SERVICE ORGANIZATION REVIEW

Department of Central Management Services
Bureau of Communications and
Computer Services

July 2011

TABLE OF CONTENTS

STATE OF ILLINOIS
OFFICE OF THE
AUDITOR GENERAL
William G. Holland, Auditor General

SUMMARY REPORT DIGEST

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
BUREAU OF COMMUNICATIONS AND COMPUTER SERVICES

SERVICE ORGANIZATION REVIEW
For the Year Ended: June 30, 2011

Release Date: July 2011

INTRODUCTION

This report covers our Service Organization Review of the Department of Central Management Services – Bureau of Communications and Computer Services for the year ended June 30, 2011.

The Department of Central Management Services' (Department) Bureau of Communications and Computer Services carries out statutory responsibilities relating to data processing and telecommunication services. 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 102 user agencies.

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 processing integrity, availability, and security of computerized data and functions.

The Department has defined and documented policies and procedures to restrict physical access to facilities and defined systems. However, we found the controls over verifying the identity of an individual prior to resetting their password and the granting, modifying or revoking physical access badges had not been effectively implemented and, therefore, were not operating effectively throughout the period July 1, 2010 to June 30, 2011. With the exception of these matters, the procedures were generally sufficient to provide reasonable assurance that relevant control objectives were achieved.

WILLIAM G. HOLLAND
Auditor General

Office of the Auditor General, Iles Park Plaza, 740 E. Ash St., Springfield, IL 62703 • Tel: 217-782-6046 or TTY 888-261-2887
This Report Digest and a Full Report are also available on the internet at www.auditor.illinois.gov

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

STATISTICS	2011
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 – 4.0 Million Lines per Month Laser Printing – 18.4 Million Pages per Month
State Agency Users	102
Bureau Employees	2008 -- 708 2009 -- 679 2010 -- 641 2011 -- 577
Historical Growth Trend**	2008 -- 4,018 -- MIPS 2009 -- 4,035 -- MIPS 2010 -- 3,908 -- MIPS 2011 -- 4,184 -- MIPS -- Million Instructions Per Second ** In the month of April for each year listed

Information provided by the Department – Not Examined

DEPARTMENT DIRECTOR AND DEPUTY DIRECTOR/BUREAU MANAGER
During Audit Period: Director: James Sledge – July 1, 2010 to June 17, 2011 Currently: Acting Director: Malcom Weems – June 17, 2011 to Present During Audit Period and Current: Acting Deputy Director/Bureau Manager: Rich Fetter

Springfield Office:

Iles Park Plaza
740 East Ash - 62703-3154
Phone: 217/782-6046
Fax: 217/785-8222 TTY (888) 261-2887

Chicago Office:

State of Illinois Building - Suite S900
160 North Lasalle – 60601-3103
Phone: 312/814-4000
Fax: 312/814-4006

Office Of The Auditor General
William G. Holland

INDEPENDENT SERVICE AUDITOR'S REPORT

The Honorable William G. Holland
Auditor General - State of Illinois

We have examined the attached description titled "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' Assertion Regarding the State of Illinois Information Technology Environment" for the Period July 1, 2010 to June 30, 2011 (the description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the security, availability, and processing integrity principles set forth in *Trust Services Principles, Criteria, and Illustrations for Security, Availability, and Processing Integrity* (AICPA, *Technical Practice Aids*), throughout the period July 1, 2010 to June 30, 2011. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of the Department of Central Management Services, Bureau of Communications and Computer Services' controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

Service organization's responsibilities
The Department of Central Management Services, Bureau of Communications and Computer Services has provided the attached assertion titled "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' Assertion Regarding the State of Illinois Information Technology Environment" for the Period July 1, 2010 to June 30, 2011, which is based on the criteria identified in management's assertion. The Department of Central Management Services, Bureau of Communications and Computer Services is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in the Department of Central Management Services, Bureau of Communications and Computer Services' assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants; the standards applicable to attestation engagements contained in *Government Auditing Standards* issued by the Comptroller General. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period July 1, 2010 to June 30, 2011.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion

The Department of Central Management Services, Bureau of Communications and Computer Services states in the description of its system that the Department has defined and documented policies and procedures to restrict physical access to facilities and defined systems. However, as noted on pages 66-67 and 95-97 of the description of tests of controls and the results thereof, controls over verifying the identity of an individual prior to resetting their password, and granting, modifying or revoking physical access badges had not been effectively implemented and, therefore, were not operating effectively throughout the period July 1, 2010 to June 30, 2011.

The Department's Mainframe Security Procedures required the confirmation of an individual's identity prior to resetting their password. However, the Help Desk and Security Compliance security staff routinely bypassed the confirmation process for password resets.

In addition, the Department's requirements for obtaining, modifying or revoking a physical security access badge were not complied with. Specific requirements, including the completion and approval of forms were required; however, the Department did not always observe or have documentation to support compliance with these requirements.

The control deficiencies resulted in not meeting the following criterion: procedures are in place to implement policy requirements and to monitor the systems and policies.

In our opinion, except for the matter referred to in the preceding paragraph, based on the description criteria identified in the Department of Central Management Services, Bureau of Communications and Computer Services assertion and the applicable trust services criteria, in all material respects

a. the description fairly presents the system that was designed and implemented throughout the period July 1, 2010 to June 30, 2011.

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period July 1, 2010 to June 30, 2011, and user entities applied the complementary user-entity controls contemplated in the design of the Department of Central Management Services, Bureau of Communications and Computer Services' controls throughout the period July 1, 2010 to June 30, 2011.

c. the controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period July 1, 2010 to June 30, 2011.

Description of tests of controls

The specific controls we tested and the nature, timing, and results of our tests are presented in the section of our report titled "Description of Test of Controls and Results Thereof."

Supplementary Information

The information attached to the description titled "Other Information Provided by the Department of Central Management Services, Bureau of Communications and Computer Services That Is Not Covered by the Service Auditor's Report" describes the Department of Central Management Services, Bureau of Communications and Computer Services' State of Illinois Information Technology Environment. It is presented by the management of the Department of Central Management Services, Bureau of Communications and Computer Services to provide additional information and is not a part of the service organization's description of the State of Illinois Information Technology Environment made available to user entities during the period from July 1, 2010 to June 30, 2011. Information about the Department of Central Management Services, Bureau of Communications and Computer Services State of Illinois Information Technology Environment has not been subjected to the procedures applied in the examination of the description of the State of Illinois Information Technology Environment and the suitability of the design and operating effectiveness of controls to meet the related criteria stated in the description

of the State of Illinois Information Technology Environment, and accordingly, we express no opinion on it.

