings were for the DHS, CMS and HFS printers. During our review, we noted the December 2008 monthly job performance report appeared appropriate. We noted the monthly job performance reports documented downtime, printer status, and performance information.

Inventory was monitored and orders were created via the DHS Warehouse Control System.

No significant exception noted.

Department Description of Control: With the exception of the printing performed for REV at the Willard Ice Building, physical control over the distribution of printed material for the remaining I/O Managed Agencies (done at the Harris Building 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 memorandums and reviewed the Focal system.

Test Results: The Department distributed memorandums to the I/O Managed agencies, dated from November 2006 to November 2008, documenting the relocation of the print shop and new security controls in place for picking up the reports.

The Focal system documented the listing of individuals who were authorized to pick up reports. We reviewed 25 individuals who signed for reports to ensure the individuals were appropriately authorized, noting no exceptions.

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

OPERATIONS
Enterprise Production Operations Services
Library Services

EXISTING ENVIRONMENT

Background Provided by the Department: Library Services consists of four functional units: CCF Tape Library, CCF Tape Media, Library Support, and Tape Administration.

CCF Tape Library

Department Description of Control: The Tape Library 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. The Tape Library is responsible for all tape orders, initializing, labeling, degaussing, and destruction of media, as well as movement of media resources.

Tests Performed: Reviewed ISD Media Guide, ISD Library Guide, 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.

Tape Library provided 24X5 services with three shifts. The first and third shifts were appropriately staffed; however, the second shift was not staffed. During our review, we noted the Tape Library averaged 50 hours of overtime per month.

No significant exception noted.

Department Description of Control: The Tape Library utilizes the ISD Library Guide and the ISD Media Guide to ensure that duties are performed in a consistent manner. All media is identified with unique tracking alpha numeric identification numbers (volume serial number).

Tests Performed: Reviewed the ISD Tape Library Guide and the Media Check-In/Media Check-Out Transmittal Forms.

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.

The Guide identified the following as the process for media transmittals, including the transportation of media to and from the secured off site vault.

Agencies were responsible for sending a request, which required a Media Transmittal Form or a broadcast via e-mail to the Media library staff, listing the tape media volumes they wish to have moved from the vault to the CCF library or vice versa.

When the tape librarian received a Media Transmittal Form, with less than five VOLSER(s), the VOLSER was manually written on the Computer Tape Log. When the media transmittal form contained more than five VOLSER(s), a copy was made and attached to the Tape Log. Information from the Media Transmittal Form(s), Computer Tape Logs with attachments and Broadcasts were utilized to update TMS after the transaction was completed.

We reviewed 25 Media Check-In/Media Check-Out Transmittal Forms for February 3, 2009, to ensure the forms were correctly completed, noting all were properly completed and the transmittal forms reviewed were approved by authorized staff.

No significant exception noted.

Department Description of Control: 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 procedures and tapes.

Test Results: TMS was a database which tracked tapes by VOLSER that had been registered to it, with information regarding the VOLSER, and utilized by the tape librarians to track and record the location of tapes/cartridges. Tape librarians continually maintained and updated TMS in order for a customer to know the proper location and status of their tapes.

The transient tape tracking began when the customer checking in transient tapes into the library used the Media Check-In Transmittal Form. The transient tape was logged into the library by adding them to the Transient Tape System (TTS) with the agency code name, VOLSER, and a date that was two weeks following the date the tape was received. When the two-week date occurred, then the tapes were sent back to the agency (unless the agency specifies the tape should be retained longer).

We reviewed 163 tapes, noting all were identified with unique tracking alpha numeric identification numbers.

No significant exception noted.

CCF Tape Media

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 ISD Media Guide 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 Media Guide, dated by section, which provided staff guidance with job duties. Specifically, the ISD Media Guide provided detailed information on the following processes:

- Monitoring tapes through the tape management system,
- Cleaning cartridges,
- Error reports,
- Cartridge pull and review,
- Tape manual mounts/dismounts, and
- Service requests.

Tape Media provided 24X7 services with three shifts. The third shift was not staffed. The second shift had one individual and the first shift was appropriately staffed. During our review, we noted the Tape Media unit averaged 380 hours of overtime per month.

No significant exception noted.

Library Support

Department Description of Control: Library Support staff are responsible for migrating test environments to DHS, HFS, DOT, and EBAS 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 move to production forms and interviewed staff.

Test Results: The Department was responsible for select mainframe production libraries of 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.

During our review we found the production libraries were protected by security software; however, the ability to update or edit was not limited to Library Support. Specifically, we found that DOT still maintained security access to production libraries and was completing move to productions for some production libraries.

However, we did test moves to productions that were performed by Library Support for specific production libraries to ensure appropriate approvals and authorizations were provided prior to the move of the changes into production. We tested 55 moves to production and found that all 55 had the appropriate approvals and authorizations.

Library Support staff stated they were only responsible for backups of the four agencies production libraries.

No significant exception noted; however, standardized policies and procedures had not been developed to control moves to production and access to production libraries was not limited to Library Support.

Tape Administration

Department Description of Control: For 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 modification 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 and manually produced reports and interviewed staff.

Test Results: The TGS and manually produced reports were used to document tape activities for the Department, DHS, HFS, and DOT.

The TGS and the manually produced reports pulled data from the Tape Management System. These reports were utilized to guide staff in agency requests in managing tapes or to handle any problems or issues that may arise.

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

The Department and DOT used manually produced reports to review tape activities.

We reviewed the TGS and the manually produced reports for February 18, 2009, noting reports contained dates, report name, and appropriate detailed information regarding agency tapes.

In addition, Tape Administration staff managed technical duties and implemented tape control features, project tape media, etc. at the request of user agencies.

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:

- Formally review staffing levels to determine if the use of overtime is more beneficial than hiring additional staff.
- Develop standardized Library Support policies and procedures for use by all consolidated agencies.
- Ensure access to production libraries is appropriately restricted and conforms to policies and procedures.

CHANGE CONTROL

EXISTING ENVIRONMENT

Department Description of Control: The Department's Change Management Unit is responsible for managing changes to the Department's environment (except for applications under EBAS control) that are initiated as the result of an ESR (Enterprise Service Request), a configuration change, or an internal work assignment.

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

Test Results: According to the Change Management Policy (Policy), "infrastructure changes for all technology platforms and systems of the CMS/BCCS management infrastructure and environment" were to follow the Policy and all "corresponding Change Management processes and/or procedures."

Although the Change Management Unit was responsible for the majority of the primary functions covered by this review; several other related functions, such as LAN services, DOT, DHS and DHFS mainframe, and networks for non-state agencies followed different processes for change management.

Although an established procedure existed, several additional functions related to the Department's primary services did not follow the established change management policies and procedures.

Department Description of Control: The Remedy Change Control System is used to create, review, approve and track change requests to Department systems. The Change Management Policy is used to govern these activities. The Remedy Change Guide is a procedural document which supports the Change Management Policy.

Tests Performed: Reviewed Change Management Policy, Remedy Change Management Guide, CMS/ICN WAN Change Management process, Remedy Change Control System, change tickets, and interviewed staff.

Test Results: The Department utilized the Remedy Change Control System to track changes in the Department's infrastructure.

The Department had developed the Change Management Policy (Policy), effective December 15, 2008 and the Remedy Change Management Guide (Guide), effective December 8, 2008. The Policy and Guide provided staff guidance on documenting changes and entering changes into the Remedy System.

The purpose of the Guide was to "standardize the actions, behavior and responsibilities related to the processing of change requests for utilizing the Remedy Change Management System."

The Guide was divided into nine steps, which identified "specific instructions/requirements." Our review of the Guide indicated deliverables and affected resources were to be identified, along with the quantifying the impact of the change. However, the Guide did not outline the requirements to achieve these objectives.

We reviewed a sample of change tickets for compliance with the Guide, noting:

- 25 of 25 change tickets complied with the general requirements of the Guide.
- Nine of ten high impact change tickets had the required back out plans, implementation plans, and test plans.

No significant exception noted; however, one high impact change ticket did not meet all requirements.

Department Description of Control: Change requests are visually reviewed for content and completeness by the Change Management Unit. A Change Advisory Committee (CAC) has been established which meets as needed to review submitted changes. While the Change Management Unit reviews all changes, this committee is responsible for reviewing the changes submitted as either a "medium" or "high" priority. Changes to be reviewed are made available to members of the CAC before the meeting, and the results of the meeting are made available after the meeting as meeting minutes.

Tests Performed: Reviewed Change Management Policy, Remedy Change Management Guide, CAC meeting minutes, change tickets, and interviewed staff.