Intended use

This report and the description of tests of controls and results thereof are intended solely for the information and use of the Department of Central Management Services, Bureau of Communications and Computer Services; user entities of the "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' Assertion Regarding the State of Illinois Information Technology Environment" during some or all of the period July 1, 2010 to June 30, 2011, the Auditor General, the General Assembly, the Legislative Audit Commission, the Governor, and independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

However, this report is a matter of public record and the distribution is not limited.

William J. Sampias, CISA
Director, Information Systems Audits

Mary Kathryn Lovejoy, CPA, CISA
Information Systems Audit Manager

June 29, 2011

CMS
ILLINOIS Pat Quinn, Governor
DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
Malcolm Weems, Director

June 29, 2011

The Honorable William G. Holland
Auditor General-State of Illinois
Springfield, Illinois

RE: Management of the Department of Central Management Services, Bureau of Communications and Computer Services' Assertion Regarding the State of Illinois Information Technology Environment for the Period July 1, 2010 to June 30, 2011

We have prepared the attached description titled " Description of the Department of Central Management Services, Bureau of Communications and Computer Services' Assertion Regarding the State of Illinois Information Technology Environment for the Period July 1, 2010 to June 30, 2011" (the description), based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraphs 1.33–.34 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the State of Illinois Information Technology Environment, particularly system controls intended to meet the criteria for the security, availability, and processing integrity principles set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria).

We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the State of Illinois Information Technology Environment throughout the period July 1, 2010 to June 30, 2011 based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided

(2) The components of the system used to provide the services, which are the following:

- *Infrastructure.* The physical and hardware components of a system (facilities, equipment, and networks).
- *Software.* The programs and operating software of a system (systems, applications, and utilities).

- *People.* The personnel involved in the operation and use of a system (developers, operators, users, and managers).
- *Procedures.* The automated and manual procedures involved in the operation of a system.
- *Data.* The information used and supported by a system (transaction streams, files, databases, and tables).

(3) The boundaries or aspects of the system covered by the description

(4) How the system captures and addresses significant events and conditions

(5) The process used to prepare and deliver reports and other information to user entities and other parties

(6) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system

(7) Other aspects of the Department's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria

(8) Relevant details of changes to the Department's State of Illinois Information Technology Environment during the period covered by the description

ii. The description does not omit or distort information relevant to the State of Illinois Information Technology Environment while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. the controls stated in the description were suitably designed throughout the specified period to meet the applicable trust services criteria.

c. the controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria, except as noted in the report over the Department of Central Management Services, Bureau of Communications and Computer Services' Assertion Regarding the State of Illinois Information Technology Environment.

Sincerely,

Rich Fetter

Rich Fetter
Acting Deputy Director
Central Management Services
Bureau of Communications and Computer Services

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
BUREAU OF COMMUNICATIONS AND COMPUTER SERVICES'
ASSERTION REGARDING THE STATE OF ILLINOIS
INFORMATION TECHNOLOGY ENVIRONMENT
(DESCRIPTION OF SYSTEM)

The following Description of System (pages 7 to 32) has been provided by the management of the Department. The accuracy and completeness of the Description of System is the responsibility of the Department.

Strategic Planning

Objective: Defined goals are required to properly align the Bureau's strategic plan with the mission and objectives of the State, Department and user entities.

Controls:

- Management has periodic meetings with the State CIO and Department senior management to define direction and objectives.
- Management conducts periodic meetings with consolidated agencies, Illinois State Police, Department of Children and Family Services, and the Department of Corrections to provide updates on technology initiatives, discuss technology needs, issues, and strategic plans.
- Management conducts periodic meetings with State Agency CIOs and Senior IT managers to share information and solicit discussion on broad issues that may affect the use of technology in Illinois Government. Agendas are provided and handout materials are distributed as is warranted.
- Management meets frequently with individual user entities to discuss various topics including direction and objectives.
- BCCS determines its goals by analyzing the needs of user agencies, changes in technology and trends in the industry, and the direction given by Department management and the Governor's Office.

Objective: Research and information regarding technology and trends in Government and the industry is utilized in setting goals.

Controls:

- Management and technical subject matter experts meet and request information on a regular basis from existing vendors, other technology providers, and industry experts to monitor technology trends.
- Management receives information on technology options through the Request for Information and procurement processes.

Objective: Management monitors progress of specific projects and activities that arise from the strategic plan.

Controls:

- Processes exist for management to track the progression of all priority projects and procurements through the Enterprise Project Management (EPM) Portal.
- Management holds priority project meetings on a regular basis to track and discuss the progression of all priority projects and procurements using reports from the EPM portal.
- Management holds executive leadership meetings and manager meetings to discuss activities and progress toward goals.

User Agency Controls:

- Agencies are to ensure their priorities related to Department services are effectively communicated to Department management by participating in the group meetings, requesting individual meetings and contacting the Bureau and Department management regarding issues important to their agency.

Billing

Objective: Procedures exist to ensure rates have been established for services supplied to the entities.

Controls:

- Expenditures are coded to cost centers and assigned to services through a cost accounting model.
- Revenues for each service are compared to costs to determine the appropriateness of individual rates.
- Rates for many services are available in the BCCS Service Catalog.
- In order to comply with federal requirements (A-87), an analysis is performed annually to determine the profit/loss for each service.

Objective: Procedures exist to help ensure accurate billings and billing details are provided to entities for which services are provided.

Controls:

- Documented billing practices and procedures are followed to ensure the accuracy of billing statements for both funds.
- Reports are produced and verified against each other and an edit check is completed to help ensure the completeness and accuracy of each billing.
- Details on each billing are available on the invoices, through the EMS11 system for CRF billings, and on a SharePoint site for SSRF billings.

Objective: The CMS Fiscal Operation Policy ensures the collection of outstanding accounts.