Test Results: According to the Change Management Unit's Manager, changes were reviewed for content and completeness by the Change Management Unit by using the "Validate Change Variables-Technical/Business" process in the Guide.

Our review of the Guide indicated the Shared Service Manager was to perform the technical review and the Change Management Unit was to perform the business review.

The Department had established a SharePoint site which contained information for upcoming CAC meeting and meeting minutes for CAC members to review.

We reviewed meeting minutes from eight meetings, noting they indicated the change ticket number, status, impact, discussion notes, and CAC approval.

We also reviewed 25 changes to determine if the appropriate approval was obtained, based on the "Impact Classification Criteria for Request for Change" outlined in the Guide, noting no exceptions. Additionally, we reviewed 25 changes to ensure they were indicated in the CAC meeting minutes or documented in the work log as defined by the Guide, noting 24 were indicated.

No significant exception noted; however, one change was not included in the CAC meeting minutes.

Department Description of Control: If a major incident or problem is directly related to an implemented change, A Post Implementation Review (PIR) is completed. This information is then attached to the change request for documentation purposes. A spreadsheet is maintained by the Change Management Unit which tracks these PIRs.

Tests Performed: Reviewed Change Management Policy, Remedy Change Management Guide, PIR spreadsheet, change tickets, and interviewed staff.

Test Results: The Policy defined a Post Implementation Review (PIR) as a "standard method to follow up with the change owner and/or customer on the results of the change request." However, the Guide stated a PIR was required to be performed on emergency changes and "scheduled changes that cause a major outage."

According to the Guide, for non-emergency changes an incident form was to be completed and for emergency changes resolution information was to be documented. The incident report was to be attached to the change ticket and the resolution information was to be documented in the work log. However, the Guide did not indicate the specific information which was to be recorded in the incident form or the resolution information. In addition, the Guide did not document communication with the owner or users.

We reviewed eight changes which required resolution information, noting the information was contained in the help desk ticket or change ticket. In addition, we reviewed five major outage change tickets, noting four did not have the required incident report.

Additionally, we noted the eight changes and five major outage changes were included on the PIR spreadsheet.

Although PIRs were conducted, the depth of documentation and communication was lacking. In addition, documentation was not always attached to the change request, but the help desk ticket.

Although a formal process to review major incident or problem directly related to an implemented change existed, it was not always followed and did not apply to all major changes.

OVERALL CONCLUSION

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

- Ensure policies, procedures and guides provide clear and consistent controls over the change process.
- Ensure all changes to the Department's environment follow the Change Management Policy and are tracked in the Remedy Change Management System.

- Ensure all changes are adequately documented. Specifically, the Department should:
    - Ensure the PIR process is always followed.
    - Ensure all requirements are met on all high impact change tickets.
    - Ensure all appropriate changes are discussed at CAC meetings and documented in minutes.

QUALITY ASSURANCE

EXISTING ENVIRONMENT

Department Description of Control: The Infrastructure Quality Assurance and Methods group act as facilitators for organizing, planning and controlling work activities for the Infrastructure Services Division related to Agency IT projects. Process and procedures that govern this process are located in the IQAM Guide.

Tests Performed: Reviewed IQAM Procedure (Procedure), project list, and interviewed staff.

Test Results: The Department developed the Infrastructure Quality Assurance and Methods (IQAM) Charter Review Procedure, issued October 31, 2008.

IQAM staff utilized these procedures to facilitate agency IT projects. After IQAM received notification of a new project, a meeting with the user agency was scheduled. Meeting minutes and project documentation were maintained on IQAM's Sharepoint site.

We reviewed the project list and noted that none of the projects completed during the audit period were required to follow the current Procedure.

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.

SECURITY ADMINISTRATION

EXISTING ENVIRONMENT

Background Provided by the Department: The Department's security posture is comprised of compliance and auditing functions that include corrective action tracking, security assessments, security awareness promotion, security strategy development, security authorization list review, and policy development.

Department Description of Control Corrective action tracking is achieved through collection of recommended improvements from sources such as audit recommendations and internally conducted vulnerability assessments. These recommended improvements are entered into a database. Reports generated from this database are discussed at BCCS Leadership meetings. Each appropriate BCCS Leadership member is responsible for developing detailed actions that address recommendations and for entering any updates into the database. The implementation of the corrective action is the responsibility of the appropriate area.

Tests Performed: Reviewed correction action tracking reports, BCCS Leadership meeting agendas, and interviewed staff.

Test Results: The Department developed a database to track corrective actions to be taken as a result of audit recommendations and internal vulnerability assessments.

BCCS Leadership members were responsible for the development and entry of detailed actions which addressed recommendations. Additionally, each applicable Unit's manager was responsible for ensuring completion of corrective actions by the stated due date.

The corrective action database was discussed at BCCS Leadership meetings.

We reviewed the database and found vulnerability assessment recommendations were not included in the database. We also noted corrective action plans were not included for all recommendations. Additionally, we reviewed an "overdue" report from the corrective action database, noting 23 action items had missed their completion date.

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

Department Description of Control: Security assessments are conducted by the Department's Technical Safeguards unit. Results of those assessments are made available to appropriate BCCS staff that has responsibility for remediation. The Technical Safeguard Unit Security Audit Procedures Rules of Engagement, located on a secure, shared network drive, outlines typical actions that Technical Safeguards staff follow when conducting assessments. Cyber security incident responses are also addressed by the team. Procedures for responding to these incidents exist.

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

Test Results: During our review, the Department updated the Security Audit Procedures Rules of Engagement (March 10, 2009) and the Critical Incident Response Procedures (March 12, 2009).

The Technical Safeguards Unit conducted 25 security assessments that included discovery enumeration, vulnerability assessments, and website assessments. Upon completion of the assessments, the Technical Safeguards Unit made available to the appropriate staff the assessment results.

During calendar year 2008, the Technical Safeguards Unit conducted assessments of the 12 "consolidated" agencies. Our review of the 2008 year end report, indicated 20,961 issues had been identified; however, only 11,257 (53%) had been addressed.

Although a framework for the conduct of security assessment existed, all identified issues had not been addressed in a timely manner.

By not addressing issues which had been determined to be high risk, the Department increased the risk of security exposures impacting the disclosure, integrity, and availability of information.

Department Description of Control: Security awareness is promoted by placing relevant information on an enterprise accessible web site (http://bccs.illinois.gov) where security related news releases, tips, posters, and guidelines can be viewed by Department staff.

Tests Performed: Reviewed web site, memorandums, policy acknowledgement forms, and interviewed staff.

Test Results: The Department developed a website where security related news releases, tips, posters and guidelines could be viewed by Department staff and user agencies.

Our review of the website indicated it provided high-level and general security information.

In addition, on February 20, 2009, the Department's Director issued a memo to all Department employees announcing all employees would be required to complete security awareness training annually. During our review, the Internet training program was still in development.

In January 2009, all Department employees were required to complete an "employee acknowledgement of policies" statement, stating they had read and would abide by the policies. We selected 31 employees to determine if they had completed the employee acknowledgement of policies statement, noting three had not.

A framework to promote security awareness had been created; however, documentation to support individual employee acknowledgement of policies was not always available.

Department Description of Control: Security authorization list are continuously updated and reviewed every six months with the agencies. Process and procedures documentation guide these activities. The areas reviewed include; RACF coordinators, media pickup, IMS/DB2, CICS regions, Mobius, Web Services, and IDMS.

Tests Performed: Reviewed memorandums, agency updates, procedures, and interviewed staff.

Test Results: The Department developed several procedures for the maintenance of the security authorization listings.

Twice a year the Department staff request agencies to update the RACF coordinators, media pickup, IMS/DB2, CICS regions, Mobius, Web Services, and IDMS security authorization listings. The Department requested agencies to update the authorization listings in May 2008 and January 2009 and used a spreadsheet to track responses.

No significant exception noted.

Department Description of Control: RACF violations for BCCS staff are reviewed every two weeks. Violation reports are provided to the individual responsible, requesting an explanation of the violation. These explanations are then reviewed for reasonableness. Procedures exist for this process.

Tests Performed: Reviewed violation reports, procedures, and interviewed staff.

Test Results: The Department had a procedure in place for the monitoring of security violations.

Department staff reviewed violation reports twice a month and distributed noteworthy violation summaries to staff for explanation.

We reviewed the violation reports for August and September 2008, noting they appeared to have been reviewed and submitted to staff for explanation.

No significant exception noted.