Controls:

- The CMS Fiscal Operation Policy outlines the process for the collection of outstanding accounts.

- Delinquency letters are sent out based on the number of days an invoice is past due. An account aging analysis is sent out on a quarterly basis.

Objective: Procedures exist to ensure billing discrepancies are reviewed and adjusted as needed.

Controls:
- Requests for billing credits must be submitted in writing, and be properly approved.
- Approved billing credits are sent to A&R Shared Services for processing and posting via an ARCM request form.

User Agency Controls:
- User entities should review and monitor their monthly billings to ensure charges are appropriate.
- User entities should ensure all payments are made in a timely manner.

Service Communications

Objective: The Department and User Agencies are provided with access to information regarding the Department and the services it provides.

Controls:
- Periodic meetings are held with the User Agencies to share information regarding the Department and the services it provides.
- The BCCS Service Catalog is available online and outlines information on most available services and rates.
- The BCCS website serves as a central location for communicating information about available services, policies and procedures, contact information, forms and guides for requesting services, announcements/bulletins, and a variety of other information to the Department and its User Agencies.
- Quarterly newsletters, memos and bulletins regarding Department changes, updates and notifications are produced and distributed to the Department and its User Agencies.

Objective: The Department provides avenues for User Agencies to submit and receive information on incidents, service requests and changes.

Controls:
- User Agencies can submit incidents and service requests via e-mail or phone for processing and tracking by the Department. The Department provides and maintains status information via the Remedy Service Desk System as well as by offering additional ad-hoc reporting capabilities to User Agencies.
- An Enterprise Change Management website is maintained to provide an updated listing of scheduled changes, stakeholders, and affected parties.

Objective: The Department and select User Agencies are provided with access to data and reports related to service delivery and performance.

Controls:

- Various reporting systems that provide service delivery and performance monitoring capabilities are available to select User Agencies and Department managers.
- The Enterprise Program Management system is used to track and provide status on ongoing service related projects, initiatives, and reporting.

Objective: User Agencies are provided a means to discuss and resolve issues regarding the services the Department provides.

Controls:

- Periodic meetings are held with User Agency Telecom Coordinators to share information and to address User Agency service concerns.
- Meetings are held upon request of the User Agency to discuss and resolve service related issues.
- E-mail boxes are available that allow User Agencies to submit service related questions or concerns. In addition, User Agencies may also contact the Customer Service Center (CSC) with any service questions or concerns.

User Agency Controls

- User Agencies have the responsibility of reviewing service delivery and performance information made available by the Department.
- User Agencies have the responsibility to notify the Department of any service issues they have.

Continuous Service

Objective: The Department has policies and procedures in place to help safeguard the availability of critical Department-managed resources.

Controls:

- A disaster recovery policy exists.
- Disaster recovery plans are tested periodically for critical IT assets.
- The Department has an alternate recovery site.

Objective: The Department communicates recovery responsibilities to appropriate users and responsible parties.

Controls:

- The Department periodically conducts meetings, and initiates audio conferences to keep appropriate users informed of procedures and the status of support services.
- A disaster recovery communications portal (SharePoint site) contains relevant information such as standards and templates as well as critically important information during a rehearsal.

Objective: Procedures exist to assist maintaining the integrity of critical data and system backups.

Controls:

- An inventory of backups and their location is maintained.
- Backups are stored at an off-site location.
- Backups are utilized during the annual recovery testing.

User Agency Controls:

- Each Agency is responsible for; developing and maintaining appropriate and viable business continuity plans, application recovery scripts, designated application information updates to the BRM, recovery exercise procedures and schedules, and ongoing communications with CMS/BCCS
- Each Agency is responsible for establishing procedures and assigning responsibility to specific agency personnel, such as an IT Recovery Coordinator to achieve policy compliance.
- Each Agency is responsible for:
    - understanding the IT Recovery Policy and the CMS/BCCS IT Recovery Methodology;
    - determining the appropriate criticality and RTO classification of their applications;
    - communicating the criticality and RTO classification to CMS/BCCS;
    - actively participating in local and regional exercises as business needs dictate.

Help Desk

Customer Service Center (CSC)

Objective: Policies exist to report and act upon issues and incidents.

Controls:

- The Incident Ticket procedures document the process by which the CSC enters incident calls from customers in Remedy Help Desk Case module.
- The EMS manual documents the process by which the Telecom Provisioning Unit enters the customer service requests in EMS.
- The ESR procedures for IT MAC (Move/Add/Change) document the process by which the IT Service Desk enters customer service requests in Remedy Change Request module.
- The Non-routine procedures document the process by which the Telecom Project Unit enters the request information in Remedy PRV module.

Objective: Policies exist to ensure only authorized requests are made.

Controls:

- Agency management delegates, in writing, an IT and Telecom coordinator(s) authorized to expend funds.
- CSC verifies submitter is authorized.

- The Telecom Service Desk has documented M&Ps for voice mail password resets.

Objective: The Department monitors, logs and tracks calls, incidents and service requests.

Controls:

- The Avaya phone system and its internal functionality provides the tools and means by which the number of customer calls are logged and tracked.
- The Remedy Help Desk Case Module and its internal functionality provides a system generated Case Number and the tools and means by which customer incidents are logged, tracked, and updated with supporting documentation through resolution.
- The EMS system and its internal functionality provides a system generated Request Number and the tools and means by which all Telecom service requests are logged, tracked, scheduled with external vendors and/or internal teams and updated through completion.
- The Remedy Change Request module and its internal functionality provides a system generated Change Request Number and the tools and means by which customer incidents are logged, tracked, scheduled with external vendors and/or internal teams and updated through completion.
- All Help Desk Cases and Service Requests are to be properly documented and updated through completion detailing resolution steps and work performed.
- ESRs are assigned tasks for engaging and tracking external vendors and internal teams.
- The Remedy PRV module provides the tools and means by which Non-routine requests are logged, tracked and updated to obtain the necessary procurement approvals.