Department Description of Control: Information collected from all the activities described above is used as the foundation to develop and maintain the Department's long-term security strategy – *Secure Illinois*. The strategy includes eight domains defined by; capabilities to implement, the projects to attain those capabilities, and high-level timelines for completion.

Tests Performed: Reviewed the Secure Illinois report and interviewed staff.

Test Results: The Department developed a long-term security strategy - Secure Illinois – A Framework for Ensuring the Security of State Information Technology Assets. Although the Framework had an effective date of July 1, 2008, it was not approved until March 3, 2009. The Department identified eight areas and outlined specific projects and target dates. We reviewed the project lists and identified seven projects which had completion dates of January 1, 2009 that were not finalized.

A long-term security framework had been developed and approved; however, several projects had not been finalized within the approved timeframes.

Department Description of Control: Policy development is a collaborative effort that crosses multiple organizational units. Results of this effort are approved policies published on the Department's web site (http://bccs.illinois.gov). Procedures to guide the development and approval process are documented for reference. Templates have been developed to ensure consistency in writing policy, procedures and standards. Policy update memos are distributed periodically to impacted users to announce updates to the policies.

Tests Performed: Reviewed policies, memorandums, distribution listings, and interviewed staff.

Test Results: The Department developed and published the following policies on its website:

- General Security For Statewide IT Resources Policy, effective December 15, 2008,
- General Security For Statewide Network Resources Policy, effective December 15, 2008,
- State of Illinois Enterprise Desktop/Laptop Policy, effective December 15, 2008,
- Data Classification Policy, effective December 15, 2008,
- Data Breach Notification Policy, effective December 1, 2007,
- IT Resource Access Policy, effective December 1, 2007,
- Laptop Data Encryption Policy, effective December 1, 2007,
- Wireless Communication Device Policy, effective December 15, 2008,
- Statewide CMS/BCCS Facility Access Policy, effective December 15, 2008, and
- Electronically Stored Information Retention Policy, effective February 15, 2009.

According to each policy, "In order to implement this policy, CMS establishes procedures and designates responsibility to specific personnel. Each agency should also establish procedures and assign responsibilities to specific agency personnel to achieve policy compliance.

Additionally, "statewide agency security personnel, or their designee, are responsible for monitoring, auditing, tracking, and validating compliance with policies and procedures and conducting investigations into violations of law, policies, or procedures."

However, per the Chief Security Officer, the Department had not designated responsibility to specific personnel, and had not determined if the agencies had established procedures or assigned responsibility to ensure compliance.

Our review of the policies indicated they were targeted to a broad audience and at a general level. The policies did contain references to detailed procedures; however, in several cases, the referenced procedures had not been developed.

Per the Chief Security Officer, the Statewide CMS/BCCS Facility Access Policy was no longer in effect as of January 2009. However, the Policy was still present on the Department's website and employees had not been informed of the revocation.

The Department developed procedures and templates for the development and approval of policies, standards, and procedures.

The Department distributed several security related memorandums/emails during the audit period.

Several of the policies had scope statements such as - this policy applies to all State of Illinois employees, contractors, vendors and agents. The definition of policy scope and applicability is critical in the effective implementation of the policies. Additionally, it is imperative that all employees, contractors, vendors, etc. that are required to comply with policies have been made aware of the policies.

The Department had developed security related policies and posted them on its website. However, the policies referenced documentation which had not been fully developed and requirements to assign responsibility to Department and user agency personnel had not been implemented.

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. Although the Department has taken steps to strengthen its security practices, to further enhance, promote, and guide security practices, the Department should:

- Ensure all audit recommendations and vulnerability assessment recommendations are included in the corrective action database.
- Develop a mechanism to promote the timely remediation of security vulnerabilities and issues classified as high risk.
- Ensure all employees properly complete the policy acknowledgement statement and appropriate documentation is maintained.
- Ensure policies are routinely updated and reflect the current environment.
- Ensure documents referenced in policies are fully developed and current.
- Formally designate responsibility to Department personnel to implement the policies.
- Develop a mechanism to assist user agencies in establishing procedures and assigning responsibilities to specific agency personnel to achieve compliance with the policies.
- Review policy scope statements and clearly define the parties that are required to comply with the policies. Once defined, ensure all appropriate parties are formally informed of the policies.

Additionally, the Department should ensure the Description of Controls is accurate.

PHYSICAL SECURITY

EXISTING ENVIRONMENT

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

Department Description of Control: Access control includes limiting physical entry into buildings and/or locations within a building and uses Access Cards, Badges, locks, 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 forgot their ID badges.

The Physical Security Coordinator issued access cards and PIN Codes. The Department had a Badge Production Matrix, not dated, that detailed the procedure/process utilized to issue badges.

The following was identified as the process for granting access to BCCS facilities:

The Physical Security Coordinator stated once he had received request for ID badge and secured required information from the Department's Personnel Liaison, he then forwarded the request to the individual's on the Physical Access Request Approval Authority list, dated January 15, 2009 for approval. The List identified the staff with the authority to approve ID badge issuance for certain facilities and areas within the facilities.

We selected 25 individuals (23 staff and 2 contractors) who had access to the CCF 3rd floor, and all 73 individuals with access to the Technical Safeguards Lab to determine the appropriateness of access rights. We found 2 individuals that no longer needed access to the 3rd floor and 53 individuals who did not need access to the Lab. Upon notification, the Department removed the access rights for these individuals.

A framework existed to control access to facilities; however, access rights were not routinely reviewed or always deactivated on timely basis.

Department Description of Control: 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.

Tests Performed: Viewed the H/V System and interviewed staff.

Test Results: 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.

The H/V System Administrator's Manual contained instructions to create the physical card or badge. The Manual provided a detailed review over the application's components.

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, individual access rights, and the Department's Policy Manual.

Test Results: The access cards (badges) were FIPS 201-1 compliant as they contained the following, among others:

- Photo.
- Name.
- Bar code.
- Expiration dates.
- Anti-counterfeit feature.

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 17 separated individuals, noting several cases where access cards were not returned as required by the Policy Manual.

Access cards were FIPS 201-1 compliant; 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 interviewed staff.

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 one month of the Building Admittance Registers for both the CCF and Communications Building. We found general compliance with the completion of the Registers.

Security Guards were required to inventory temporary badges at the start of each shift to ensure accountability. We noted at the time of the audit, all badges were accounted for.

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: Reviewed prior year audits and interviewed staff.

Test Results: This Description of Control was referencing the Business Services Building, which as of October 31, 2008 was vacated by the Bureau.

This Description of Control referenced the Business Services Building which no longer used by the Bureau.

Department Description of Control: The H/V system, Access Cards, Badges, security guards, and video surveillance are used to limit or monitor physical entry into the following buildings: the Central Computer Facility and the Communications Building in Springfield.

Tests Performed: Toured facilities and interviewed staff.

Test Results: The Central Computer Facility (CCF), Communications Building, 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, and the Harris Facility utilized video surveillance to monitor the facilities.

No significant exception noted.

Department Description of Control: Physical security at the Clinton facility, Chicago is a joint effort between the Department of Human Services, Department of Health and Family Services and the CMS Bureau of Property Management. Security guards operate during business hours. CMS computing facilities are protected by Cipher locks.

Tests Performed: Toured facility and interviewed staff.

Test Results: The Clinton facility was shared between the Department of Human Services, Department of Healthcare and Family Services, and the Department.

The entrance to the building was unlocked from 7:00am to 6:00pm. All employees were provided with an employee badge to permit access to the facility. A security guard monitored the entrance to the facility from 6:00am to 10:00pm. A second guard patrols the facility from 9:00am to 5:30pm.

After 6:00pm and until 7:00am the next morning, the facility was locked with Cipher locks. The facility was also equipped with an alarm system.

The facility was equipped with external cameras that were monitored at the guard's desk. The loading dock entrance was secured at all times and was equipped with an intercom system.

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.

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 an access card was used, description of access (exit or entry), access granted or denied, door name, and user name and ID number.

Several reports were available on the H/V system menu.

No significant exception noted.

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

Tests Performed: Conducted walkthroughs and interviewed staff.

Test Results: 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: 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 the facilities.

Test Results: Video cameras were used to monitor the CCF, Communications Building, 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: The H/V system control panels have their own Uninterruptible Power Supply (UPS) to provide power to the control panels, and the access control devices they support. Separate UPS module supplies uninterruptible power to certain electric locks.

Tests Performed: Interviewed staff.

Test Results: The UPS for the HV system was the batteries for the system located inside the HV control panel. An automated system monitored the batteries and if there was a problem, the system notified the Physical Security Administrator.

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 process of managing the physical environment includes monitoring environmental factors and providing appropriate preventative maintenance to reduce operating interruptions and damages to the computing resources.

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.

The Department maintained two contracts for the UPS/Batteries for both the Communications and CCF buildings and a contract for the generator at the CCF.

We reviewed maintenance reports conducted at both facilities on the UPS/Batteries and the generator, noting maintenance reports complied with contracts and that all systems appeared to be running appropriately.

During the audit period, the Department experienced a power/interruption failure at the CCF; however, the Department had mitigated this issue by conducting an electrical review over the facility (completed in October 2008) and purchased and installed new backup battery systems (installed in October 2008).

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls (with the exception of routine reviews of access rights) were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should:

- Routinely review the appropriateness of individual access rights.
- Ensure timely revocation of access rights. Specifically, we recommend:
    - Supervisors should 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.
    - Supervisors should be required to notify a change in employment status to the Physical Security Coordinator
    - Contract managers (or the staff member who authorized access rights) should 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.

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, and at the Communications Building.

Tests Performed: Reviewed contracts and toured facilities.

Test Results: The process of managing the physical environment included monitoring environmental factors and providing appropriate preventative maintenance to reduce operating interruptions and damages to the computing resources.

The Department maintained contracts for the following preventative maintenance measures: fire suppression and detection systems, and the water detection system.

The Department also maintained battery and uninterruptible power supply contracts for the two facilities. See the Physical Security control for further information.

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 2008.

In addition, the Department had a contract for the TraceTek water detection system for the CCF. The water detection system was monitored in the Command Center, and the alarm board alerted personnel when potential water hazard had been detected. The water detection system was last inspected in March 2009.

The Communications Building contained fire detection and suppression systems and fire extinguishers. During our tour of the facilities, we noted the fire detection and suppression systems and fire extinguishers were inspected in July 2008.

In addition, the Department maintained an offsite storage facility. During our review, we noted appropriate environmental controls were in place.

We randomly selected times to observe the temperature and humidity readings for the CCF computer room over a 10 day period to ensure the readings were within the recommended industry best practices. The recommended industry best practices require a temperature reading of between 70 to 74 degrees F with a relative humidity reading between 45 to 60%. Auditor noted the computer room during the 10 day period had an average temperature reading of 75.5 degrees F with an average relative humidity reading of 47.9%.

No significant exception noted.

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, critical key processes, 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.

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.

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.

A Pass Down Book was available to provide additional instructions to security guards at the Communications Building. The book was last updated in November 2008. The Pass Down Book for the CCF was not located.

We reviewed the following documentation for the CCF and Communications building, noting the Security Guards appeared to appropriately document duties: Building Admittance Registers, Daily Patrol Reports, and Incident Reports. In addition, we noted all visitor badges were accounted for at the time of the audit.

We did not identify any significant deficiencies in the security guard's performance of duties.

Although security guards existed to protect facilities, information to assist in the performance of duties was not always available.

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, background checks and training documentation, and conducted tours of the facilities.

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 17 individuals assigned to the CCF, Communications Building, and other facilities for janitorial services. We randomly selected five individuals and found background checks were only performed on three out of five individuals reviewed. In addition, we also noted the Department did not maintain appropriate documentation of training provided for four of the five individuals.

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 information to assist in the performance of security guard duties is available and current.
- 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.
- Review temperature readings in the CCF computer room and develop means to maintain temperature readings within recommended industry best practices.

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. Access card and badge issuance to non-Departmental areas is the responsibility of the Department of Human Services (DHS).

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; and
- Limited access, brightly colored badges for use by individuals entering the building to pick up printed output from the I/O Control area.

Test Performed: Toured Harris Facility, reviewed card reader system, access rights, badges, video surveillance system, and interviewed staff.

Test Results: During our review, we found the following physical security controls were established to safeguard the Harris Facility:

- Security guards were stationed in the front entry way 24 hours a day, 7 days a week.
- Multiple video cameras were located inside and outside the building to provide viewable images for security guards.
- Proximity card readers required an active access card for entry to restricted areas and were located throughout the facility.
- Brightly colored badges with limited access for use by individuals entering the building to pick up printed output from the I/O Control area were utilized.

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, since physical security of the Harris Facility is a shared responsibility between the Department and the Department of Human Services, we recommend the Department continue working with DHS to ensure access to restricted areas is adequately secured and restricted to authorized personnel.

SYSTEMS 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. 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.

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 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, protect resources, and data.

No significant exception noted.

Department Description of Control: Remote Monitoring Facility (RMF) reports are run weekly and monthly. These reports are stored on a secured drive and are available to management to monitor system resources and CPU utilization.

Tests Performed: Reviewed RMF reports and interviewed staff.

Test Results: The Department generated Remote Monitoring Facility (RMF) reports on a weekly and monthly basis to assist management in monitoring system resources and CPU utilization.

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.

SYSTEMS SOFTWARE
Zero Downtime Virtual Machine (z/VM)

EXISTING ENVIRONMENT

Background Provided by the Department: z/VM (z/Virtual Machine) is a mainframe operating system utilized at the Central Computer Facility. z/VM is a time-sharing, interactive, multi-programming operating system for IBM mainframes. The major subsystem that is supported in z/VM is NOMAD which is business intelligence software for enterprise reporting and rapid application development.

Department Description of Control: The agency security software administrator must request and obtain a VM User ID from the z/VM staff. Users are assigned user IDs with 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.

No significant exception noted.

Department Description of Control: The z/VM directory is restricted to general access as it 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 objective.

SYSTEMS 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 appear to be operating with sufficient effectiveness to achieve the control objective.

SYSTEMS SOFTWARE
Information Management System (IMS)

EXISTING ENVIRONMENT

Background Provided by the Department: 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.

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 interviewed staff.

Test Results: Security software and system options were implemented to secure libraries, and protect resources and data. IMS was integrated with RACF security software. Users must have a valid RACF ID and password before they could gain access to IMS resources.

No significant exception noted.

OVERALL CONCLUSION

No significant exception noted. Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective.

SYSTEMS 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 ten+ 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 technical support.

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, and if authenticated DB2 allowed access according to established DB2 authorizations.

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.

We obtained and reviewed the Department's listing of the DB2 Coordinators and noted that each agency had assigned a DB2 Coordinator.

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.

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.

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.

SYSTEMS SOFTWARE
Security Software

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: 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 and passwords were used to identify and verify users and were key control mechanisms in the security software. The security software 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 if a violation occurred.

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 monitoring the security violations. The CMS Data Security Administrator reviews CCF staff violations and distributes to each CCF staff their violations, Staff must sign and return their report with an explanation to the CMS Data Security Administrator.

Tests Performed: Reviewed violation reports, procedures, and interviewed staff.

Test Results: The Department had a procedure in place for the monitoring of security violations. Department staff periodically reviewed violation reports and distributed noteworthy violation summaries to staff for explanation.

We reviewed the violation reports for August and September 2008, noting they appeared to have been reviewed and submitted to staff for explanation.

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: 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 the user of their responsibilities including protecting their program and data files.

No significant exception noted.

Department Description of Control: The client security software administrators have the capability of producing the violation 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.

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 as of April 2008. 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. However, to enhance the Department's controls, the Department should work with user agencies to decrease the number of unused (revoked) IDs.

TELECOMMUNICATIONS/NETWORK SERVICES
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.

Department Description of Control: Bureau staff monitors these systems to confirm that devices and systems are properly, installed, configured, and maintained.

Test Performed: Interviewed staff.

Test Results: Together, the Network Operations, Enterprise Network Support, Field Operations and LAN Services groups provided intra-agency and inter-agency network and Internet communications.

No significant exception noted.

Department Description of Control: Network Services manages the Illinois Century Network (ICN), the Illinois Wireless Information Network, and engineering responsibilities related to State of Illinois telecommunications services. The Division consists of two teams which includes Network Operations and Enterprise Network Support.

Test Performed: Reviewed network topologies, device configurations, organizational chart, and interviewed staff.

Test Results: The Department maintained the State of Illinois Statewide Network. Network Services (Network Operations and Enterprise Network Support) was responsible for maintaining the following elements of the network:

- State of Illinois (ICN) Backbone Network (core and distribution routers and firewalls) – maintained by the Network Operations group.
- State Agency Access Network (routers and switches) – maintained by the Enterprise Network Support with support from Field Operations groups.
- IWIN (Illinois Wireless Information Network) – Law Enforcement LEADS Network.