Objective: The Department classifies and prioritizes incident calls and new service requests to ensure timely and satisfactory customer service**.**

Controls:

- The Avaya phone system and its internal functionality provides the ability to classify and prioritize calls via announced menu options, "blind" options, and personnel changes via skill based routing as necessary.
- The Remedy Help Desk Case module uses category, type and item (CTI) to identify classification and assignment to appropriate individuals/groups.
- The priority field in Remedy Help Desk Case identifies the priority of the incident per user agency request.
- User agencies have the ability to verbally request the level of priority of their reported incident or by designating priority on the Telecom and IT service request forms.
- CSC obtains customer confirmation/satisfaction before closing incidents.
- IT Service Desk obtains customer confirmation/satisfaction before closing ESRs/addendums.

Objective: The Department communicates information regarding services to user agencies.

Controls:

- User agencies have the ability to call back for updates on incidents by referencing the assigned Remedy Case Number provided by the CSC when reporting an incident, or they can track current status if they have Remedy access.
- Telecom user agencies have the ability to call back for updates on service requests referencing the EMS Request Number or their agency assigned control number, or they can track current status if they have EMS access.
- IT user agencies have the ability to call back for updates on service requests referencing the assigned Remedy Change Request Number or they can track current status if they have Remedy access.
- If IT user agency has Remedy access, the Change Request Number and status updates are automatically sent to customer upon CSC entering their request, during status changes of the request, and at resolution.

Objective: Procedures exist to escalate unresolved incidents.

Controls:

- The CSC has M&Ps for CSC incidents based on specified criteria defined by management.
- The IT Service Desk has M&Ps for management and VIP ticket escalations and MORT (Major Outage Response Team) procedures.

Objective: External vendors and internal team performance are monitored.

Controls:

- Monthly reports are generated from Remedy and EMS to track and monitor vendor performance for Telecom Services.
- For Telecom Services, the Department and vendors reconcile misses against contractual intervals. Based on reconciliation, penalty amounts are calculated and deducted from the monthly maintenance invoice in accordance with the contract specifications.

Objective: Trends and recurring problems are monitored.

Controls:

- The Telecom Help Desk staff asks all callers if the reported incident is chronic. If identified as a chronic issue, procedures exist to pull history report and escalation.
- The IT Service Desk managers review multiple reporting sources (Remedy metrics, Avaya phone metrics) from the CSC Quality Assurance Team to identify spikes in service demands, call volumes, and ticket counts. Corrective actions and resource allocations are implemented as needed at the IT Service Desk.

Customer Management Center (CMC)

Objective: Procedures exist to report and act upon issues and incidents.

Controls:

- Methods and procedures are available to assist staff members in providing support and resolving network issues.

Objective: The Department monitors, logs and tracks calls, incidents and service requests.

Controls:

- CMC staff use Remedy to document incidents and service requests.
- Remedy ticket logs are used to document the incident and actions taken to bring the incident to resolve.

Objective: Procedures exist to escalate unresolved incidents.

Controls:

- The CMC has established procedures for managing the escalation of incidents.

User Agency Controls:

- User agencies should review and monitor their monthly billings to ensure Telecom provisioning and repair charges are accurate.
- User agencies should review EMS and monthly billings to monitor usage and submit change requests based on evaluation and eliminate paid services with non-usage.
- User agencies should engage CSC Projects Unit to assist in the evaluation of telecommunications options to reduce costs and/or improve efficiencies as needed.

Change Management

Objective: Policies exist to provide that only authorized and documented changes are made to the Department's production environment.

Controls:

- The Department's Change Management Policy and the Remedy Change Management Guide describe the change initiation, documentation standards, approval process, and post implementation review process.
- Requests for changes (system maintenance and vendor maintenance) follow the Change Management Policy and Guide.
- A Request for Change (RFC) is required to be completed for all production changes.
- The Remedy Action Request System is utilized to track all RFCs to the Department's environment.
- Requests for Change (RFC) are based on the Category, Type and Item (CTI).
- The Remedy Action Request System routed the changes to the appropriate staff based on CTI and documents the approvals and authorizations for the requested changes.
- High Impact Changes require that a test plan be attached to the RFC, if applicable.
- High Impact Changes testing documentation is maintained by the applicable area.
- Post implementation reviews are conducted on all emergency changes and scheduled changes which cause a major outage.

- Planned (low, medium, and high impact) changes are reviewed by the technical approver (Shared Services Manager) and both reviewed and scheduled by the business approver (Enterprise Change Management Team). In addition, medium and high impact changes are reviewed by the Change Advisory Committee.
- Changes are communicated to users via Change Advisory Committee Meetings and reports located on the ECM SharePoint Site.
- High Impact Changes require a back-out plan be attached to the RFC for use in the event of a disruption.

Objective: Procedures exist to provide that emergency changes are documented and authorized timely.

Controls:
- All emergency changes are required to complete the standard documentation outlined in the Change Management Policy and the Remedy Change Management Guide.
- All emergency changes are reviewed by the technical and business approver post implementation.
- Emergency changes are communicated to users post implementation via the Change Advisory Committee Meeting.

User Agency Controls:
- Users should develop adequate internal controls for application changes.

Information Assurance

Objective: The Department defines and documents IT policies for security.

Controls:
- The Department's security policies have been established and posted to the publically accessible web site http://bccs.illinois.gov/it_policies.htm.

Objective: The Department communicates security obligations to users and responsible parties.

Controls:
- Security summits are hosted by the Department to share relevant cyber security topics of interest to State government security professionals and other IT professionals.
- Security awareness month educational materials are distributed to user agency IT management.
- Public facing website disseminates awareness and educational information and is accessible at http://bccs.illinois.gov/security/awareness.htm.
- Notification of newly published or significantly modified cyber security policies is achieved through inter-office email notifications coordinated by Agency Relations.
- Pertinent information is disseminated to appropriate parties and posted when appropriate on Department repositories such as IL-ISAC and the Department's Web portal.

Objective: The Department has procedures in place to implement policy requirements.

Controls:

- System security account activity reports are generated and procedures have been developed to investigate system security violations.
- Critical Incident Response procedures exist that establish responsibility for responding to and reporting of cyber incidents that threaten Department cyber assets.

Objective: The Department monitors their systems and policies.