The ICN Backbone Network provided access to:

- Redundant Internet Access,
- State of Illinois Intra-Agency network communications,
- State of Illinois and Federal Inter-Agency network communications,
- Local county and municipal governments,
- Educational institutions public and private including school districts, private schools, colleges, and universities, and
- Healthcare institutions.

The State Agency Access Network connected each of the state agencies' networks to the ICN Backbone Network.

The IWIN network infrastructure provided access for federal, state, and local law enforcement agencies to the LEADS (Law Enforcement Agencies Data System), NCIC (National Crime Information Center), Secretary of State (SOS), NLETS (National Law Enforcement Telecommunications Systems), and CHRI (Criminal History Record Information) platforms.

No significant exception noted.

Department Description of Control: The ICN obtains public Internet services from multiple providers. 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. An additional and final pass through a centralized firewall system provides security for all agencies before reaching the 'Internet'.

Test Performed: Reviewed network topologies, device configurations, and interviewed staff.

Test Results: Network Services obtained public Internet services from multiple providers; however, firewall hardware and configurations protecting agency networks were maintained by LAN Services. (See LAN Services section for additional information.)

No significant exception noted.

Department Description of Control: Network Operations develops standards and designs, installs, maintains and manages the ICN Backbone including backbone circuits, egress circuits, routers, firewalls, switches, fifteen Point of Presence (POP) sites, WAN monitoring tools and WAN services, including DNS, educational and state agency content filtering, and IP Video. Network Operations maintains network diagrams associated with the ICN backbone connectivity and WAN services. Solarwinds Orion is used to manage and monitor the ICN Backbone. TACACS servers authenticate authorized individuals for device configuration and maintenance.

Test Performed: Reviewed network topologies, device configurations, hardware and software vendor websites, access rights, account parameters, Department websites, and interviewed staff.

Test 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 current electronic configurations of the devices, which contained software revision levels and fully documented high-level rule base descriptions. We reviewed the full configurations for a selection of devices as follows:

- 26 Core Routers.
- 23 Agency Distribution Routers.
- 23 Educational Institution Distribution Routers.

Upon review it appeared the ICN Backbone router 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. Upon review and discussion with staff, topology maps provided appeared to be, for the most part, accurate and complete. Additionally, during our review of topologies and configurations we determined devices were placed in suitable logical positions.

Network Operation staff were responsible for installing, customizing, maintaining and supporting WAN management and monitoring tools. Solarwinds was utilized for monitoring and managing the ICN Backbone. Alerts were issued for device and interface up/down status, CPU utilization, memory utilization, bandwidth utilization, and environmentals.

No significant exception noted; however, we did note some parameters which should be reviewed to ensure security issues are appropriately addressed.

Department Description of Control: Enterprise Network Support designs and supports 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. TACACS servers authenticate authorized individuals for device configuration and maintenance.

Test Performed: Reviewed network topologies, device configurations, hardware and software vendor websites, access rights, account parameters, Department websites, and interviewed staff.

Test Results: Access devices connected each of the respective agencies' and non-state agencies' networks to the ICN Backbone Network via distribution routers. We reviewed the current electronic configurations of the devices, which contained software revision levels and fully documented high-level rule base descriptions. We reviewed the full configurations for 38 Agency Access Routers. Upon review it appeared the State Agency Access router configurations were, for the most part, appropriately configured; however, we did note instances where configurations could be enhanced.

Agencies included in the review consisted of CMS, DHFS, DHS, DOT, and REV. Additionally, routers connecting the IWIN infrastructure to the backbone network were reviewed.

Three authentication servers were utilized to provide authorized access to the firewalls, routers, and switches maintained by Network Operations, Enterprise Network Support and Field Operations. 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 utilized appropriate access restrictions.

Due to the nature of the Access segment of the network maintained by Enterprise Network Support and Field Operations, maintaining network topology documents was a joint effort between the two groups. Enterprise Network Support and Field Operations maintained individual network topology maps for each segment of the network it maintained connecting the backbone network (Network Operations) to the agency network (LAN Services). Upon review and discussion with staff, topology maps provided appeared to be, for the most part, accurate and complete. Additionally, during our review of topologies and configurations we determined devices were placed in suitable logical positions.

Solarwinds was utilized for monitoring and managing the Illinois Century Network. Alerts were issued for device and interface up/down status, CPU utilization, memory utilization, bandwidth utilization, and environmentals.

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: Enterprise Network Support has oversight of 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. Fiber records are maintained in a Microsoft Access database as well as within EMS 11. 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 team 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.

Test Performed: Reviewed procedures, dig notices, and interviewed staff.

Test 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 CMS 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.

Fiber records were maintained in a Microsoft Access database for outside plant cable/fiber and major fiber runs in facilities. The Access database contained records of all active and inactive fiber circuits. Additionally, a record of active fiber circuits was maintained in EMS 11 for billing purposes.

The Springfield Fiber Locate Methods and Procedures documented the groups process associated with J.U.L.I.E notices. Upon review of the procedures we noted they appeared to accurately depict the process utilized for dig notices.

We judgmentally selected 20 J.U.L.I.E tickets, for the period of July through December 2008, from CMS Remedy for detailed review. Of the 20 tickets, 17 required dispatch and 5 were considered emergency/rush. 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 tickets, we noted notifications appeared to be dispatched to the vendor in a timely manner.

No significant exceptions noted.

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.

Test Performed: Interviewed staff.

Test Results: Two servers were utilized by Network Operations, Enterprise Network Support and Field Operations to backup firewall, router, and switch configurations for backbone and access devices.

Configurations were automatically backed up daily to a server and the server backed up via tape and rotated off-site.

No significant exception noted.

Department Description of Control: Network Services has established standard network configuration templates for core and distribution routers.

Test Performed: Interviewed staff, reviewed templates and configurations devices

Test Results: Configuration templates were maintained by Network Operations for their core and distribution routers; however, templates were not maintained for Network Operations firewalls. Additionally, a group consisting of staff from Network Operations and Field Operations maintained configuration templates for access routers maintained by the Enterprise Network Support and Field Operations groups. 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.

No significant exception noted; however, we noted some parameters which should be reviewed to ensure security issues are appropriately addressed.

Department of 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.

Test Performed: Interviewed staff.

Test Results: Network Services maintained various standards and methodologies. Per management, the standards and methodologies had not changed since the prior 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 complexity of the statewide network necessitates continual review and analysis to ensure security controls meet the Department's standards. To enhance the controls, the Network Services should continually review security parameters to ensure security issues are adequately addressed.

TELECOMMUNICATIONS/NETWORK SERVICES
IWIN

EXISTING ENVIRONMENT

Department Description of Control: 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).

Test Performed: Reviewed policies and interviewed staff.

Test Results: The Department and the Illinois State Police (ISP) had coordinated efforts to provide IWIN; a wireless wide area data network using code division multiple access (CDMA). The Department administered the IWIN network and ISP provided the connection to the LEADS, NCIC, SOS, NLETS, and CHRI platforms.

No significant exception noted.

Department Description of Control: The "Illinois Statewide Policy Manual," located on the CMS BCCS Catalog website at: http://bccs.illinois.gov/pdf/iwin/iwinpolicymanual.pdf 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.

Test Performed: Reviewed policies.

Test Results: The IWIN Policy Manual (Manual), dated October 2008 and posted on the Internet, outlined the responsibilities for DCMS – IWIN Support Center, Illinois State Police, Local Agency IWIN Coordinators, and IWIN users.

No significant exception noted.

Department Description of Control: The IWIN network infrastructure utilizes redundant routers which connect servers to the provider network. TACACS Servers authenticate authorized individuals for device configuration and maintenance.

Test Performed: Reviewed network topologies, device configurations, and interviewed staff.

Test Results: The IWIN infrastructure contained redundant routers and switches maintained by Enterprise Network Support. Additionally, the infrastructure contained firewalls maintained by Network Operations. (See Network Services for additional information on firewalls, 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.

Test 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.

OVERALL CONCLUSION

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

TELECOMMUNICATIONS/NETWORK SERVICES
Field Operations

EXISTING ENVIRONMENT

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. The RTCs are strategically placed to provide close proximity to the constituents they serve.

Test Performed: Reviewed website and interviewed staff.

Test Results: Field Operations staff were located throughout nine RTCs, representing 15 Market Service Areas. The RTCs were 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 is responsible for the provisioning of hardware and circuits for constituent connections to the ICN as well as providing technical help desk support as needed. Field Operations uses CMS Remedy, ICN Remedy and EMS11 for help desk and provisioning in accordance with established procedures posted to the team Sharepoint site. Service request forms used by constituents are available on Illinois.net and bccs.illinois.gov.