Controls:

- Scans on IT resources are conducted and logs are produced by the Technical Safeguards staff to detect operating system and Web application vulnerabilities, unauthorized software, potential intrusion activity, and/or to identify mission software patches when operationally appropriate or when other circumstances warrant.
- Department employees must acknowledge acceptance of security policies which is monitored by the Department's Personnel Liaisons.
- Evidentiary discovery tasks are initiated by cyber security specialists when requested by law enforcement or cyber security professionals and findings are reported to authorized parties.

User Agency Controls:

- User agencies should ensure they have reviewed the security polices located on the Department's website.
- User agencies should communicate to the Department their specific security requirements.

Physical Security

Central Computer Facility (CCF) and the Communications Building

Objective: Procedures exist to restrict physical access.

Controls:

- Physical access to facilities is restricted to authorized individuals by a card key system. Proximity card readers also restrict access to areas within the facilities.
- Absentee limits and restrictions on employee pass-back are activated to help control physical access to buildings.
- In order to obtain an access badge:
    - Privileges must be approved by an appropriate authority and are subject to modification or revocation by same.
    - All employees and contractors of the CMS Bureau of Communication and Computer Services (BCCS) will be issued a photo card credential subject to the confirmation of CMS employment or contractual relationship, a screening for outstanding warrants and criminal history.

    - Presentation of one of the following identity source documents: State issued Driver's License, State issued State ID card, a U.S. Government photo ID if not a U.S. citizen.
- Physical access cards are managed by BoPM Security Administrator.
- Access is logged, maintained and reviewed by BOPM Security Administrator.
- Supervisor or Manager is responsible for collection and return of ID Badge's upon employee or contractor discharge, separation or card expiration.
- Processes exist for issuing and maintaining real property keys.
    - The Facility Managers or designee determines the need of an employee and/or contractor to be issued a facility key and to keep to a minimum the number of keys issued.
    - Employees are to report a lost key to the issuer (Manager) immediately.
    - Key(s) are to be returned at the end of State employment, contractual obligation or upon issuer's request.
- The Department has a contract with a security firm.
- Security guards staff facilities 24/7.
- Security guards patrol the interior and exterior of the facilities.
- Security guards document their daily shift activities.
- Security Guards issue temporary badges (with limited access rights) to visitors, and to employees who forget their assigned access card.
- Those issued a temporary badge must sign the Building Admittance Register.
- Security guards inventory the temporary badges at the start of each shift.

Objective: Procedures exist for the identification and escalation of physical security breaches.

Controls:
- Post orders and emergency evacuation procedures are at every guard desk.

Objective: Measures to prevent or mitigate threats have been implemented.

Controls:
- Controlled areas are protected against fire using smoke detectors and fire suppression systems. The smoke detectors and fire suppression system are tested periodically.
- Water detectors are installed within the raised floor area.
- The Central Computer Facility is supplied by two different power sources.
- The Central Computer Facility is equipped with an uninterruptible power supply (UPS).

<u>Clinton Facility</u>

Controls:
- Physical security controls over the Clinton Facility include:
    - Security guards,
    - Video cameras strategically located inside and outside the building,
    - Proximity card readers requiring an active Access Card to allow entry, and
    - Alarm System.

Harris Facility

Controls:

- Physical security controls over 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.

Willard Ice Building

Controls:

- Security guards staff facilities 24/7.
- Proximity card readers that require unique access codes are located in the interior of the buildings to control and restrict access to controlled areas.
- Controlled areas are protected against fire using smoke detectors and fire suppression systems.
- The smoke detectors and fire suppression system are tested periodically.
- Controlled areas temperature and humidity are controlled and monitored.
- Controlled areas are protected with uninterruptible power supplies.
- Preventive maintenance agreements are in place.

User Agency Controls:

- Security authorization lists should be reviewed, updated, approved, and returned to the Department on a bi-annual basis.

Production Control and Input Units

Objective: The Department has computer operations and job scheduling procedures which document procedures and instructions.

Controls:

- Production Control staff utilizes agency procedures to determine and define all batch processing schedules and to assist with problem determination and resolution.
- The Computer Operations unit can use Visio flowcharting, historical data and or agency provided documentation to determine the job flow of batch processing scheduled by the Production Control unit.
- The Reporting Unit is responsible for setting up and maintaining reports produced from the agencies and placing them in Mobius for electronic viewing, archival and retrieval.
- Production Control staff monitors the JCL of scheduled batch processing for any abnormal conditions and modifies as necessary before programs are processed, reran or set up for the next schedule.

Objective: The Dept provides a batch job monitoring and problem resolution service to the CMS, DHS, DOT, EPA, HFS and IDOR agencies.

Controls:

- Production Control utilizes automated scheduling systems CA-Scheduler to control and schedule the batch processing for assigned agencies.
- Input Control utilizes the automated scheduling system, Zeke to control and schedule Department of Revenue batch processing.
- The Bluezone emulation software is utilized to monitor all assigned processing.
- Emergency (after-hours) program migrations from test to production status are performed at the request of agencies. These requests are forwarded to the Production Control unit for follow-up and to ensure documentation is accurately updated.
- Agency processing schedules and requests are submitted through shared e-mail address.
- Production Control staff contact lists for problem resolution are maintained and available in SharePoint, e-mail and hardcopy.
- Problems are logged on daily shift reports and reviewed by supervisors, management and staff.
- Shift reports are available to the agencies on SharePoint and the agency then controls internal access to these reports.

User Agency Controls:

- Daily schedules are supplied to the after-hours Input unit for CMS, DHS, HFS and DOT by the Production Control unit with access through a EPOS (Enterprise Production Operation Services) SharePoint site. IDOR sends a schedule copy to the Input unit shared email site.
- For problem resolution, HFS (except the Medical unit) allows access to database TSO.Info.Clist listing primary, secondary and supervisor contacts.
- The HFS Medical unit supplies resolution information.
- DHS provides a Microsoft Access database for problem contacts.
- DOT has an in-house SharePoint site for problem resolution to maintain and grant access to Input personnel.
- EPA uses a mainframe – accessible file.
- IDOR provides emails and call-lists for resolution.

Library Services

Objective: Agency standards and policies.