Test Performed: Interviewed staff.

Test Results: Field Operations utilized two versions of Remedy and EMS 11 for provisioning. Field Operations also 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. (See the Help Desk section for details regarding testing of Remedy and EMS 11.)

No significant exception noted.

Department Description of Control: Field Operations is also responsible for maintaining ICN DNS records within the regional DNS servers in accordance with established procedures.

Test Performed: Reviewed procedures and interviewed staff.

Test Results: Field Operations was responsible for maintaining DNS records in accordance with established procedures, as defined by the Internet Engineering Task Force RFC that corresponded with the various DNS record types maintained.

No significant exception noted.

To support our evaluation and testing of this control objective 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.

Test Performed: Reviewed network topologies, device configurations, hardware and software vendor websites, access rights, account parameters, websites, and interviewed staff.

Test Results: The Department maintained the State of Illinois Statewide Network. Field Operations was responsible for maintaining the non-State Agency Access Network (routers)

Access devices connected each of the respective non-State agencies to the ICN Backbone Network via distribution routers. We reviewed the current electronic configurations of the devices, which contained software revision levels and fully documented high-level rule base descriptions. We reviewed the full configurations for 30 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.

Non-State Agencies included in the review consisted of Higher Ed Main Campus.

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.

Test Performed: Interviewed staff.

Test 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 Field Operations should continually review security parameters to ensure security issues are adequately addressed.

TELECOMMUNICATIONS/NETWORK SERVICES
LAN Application Development

EXISTING ENVIRONMENT

Background provided by the Department: The LAN Application Development section is responsible for the development of custom application software, including but not limited to microcomputer, LAN, Internet/Intranet, and client server applications.

Department Description of Control: The section follows the set standards and methodology for Rapid Application Development maintained by the EBAS Quality Assurance section. Tracking the status of requests is performed by using the Service Request Registration System (SRRS).

Tests Performed: Reviewed EBAS Methodology, SRRS, and interviewed staff.

Test Results: The LAN Application Development Unit utilized the Rapid Application Development (RAD) process defined in the EBAS Methodology, dated August 2005, for developments.

RAD projects were exceptions to the sequential processes of the Methodology. The purpose of this exception was to utilize iterative and prototyping development technologies that could expeditiously provide completed systems to the user. The criteria for using the RAD Methodology were: the development platform supports the iterative process or supports prototyping; the scope was limited; or the estimated hours for the project were under 200. The RAD Methodology provided the same information as the sequential Methodology process, except the deliverables were grouped differently.

We noted there were no new developments for the LAN Application Development Unit during the fiscal year.

The LAN Application Development Unit utilized the SRRS database to track requests. We reviewed the SRRS and examined all five of the changes completed during the fiscal year, noting all five changes complied with the EBAS Methodology.

Of the five changes completed during the fiscal year, only one change altered data when moved into production. The change was properly approved; however, the staff member who programmed the change also moved the changed into production. Generally accepted information technology guidance endorses the development of adequate change control procedures to ensure proper segregation of duties. These procedures include restricting programmers/analysts from making a change and moving it into the production to ensure all changes have been independently authorized and moved to production.

Department officials stated that due to staff limitations in the LAN Application Development Unit, the individual making the changes sometimes moved the changes into production.

Although there were limited changes during the audit period, the one move to production was not performed by an independent person.

Department Description of Control: The Enterprise Remedy Change Management system is used for change control. The business owner can request changes to their applications via Remedy. User security to applications is determined and implemented based on the software tool used for development. Section personnel are responsible for maintaining security for applications, but the business owner is responsible for informing the section of user access requirements.

Tests Performed: Reviewed SRRS and interviewed staff.

Test Results: Business owners requested changes to their applications through the Change Management module via Remedy and/or Help Desk module via Remedy. All five changes completed during the fiscal year were originally requested through Remedy and then documented in SRRS.

Application security procedures and individual access rights were dictated by the business owners. We noted that end user access rights requests were documented in the SRRS database.

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 controls, the Department should ensure an appropriate segregation of duties exists and have an independent person perform moves to production.

TELECOMMUNICATIONS/NETWORK SERVICES
Web Services

EXISTING ENVIRONMENT

Department Description of Control: The Bureau provides web services that enable 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 sites/applications. The "New Web Site Checklist" is used to ensure completeness of information for new static web sites. This checklist resides on the Web Services/Lan Application Development sharepoint site.

Tests Performed: Reviewed the New Web Site Checklist 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 the New Web Site Checklist. The checklist was utilized by Department staff to provide guidance on the development of websites.

No significant exception noted.

Department Description of Control: Web sites are reviewed by the Department's Illinois Office of Information and Communication for compliance with the IITAA Implementation Guidelines for Web-Based Information and Applications (based on the Illinois Information Technology Accessibility Act (IITAA). This information is located on the Illinois Depart of Human Services web site. Prior to being placed into production, updates and modifications are reviewed and approved by the owner. Once approval is obtained, the developer requests that their supervisor (or designee) move the changes into production. An Access database (which is used to track requests) is then updated with this information.

Tests Performed: Reviewed website and interviewed staff.

Test Results: During the process for new developments and major content changes, Web Services staff forwarded web sites to the Illinois Office of Information and Communication for review to ensure the web sites met the requirements defined in IITAA. The IITAA standards were located on the Department of Human Services web site at http://www.dhs.state.il.us/page.aspx?item=32765.

Web content changes were requested by user agencies via email and documented in the Web Services Access database. The content change was assigned to a developer, who completed the request and verified the changes with the user. After verification from the user, changes were moved into production.

No significant exception noted.

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. A standardized form is used for these requests. Domain naming conventions are outlined at http://www.illinois.gov/Tech/govpolicy.cfm.

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 5 Request forms, noting the forms obtained appropriate authorizations and generally complied with the instructions to complete the forms.

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.

TELECOMMUNICATIONS/NETWORK SERVICES
PIM

EXISTING ENVIRONMENT

Background Provided by the Department: The Personal Information Manager (PIM) section is responsible for providing a centralized and consolidated platform that facilitates a statewide common architecture for managing email.

Department Description of Control: The General IT Policy is used to govern these activities. The Enterprise Shared Services Email Standards is a document that supports this policy. This document and other procedural documents are used by the PIM group to guide their actions, and are available on the BCCS central repository. PIM is governed by Change Management Policy and Procedures.

Tests Performed: Reviewed standards and interviewed staff.

Test Results: The Department maintained the Enterprise Shared Services Email "Standards", effective June 9, 2008, which provided guidance on security and protection for all Department managed users and agencies. We reviewed the standards, noting no exceptions.

In addition, the Department utilized and followed the General IT Policy in conjunction with the Enterprise Shared Services Email Standard. See the Security Administration control review for further information regarding the General IT Policy.

Also, PIM staff utilized various procedural documents that were available on a Sharepoint site. We noted the PIM Sharepoint site was only available to authorized staff.

Changes in the PIM environment followed the Change Management procedures. See the Change Management control review for further information regarding change control.

No significant exception noted.

Department Description of Control: The PIM group has an Enterprise class virus filtering and SPAM solution in place called IRONMAIL that provides both anti-virus and spam filtering services. PIM also provides Blackberry server and client services.

Tests Performed: Interviewed staff.

Test Results: The Department utilized IRONMAIL for anti-virus and spam filtering. All consolidated agencies and some smaller agencies utilized IRONMAIL.

The Department supported approximately 2,200 Blackberry devices distributed among 50 agencies and commissions.

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.

TELECOMMUNICATIONS/NETWORK SERVICES
LAN Services

EXISTING ENVIRONMENT

Department Description of Control: The LAN 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.

Test Performed: Reviewed network topologies, device configurations, hardware and software vendor websites, access rights, account parameters, and interviewed staff.

Test Results: The Department maintained the State of Illinois Statewide Network. LAN Services was responsible for maintaining the State Agency Network (agency specific firewalls, routers, and switches).

LAN Services provided the LAN network architecture (including firewalls, routers, and switches) for the Department and consolidated agencies.

We reviewed the current electronic configurations of the devices, which contained software revision levels and fully documented high-level rule base descriptions. We reviewed the full configurations for a selection of devices as follows:

- 32 Firewalls.
- 55 Routers.
- 9 Switches.

Upon review it appeared the State Agency firewall, router, and switch configurations were, for the most part, appropriately configured; however, we did note instances where configurations could be enhanced.

To document its network architecture, LAN Services maintained individual network topology maps for each of the agency network segments it maintained. Upon review and discussion with staff, topology maps provided were, for the most part, accurate and complete. Additionally, during our review of topologies and configurations we determined devices were placed in suitable logical positions.

No significant exception noted; however, we did note parameters which should be reviewed to ensure security issues are appropriately addressed.

Department Description of Control: LAN Services maintains configuration standards for LAN infrastructure devices. These standards are implemented on newly deployed equipment.

Test Performed: Reviewed templates and configurations for devices.

Test Results: LAN Services maintained the CMS/BCCS LAN Services Standards for Hardware Configuration 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 baselines settings; however, we did note instances where configurations could be improved.

No significant exception noted, however, we noted some security parameters which should be reviewed to ensure security issues are appropriately addressed.

Department Description of Control: LAN Services is responsible for entering rules into the firewalls and monitoring security violations via firewall monitoring software. Security logs are processed for possible violations and reviewed for performance issues and/or intrusion prevention.

Test Performed: Interviewed staff.

Test Results: Solarwinds was utilized for monitoring and alerting issues on the agency network segments maintained by LAN Services. Alerts were issued for device and interface up/down status. Although alerts were not set up for CPU utilization, memory utilization, bandwidth utilization, environmentals, etc, they have the capability to run reports for various statistics.

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 and Solarwinds. Reports were generated daily and distributed to appropriate LAN Services, Midrange and PIM staff for review.

No significant exception noted.

Department Description of Control: LAN Services is governed by Change Management Policy and Procedures. Scheduled backups of critical device configurations are performed twice daily.

Test Performed: Interviewed staff.

Test Results: Changes to the agency network infrastructure were governed by the Change Management Policy and Procedure. (See Change Control section for additional details).

LAN services had a project under way to migrate device configuration backups to Solarwinds Network Configuration Manager (NCM) tool. Additional licenses for this product were recently procured and, at the time of review, over 350 devices were being backed up. LAN Services devices that had not been migrated to the new NCM tool were inconsistently backed up using various processes. This project is due to be completed by June 30, 2009.

No significant exception noted; however, not all devices were consistently backed up.

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 agency networks necessitates continual review and analysis to ensure security controls meet the Department's standards. To enhance the controls, the LAN Services should:

- Continually review security parameters to ensure security issues are adequately addressed.
- Ensure all configurations are routinely backed up and rotated to a secure off-site location.

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 52 entities. (See page 160 for a 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 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 have an interface with AIS; however, the interface was not being utilized.

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 the Mainframe Security Procedures, appropriateness of individuals with access to AIS, and interviewed staff.

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 obtained, users must use a separate application user ID and password to gain access to AIS.

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 AIS, noting one of the individuals should not have had access to the system. The Department immediately deleted the access rights upon notification by the auditors.

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 (Methodology), Service Requests (SR's), Program Library Procedures, and Electronic Move Production Forms.

Test Results: The Methodology was the guide, revised August 2005, developed in-house, for new systems development, modifications to existing systems, user manuals, purchase of third-party software, user training, testing, and conducting post-implementation reviews.

During the audit period, AIS had one service request. We reviewed the service request, noting it 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 Methodology, SR's, Program Library Procedures, or Electronic Move Production Forms.

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 or at the off-site storage location.

Test Results Department staff stated backups of AIS were performed daily, weekly and monthly.

We reviewed a sample of 25 AIS backup tapes and located all the tapes at the off-site storage location. In addition, we randomly selected 25 tapes to be located at the CCF, noting no exceptions.

No significant exception noted.

Department Description of Control: Project Administration includes requirements gathering, 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 of the Methodology and the IT Governance Process.

According to the EBAS Manager there were no AIS projects which required project administration.

No significant exception noted.

Department Description of Control: EBAS Quality Assurance applies to AIS.

Tests Performed: Reviewed EBAS Quality Assurance (QA) procedures.

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: 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 169,237 data records tested were properly entered within the established parameters 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 AIS Online User Manual and interviewed staff.

Test Results: The AIS Online User Manual provided a complete listing of various online and batch reports used for the balancing of transaction. Also, the 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 Revenue
14. Department of Veterans' Affairs
15. Department on Aging
16. Environmental Protection Agency
17. General Assembly Retirement System
18. Guardianship and Advocacy Commission
19. Historic Preservation Agency
20. Human Rights Commission
21. Illinois Arts Council
22. Illinois Civil Service Commission
23. Illinois Commerce Commission
24. Illinois Community College Board
25. Illinois Council on Developmental Disabilities
26. Illinois Criminal Justice Information Authority
27. Illinois Deaf and Hard of Hearing Commission
28. Illinois Educational Labor Relations Board
29. Illinois Labor Relations Board
30. Illinois Law Enforcement Training and Standards Board
31. Illinois Office of the State's Attorneys Appellate Prosecutor
32. Illinois Prisoner Review Board
33. Illinois Procurement Policy Board
34. Illinois Student Assistance Commission
35. Illinois Violence Prevention Authority
36. Illinois Workers' Compensation Commission
37. Judges' Retirement System
38. Judicial Inquiry Board
39. Office of Management and Budget
40. Office of the Attorney General
41. Office of the Auditor General
42. Office of the Executive Inspector General
43. Office of the Governor
44. Office of the Lieutenant Governor
45. Office of the State Appellate Defender
46. Office of the State Fire Marshal
47. Property Tax Appeal Board
48. State Board of Elections
49. State Employees' Retirement System
50. State Police Merit Board
51. State Universities Civil Service System
52. 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 166 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 obtained, 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 access rights of the 5 Department staff members with access to CPS, noting the access rights appeared appropriate.

No significant exception noted.

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 Systems Development (ASD) Methodology Manual (Methodology), Service Requests (SR's), Program Library Procedures, and Electronic Move Production Forms.

Test Results: The Methodology was the guide, revised August 2005, developed in-house, for new systems development, modifications to existing systems, user manuals, purchase of third-party software, user training, testing, and conducting post-implementation reviews.

We noted there were no changes to CPS in the past year.

No significant issues were identified with the contents or utilization of the Methodology, SR's, Program Library Procedures, or Electronic Move Production Forms.

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 and backups maintained at the CCF and at the off-site storage location.

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. We reviewed five CPS backup tapes and located all the tapes at the CCF or the off-site storage location.

In addition, we noted the CPS backup tapes were not encrypted to protect personal or confidential data.

No significant exception noted; however, CPS backup tapes were not encrypted to protect personal or confidential data

Department Description of Control: Project Administration includes requirements gathering, 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 of the Methodology and the IT Governance Process.

According to the EBAS Manager there were no CPS projects which required project administration.

No significant exception noted.

Department Description of Control: EBAS Quality Assurance applies to CPS.

Tests Performed: Reviewed EBAS Quality Assurance (QA) procedures.

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: 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.

Test Results: The Department had a User Manual, dated February 2007, 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 10,003 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.

<u>Tests Performed:</u> Reviewed the Payroll Release Log and CPS User Manual.

<u>Test Results:</u> 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 the Payroll Release Log, noting 25 of 25 individuals who picked up payroll were appropriately authorized.

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 ensure personal or confidential on backup tapes is adequately protected from unauthorized or accidental disclosure.

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 was 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 23 entities. (See page 171 for the list of user agencies).

Department Description of Control: CIS is an online real time system; adds, deletes, and updates to the inventory data takes affect as soon as a transaction meets all the required criteria. CIS has the ability to utilize an optical scanner to read bar code labels during a physical inventory by using additional external software. 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 meets all the GASB-34 rules; it allows the user agencies the ability to accurately track depreciation on items that they specify.

Tests Performed: Reviewed the Department's Property Control Division's rules, list of user agencies, the CIS Application, GASB-34 Rules, 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).

CIS had the ability to read bar code labels for physical inventory.

The CIS application followed GASB-34 rules mandated by the Office of the Comptroller.

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 the Mainframe Security Procedures, appropriateness of individuals with access to CIS, and interviewed staff.

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 was 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 26 staff members to CIS, noting 5 of the individuals should not have had access to the system.

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), Service Requests (SR's), Program Library Procedures, and Electronic Move Production Forms.

Test Results: The Methodology was the guide, revised August 2005, developed in-house, for new systems development, modifications to existing systems, user manuals, purchase of third-party software, user training, testing, and conducting post-implementation reviews.

During the audit period, CIS had three service 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: 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 schedule, and backups maintained at the CCF or the off-site storage location, and interviewed staff.

Test Results: We reviewed the list of backup tapes for CIS and identified completed daily, weekly, and monthly backups of CIS data.