Controls:

- CMS, DHS, HFS sets the standards and policies for their respective agencies which would include document approvals, forms to use and the responsibilities for each step of the process. This documentation is available on SharePoint. DOT requests are set up using historical knowledge, past practice and agency contact when necessary. There is no set standard in place for all agencies as they each have their own unique process to follow. These processes allow Library Services to navigate through the mainframe and/or browse the Mobius reports to ensure the integrity of the media and libraries, using the most current security software available.

- Checking reports online using Mobius and checking all library jobs in CA-Scheduler for successful completion of assigned tasks and schedules assist staff members to identify and correct any hardware or software issues to keep all system impacts to a minimum.

Objective: The Library Support unit communicates the procedures to the users.

Controls:

- All email requests contains agency, library and member information necessary for the Library Support staff to complete their tasks.

Objective: The Library Services section monitors compliance with policies.

Controls:

- Processes and reports exists to control and track media to provide accurate data as follows:
  - TGS (automated Tape Generating System) for DHS and HFS.
  - Manual system for legacy Mental Health systems.
  - Manual system for DOT.
- The following processes exist to identify and correct hardware and software issues to keep system impacts to a minimum:
  - Checking TGS reports.
  - Check for successfully completed jobs
- Automated software is used to control and track media for easy accessibility.
- Reports are used to inventory media to keep inventories current.
- Authorization lists, forms and/or broadcasts are used to control the release and receipt of media for security purposes.

User Agency Controls:

- All user agency security lists are reviewed, updated, approved, and returned to the Department on a bi-annual basis to ensure the most up-to-date lists are in place which minimizes any security breach.

Output Production

Objective: Distribution of output is restricted to authorized individuals.

Controls:

- The Focal System contains a listing of individuals authorized to pickup print jobs.
- Individuals are required to provide identification and/or verified by Revenue staff and sign the Report Distribution Log for each pickup.
- CMS/HFS/DHS print jobs are maintained in the secure print shops.
- During business hours, the remaining agencies print jobs are maintained in the distribution room. After hours, the print jobs are maintained in the secure print shop.
- All payroll jobs or any job with Social Security numbers and names are sealed.

Objective: Measures to maintain the printing equipment have been implemented.

Controls:

- Preventive maintenance agreements are in place.
- Any printer down time is recorded in the Down-time Log.
- Monthly status reports are maintained which document the number of reports produced and the printer meter readings.
- Printer configurations are backed-up weekly and stored in Revenue's tape library. However, DHFS is responsible for the backup of the printer they utilize. It is backed-up weekly and stored at Revenue's tape library.

User Agency Control:

- User agencies should ensure the security authorization listing is updated to reflect authorized individuals.

Security Software

Objective: Procedures exist to restrict access to defined systems**.**

Controls:

- Access to the defined systems is granted to an authenticated user.
- Creation, reassignment or granting access to an ID requires the ESR process.
- Users are required to have a password and ID in order to gain access to the systems.
- All IDs have a default unit.
- Use of group or shared ID's are not permitted.
- Passwords are complex and require a specific syntax.
- Security configuration parameters force passwords to be changed in defined intervals.
- ID's are disabled after a defined number of unsuccessful login attempts.
- Invalid access attempts are logged.
- Access violations are reviewed and investigated.
- The ability to establish, modify or delete a user, or user access privileges, is limited to Security Administrators.
- The ability to establish, modify or delete an Admin account, or privileges, is limited to Security Administrators.
- Access to superuser functionality and sensitive system functions is restricted to authorized staff.
- Access to data and system resources is based on the ID and role-based units.
- IP activity is limited to those ID's with an identifier field on both the ID and the ID's default unit.
- Production and Test data is protected by a general profile or specific profile.
- Verification is sent to the agencies on a semi-annual basis for the verification of agency RACF coordinators.

User Agency Controls:

- 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 ID's and delete ID's 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.

System Software

Objective: Procedures exist to maintain system components consistent with defined system policies.

Controls:
- An up-to-date listing of all software and their respective level, version and patch is maintained.
- Changes to the environment follow the Department's Change Management Process.
- The assigned CMS technician is responsible for ensuring all software is maintained at latest version/level/patch.

Objective: Procedures exist to protect against unauthorized access to system resources.

Controls:
- System logs are utilized to monitor the environment.
- Success/failure events are logged.
- Chief Security Officer is notified of potential security issues/breaches.

Objective: Procedures exist to restrict access to resources.

Controls:
- Security software is used to control access to systems and resources.
- The Enterprise Service Request (ESR) is used to request access to systems and resources.

Objective: The Department's mainframe environment availability and performance is monitored and reviewed.

Controls:
- Automated tools are utilized in monitoring the performance and availability of the environment.
- Events are logged and reviewed by the assigned CMS technician.
- System performance, availability, and capacity requirements are monitored and reviewed by CMS management.

Storage and Backup

Objective: Procedures are in place to restrict access to resources.

Controls:

- RACF administrator assigns a RACF ID after receiving approval from staff supervisor.
- Resources are secure utilizing RACF.
- Access to offline storage, backup data, systems and media is limited to authorized staff.

Objective: Procedures are in place to guide storage activities.

Controls:

- System automation is utilized to control and monitor storage levels.
- Thresholds are included in Storage Pool listings.
- The Command Center monitors thresholds after hours and notifies ESB staff if thresholds exceed limits.
- Users are notified by ESB staff if thresholds are exceeded.
- Users complete an Enterprise Service Request which initiates the completion of a Request For Change to request additional disk space. Additional disk space is allocated by ESB staff utilizing documented instructions.
- Users complete an Enterprise Service Request which initiates the completion of a Request for Change to request deletion of disk space by ESB. Deletion of disk space is performed by ESB staff utilizing documented instructions.

Objective: Procedures are in place to guide backup activities.

Controls:

- Automated software is utilized to control and schedule backups.
- Actual backup schedules are reviewed against the defined backup schedule.
- Backups are tracked through CA-Scheduler.

Objective: Procedures are in place to control verification of backups.

Controls:

- ESB Staff monitors successful completion of backups by utilizing documented instructions.
- ESB staff is notified of failed backups.
- Users are notified of failed backups.
- ESB uses restoration procedures after receiving a Help Desk Ticket requesting the restoration of data.

User Agency Controls:

- Users are to utilize an Enterprise Service Request through the Help Desk to request additional storage.
- Users are to open an ESR through the Help Desk to request the deletion of storage.
- Users are to open a Help Desk Ticket through the Help Desk for the restoration of data.