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: Project Administration includes requirements gathering, 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 of the Methodology and the IT Governance Process.

According to the EBAS Manager there were no CIS projects which required project administration.

No significant exception noted.

Department Description of Control: EBAS Quality Assurance applies to CIS.

Tests Performed: Reviewed EBAS Quality Assurance (QA) procedures.

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: The Department has developed an online CIS User Manual. 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.

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 400,321 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 the previous day's 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.

We reviewed the CIS Location Balance Report dated March 31, 2009 noting the report indicated no locations were out of balance. The Department utilized the Location Balance Report to ensure transactions posted properly.

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 Public Health
8. Department of Transportation
9. Department of Veterans' Affairs
10. Department on Aging
11. Environmental Protection Agency
12. Historic Preservation Agency
13. Illinois Arts Council
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 Violence Prevention Authority
19. Illinois Workers' Compensation Commission
20. Office of Management and Budget
21. Office of the Attorney General
22. Office of the Governor
23. 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 177 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 rights to CTAS, and interviewed staff.

Test Results: Access to CTAS was 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 2 of the individuals should not have had access to the system. The Department immediately deleted the access rights upon notification by the auditors.

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 Systems Development (ASD) Methodology Manual (Methodology), Service Requests (SR's), Program Library Procedures, and Electronic Move Production Forms.

Test Results: The Methodology was the guide (revised August 2005), developed in-house, for new systems development, modifications to existing systems, user manuals, purchase of third-party software, user training, testing, and conducting post-implementation reviews.

During the audit period, CTAS had two 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 significant issues were identified with the contents or utilization of the Methodology, SR's, Program Library Procedures, or Electronic Move Production Forms.

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 schedule, backups maintained at the CCF or 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 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. We reviewed a sample of 25 CTAS backup tapes and located all the tapes at the off-site storage location. In addition, we randomly selected 25 tapes to be located at the CCF, noting no exceptions.

In addition, we noted the CTAS backup tapes were not encrypted to protect personal or confidential data.

No significant exception noted; however, CTAS backup tapes were not encrypted to protect personal or confidential data.

Department Description of Control: Project Administration includes requirements gathering, 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 of the Methodology and the IT Governance Process.

According to the EBAS Manager there were no CTAS projects which required project administration.

No significant exception noted.

Department Description of Control: EBAS Quality Assurance applies to CTAS.

Tests Performed: Reviewed EBAS Quality Assurance (QA) procedures.

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: 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 numbers for proper input, edits, and compliance with date standards. We determined that the 1,708 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: Recovery procedures for CTAS provide guidelines for restoration.

Tests Performed: Reviewed the CTAS Recovery Reports and the Business Continuity Plan.

Test Results: The Department developed the CTAS Recovery scripts, not dated, and the Business Continuity Plan, dated December 31, 2008.

The Recovery Script report provided steps necessary to recover the CTAS database in the event of a disaster. The Plan identified the Technical Support staff responsible for the recovery of CTAS.

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, the Department staff stated CTAS generated an error report, a reconciliation report, and a file maintenance activity report. All errors were to be reconciled before the “Close” could be finalized.

The CTAS User Manual documented reports that could be requested by the user for reconciliation purposes.

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.
- Ensure personal or confidential on backup tapes is adequately protected from unauthorized or accidental disclosure.

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.

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 Housing Development Authority
45. Illinois Labor Relations Board
46. Illinois Law Enforcement Training and Standards Board
47. Illinois Math and Science Academy
48. Illinois Office of the State's Attorneys Appellate Prosecutor

49. Illinois Prisoner Review Board
50. Illinois Procurement Policy Board
51. Illinois State Board of Investment
52. Illinois State Police
53. Illinois State Toll Highway Authority
54. Illinois State University
55. Illinois Student Assistance Commission
56. Illinois Violence Prevention Authority
57. Illinois Workers' Compensation Commission
58. Joint Committee on Administrative Rules
59. Judges' Retirement System
60. Judicial Inquiry Board
61. Legislative Audit Commission
62. Legislative Ethics Commission
63. Legislative Information System
64. Legislative Printing Unit
65. Legislative Reference Bureau
66. Legislative Research Unit
67. Medical District Commission
68. Northeastern Illinois University
69. Northern Illinois University
70. Office of Management and Budget
71. Office of the Architect of the Capitol
72. Office of the Attorney General
73. Office of the Auditor General
74. Office of the Comptroller
75. Office of the Executive Inspector General
76. Office of the Governor
77. Office of the Lieutenant Governor
78. Office of the Secretary of State
79. Office of the State Appellate Defender
80. Office of the State Fire Marshal
81. Office of the Treasurer
82. Property Tax Appeal Board
83. Senate Operations
84. Sex Offender Management Board
85. Southern Illinois University
86. State Board of Education
87. State Board of Elections
88. State Employees' Retirement System
89. State of Illinois Comprehensive Health Insurance Board
90. State Police Merit Board
91. State Universities Civil Service System
92. State Universities Retirement System
93. Supreme Court of Illinois
94. Teachers' Retirement System of the State of Illinois
95. University of Illinois
96. 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 37).

Department's Description of Control	Test Results	Report Page
ADMINISTRATION-Recovery Services		
The following contingency plans and templates provide guidance and reference material to address restoration of various client environments: ▪ Continuity Methodology ▪ Recovery Activation Plan.	Per Department staff, the Continuity Methodology referenced in the Description of Control was the Recovery Methodology.	68
The Department, as defined in the Continuity Methodology, conducts scheduled annual regional and local mainframe recovery tests that exercise two levels of recovery: ▪ Comprehensive – enterprise mainframe environment to exercise all qualified critical mainframe applications simultaneously recovered on a remote host. ▪ Local – exclusive mainframe environments for individual applications recovered independently at a local recovery exercise host system.	Additionally, exercise documentation lacked detail to determine if all qualified mainframe applications were simultaneously recovered as outlined in the Department's Description of Control.	69
Recovery Services staff assist in updating and rehearsing these procedures during the comprehensive and local recovery exercises.	According to Recovery Services 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.	70
ADMINISTRATION-Vendor Management		
Documented procedures for reconciling desktop, mainframe and midrange software are outlined in the AIM/Vendor Management Guide.	Our review of the Guide 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.	77
CHANGE CONTROL		
The Department's Change Management Unit is responsible for managing changes to the Department's environment (except for applications under EBAS control) that are initiated as the result of an ESR (Enterprise Service Request), a configuration change, or an internal work assignment.	Although the Change Management Unit was responsible for the majority of the primary functions covered by this review; several other related functions, such as LAN services, DOT, DHS and DHFS mainframe, and networks for non-state agencies followed different processes for change management.	101

SECURITY ADMINISTRATION		
Corrective action tracking is achieved through collection of recommended improvements from sources such as audit recommendations and internally conducted vulnerability assessments. These recommended improvements are entered into a database.	We reviewed the database and found vulnerability assessment recommendations were not included in the database.	106
PHYSICAL SECURITY		
For those buildings not staffed with 24/7 security guard protection, each entry door remains locked.	This Description of Control was referencing the Business Services Building, which as of October 31, 2008 was vacated by the Bureau.	113

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

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

CICS – Customer Information Control System

CIO – Chief Information Officer

CIS – Central Inventory System

CMC – Customer Management Center

CMS – Central Management Services

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

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

EMS – Expense Management System

ENS – Enterprise Network Services

EPA – Illinois Environmental Protection Agency

EPM – Enterprise Program Management

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

HSM – Hierarchical Storage Management

H/V – Hirsch Velocity

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

IQAM – Infrastructure Quality Assurance & Methods

ISD – Information Services Division

ISP – Illinois State Police

IT – Information Technology

IITAA – Illinois Information Technology Accessibility Act

ITG – Information Technology Governance

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

MPLS – MultiProtocol Label Switching

NOMAD – Name of application utilized on VM

PCF – Property Control Form

PIM – Program Information Management or Personal Information Management

PIR – Post-Implementation review

PKI – Public Key Infrastructure

POP – Point Of Presence

PSR – Paging Service Request or Product Standardization Request

QA – Quality Assurance

RACF – Resource Access Control Facility

RAD – Rapid Application Development

REV – Department of Revenue

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

SMF – System Management Facility

SMS – System Management Storage

SNA – Systems Network Architecture

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

SRRS – Service Request Registration System

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

WCS – Warehouse Control System

WSR – Wireless Service Request

z/OS – Zero Downtime Operating System

z/VM – Zero Downtime Virtual Machine