Network Services

Objective: Policies exist to document the network settings.

Controls:

- The Basic MPLS Common Connectivity Model document settings.
- The Agency WAN Redundancy standard document settings.
- Created configuration templates for core and distribution routers.
- Utilizes Cisco Advanced Services quarterly reports.
  - To keep network in-line with Cisco best practices recommendations.
  - Reviewed by Cisco and Network Operations.
- Network diagrams are maintained.
- ICN Remedy and EMS 11 are utilized to inventory current data circuits.

Objective: Procedures exist to monitor against unauthorized access to system resources.

Controls:

- Authentication servers are utilized to control access and ensure only properly authenticated individuals are granted access to devices for configuration management and maintenance.
  - This is done via Cisco Tacacs+ system.
  - Granting access requires management approval.
- SolarWinds Orion is utilized to monitor the network.
  - Solarwinds is monitoring the backbone core, distribution, and customer access routers. The devices are being monitored with icmp for up/down status. Device CPU, memory, and interface bandwidth utilization and error data is also collected and stored in the database.
  - Monitored device results are under constant 24/7 review by CMC
  - Monitored, failed devices are attended to by CMC and the applicable NetOps group.
  - Notification is escalated to management level if applicable.
- ICN Remedy and CMS Remedy are utilized for trouble ticketing and tracking problem resolution.

Objective: Procedures exist to provide for the completeness, accuracy and timeliness of backups.

Controls:

- Firewall, router, and switch configurations are backed up via two methods.
  - Method 1:
    - A server is used to gather the configurations.
    - An archive file (tar) of all the configurations is created on the server.
    - The archive file is retrieved by the Data Center Storage team.
    - The retrieved file is backed up in accordance with the Data Center Storage team's defined backup strategy.

- Method 2:
  - An Orion, Solarwinds server is used to gather the configurations.
  - The configurations are stored locally on the server.
  - The configurations are backed up periodically.

Objective: Procedures exist to provide that only authorized, tested and documented changes are made to the infrastructure**.**

Controls:
- Changes to the infrastructure follow the Department's Change Management process.

User Agency Controls:
- Users should ensure the Department is aware of their specific security requirements.
- Users should ensure the Department is aware of their specific Wide Area Network requirements.

LAN Services

Objective: Policies exist to document the Department's standard/template for the LAN network settings.

Controls:
- The LAN Services Standards for Hardware Configuration and Development document the Department's configuration standards.
- Individual network topology maps are maintained for each network segment.

Objective: Procedures exist to monitor against unauthorized access to system resources.

Controls:
- SolarWinds and NCM are utilized to monitor the network and ensure configurations are appropriately backed up.
  - Events are logged daily and reviewed by LAN Services.
- Tools are utilized to monitor the network and early identification of potential security breaches.
- Incident logs are monitored and evaluated by LAN Services.
- The Security Solution Team is notified of any breaches.
- TACACS is utilized to ensure only authorized individuals have access.
- Access is granted based upon team assignment within LAN Services.
- An authorization request form is sent to the LAN Services Data Center Supervisor by the employees supervisor authorizing access.
- An authorization request form is sent to the LAN Services Data Center Supervisor by the employees supervisor requesting access to be removed when appropriate.
- LAN Services periodically monitors access rights.
- McAfee Smartfilter internet filtering service to consolidated agencies (AGR, CEO, CMS, DHS, DPH, DNR, FPR and REV).

Objective: Procedures exist to provide that only authorized, tested and documented changes are made to the infrastructure.

Controls:

- Changes to the infrastructure follow the Department's Change Management process.

User Agency Control:

- Users should ensure the Department is aware of their specific security requirements.
- Users should ensure the Department has implemented the appropriate internet filtering controls. Additionally, the Department should monitor the internet filtering logs.

Internet-Enabled Web Applications

Objective: A structured software development methodology is utilized to manage any new software developments and enhancements to existing code, and to ensure that only authorized, tested and documented changes are made to the application.

Controls:

- All application development changes are controlled in accordance with the Application Systems Development Methodology Manual.
- New developments and enhancements are documented through the use of an Enterprise Service Request (ESR) and documented in the Remedy System.
- New developments and enhancements are approved and tested before implementation into the production environment.
- New developments, as well as enhancements, are moved into production by ISD Midrange and require an approved ESR to execute changes requested by EAA Application Development staff.
- Affected program documentation is updated as part of system developments or enhancements that are required to comply with the Information Technology Governance (ITG) process.

Objective: The following System Security controls provide reasonable assurance that adequate measures are employed to ensure overall system security.

Control:

- Application Development security is controlled by Security Groups which ensure that the individual developing the application does not have the authority to move the changes into the production environment.

User Agency Controls:

- Verify only accurate and authorized data are entered into the web applications. 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 web applications to ensure access authorized is appropriate.

LAN Applications

Objective: A structured software development methodology is utilized to manage any new software developments and enhancements to existing code, and to ensure that only authorized, tested and documented changes are made to the application.

Controls

- All application development changes are controlled in accordance with the Application Systems Development Methodology Manual.
- New software developments and enhancements, and changes are documented through the use of the Remedy Change Module (ESR) or EPM Portal.
- New developments, enhancements, and changes are approved and tested before implementation into the production environment.
- New developments, enhancements, and changes are approved through Remedy Change Management Module process.
- Affected program documentation is updated as part of system developments or enhancements required to comply with the Information Technology Governance (ITG) process.

Objective: Processes exist to restrict access to LAN applications.

Controls

- Development security is controlled by Access Security Groups which, along with Drive Mapping, ensures that only authorized users are allowed access to the application.

User Agency Controls:

- Verify only accurate and authorized data are entered into LAN applications. 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 LAN Applications to ensure access authorized is appropriate.

Accounting Information System (AIS)

Objective: A structured software development methodology is utilized to manage any new developments or enhancements to existing software code to ensure that only authorized, tested and documented developments and enhancements are made to the application.

Controls:

- All application developments and enhancements are controlled in accordance with the Application Systems Development Methodology Manual.
- New application developments and enhancements are documented through the use of a Service Request Form (SR) and are documented in the Service Request Registration System (SRRS).
- New application developments and enhancements are approved and tested before implementation into the production environment.
- New developments, enhancements, and changes are moved into production by the Library Control Group.
- Affected program documentation is updated as part of system developments or enhancements required to comply with the Information Technology Governance (ITG) process.
- System Users are informed when an application development or enhancement will affect them.

Objective: Quality Assurance procedures monitor compliance with system development and change processes.

Controls:

- A technical verification is conducted to ensure the quality and completeness of each new application development or enhancement.

Objective: Processes exist to restrict logical access to AIS.

Controls:

- A checklist with the necessary security tasks is completed when new user agencies are added.
- Each AIS user agency has a Security Administrator who is responsible for adding new users. That process is the responsibility of the user agency.
- Security software is used to control access.
- AIS internal security is used to enable and limit user capabilities.
- Assignment and authorization of access rights are the responsibility of the user agency.

Objective: The AIS User Manual outlines the procedures related to completeness, accuracy, timeliness and authorization of transactions.

Controls:

- Data requirements exist to force correction of errors and completion of critical fields before a transaction is accepted.
- AIS provides various reports to assist the users in verifying and balancing transactions.
- Entry, authorization and integrity of data are the responsibility of the user agency.

User Agency Controls:

- 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 that the access authorized is appropriate.

Central Inventory System (CIS)

Objective: The structured software development methodology is utilized to manage any new developments, any enhancements and maintenance to existing code to ensure only authorized, tested and documented developments and changes are made to the application.

Controls:

- All application development changes are controlled in accordance with the Application Systems Development Methodology Manual.
- New developments, enhancements, and changes are documented through the use of a Service Request Form (SR) and documented in the Service Request Registration System (SRRS).
- New developments, enhancements, and changes are approved and tested before implementation into the production environment.
- New developments, enhancements, and changes are moved into production by the Library Control Group.
- Affected program documentation is updated as part of system developments or enhancements required to comply with the Information Technology Governance (ITG) process.
- System Users are informed when an application development or enhancement will affect them.

Objective: Quality Assurance procedures monitor compliance with system development and change processes.

Controls:

- A technical verification is conducted to ensure the quality and completeness of each new application development or enhancement.

Objective: Processes exist to restrict logical access to CIS.

Controls:

- A checklist with the necessary security tasks is completed when new user agencies are added.
- Each CIS user agency has a Security Administrator who is responsible for adding new users. That process is the responsibility of the user agency.
- Security software is used to control access.

- CIS internal security is used to enable and limit user capabilities.
- Assignment and authorization of access rights are the responsibility of the user agency.

Objective: The CIS User Manual outlines the procedures related to completeness, accuracy, timeliness and authorization of transactions.

Controls:
- Data requirements exist to force correction of errors and completion of critical fields before a transaction is accepted.
- CIS provides various reports to assist the users in verifying and balancing transactions.
- Entry, authorization and integrity of data are the responsibility of the user agency.

User Agency Controls:
- 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.

Central Time and Attendance System (CTAS)

Objective: A structured software development methodology is utilized to manage any new developments, any enhancements and maintenance to existing code to ensure only authorized, tested and documented developments and changes are made to the application.

Controls:
- Changes are logged, tracked and approved through the EPM process.
- New developments, enhancements, and changes are approved and tested before implementation into the production environment.
- New developments, enhancements, and changes are moved into production by the Library Control Group.
- Affected program documentation is updated as part of system developments or enhancements required to comply with the Information Technology Governance (ITG) process.
- System Users are informed when an application development or enhancement will affect them.

Objective: Processes exist to restrict logical access to CTAS.

Controls:
- A checklist with the necessary security tasks is completed when new user agencies are added.
- Each CTAS user agency has a security administrator who is responsible for adding new users. That process is the responsibility of the user agency.

- Security software is used to control access.
- CTAS internal security is used to enable and limit user capabilities.
- Assignment and authorization of access rights are the responsibility of the user agency.

Objective: The CTAS User Manual outlines the procedures related to completeness, accuracy, timeliness and authorization of transactions.

Controls:

- Data requirements exist to force correction of errors and completion of critical fields before a transaction is accepted.
- CTAS provides various reports to assist in verifying and balancing transactions.

User Agency Controls:

- 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.
- Regularly review those authorized to pick up timekeeping reports, and inform appropriate CTAS personnel of changes timely.

Central Payroll System (CPS)

Objective: A structured software development methodology is utilized to manage any new developments, any enhancements and maintenance to existing code to ensure only authorized, tested and documented developments and changes are made to the application.

Controls:

- Changes are logged, tracked, and approved through the EPM process.
- New developments, enhancements, and changes are approved and tested before implementation into the production environment.
- New developments, enhancements, and changes are moved into production by the Library Control Group.
- Affected program documentation is updated as part of system developments or enhancements required to comply with the Information Technology Governance (ITG) process.
- System Users are informed when a system development or enhancement will affect them.

Objective: Processes exist to restrict logical access to CPS.

Controls:

- A checklist with the necessary security tasks is completed when new user agencies are added.

- Each CPS user agency has a Security Administrator who is responsible for adding new users. That process is the responsibility of the user agency.
- Security software is used to control access.
- CPS internal security is used to enable and limit user capabilities.
- Assignment and authorization of access rights are the responsibility of the user agency.

Objective: The CPS User Manual outlines the procedures related to completeness, accuracy, timeliness and authorization of transactions.

Controls:

- Data requirements exist to force correction of errors and completion of critical fields before a transaction is accepted.
- CPS provides various reports to assist in verifying and balancing transactions.

User Agency Controls:

- 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.
- 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

DESCRIPTIONS OF TESTS OF CONTROLS
AND
RESULTS THEREOF

Using the Department's Description of System as the foundation for our review, we performed tests to determine compliance with policies and procedures, conducted interviews, performed observations, and identified specific procedures we considered necessary in the circumstances to evaluate the controls.

BILLING

EXISTING ENVIRONMENT

Objective: Procedures exist to ensure rates haves been established for services supplied to the entities.

Department's Control: Expenditures are coded to cost centers and assigned to services through a cost accounting model.

Tests Performed: Reviewed expenditures, cost accounting model, and interviewed staff.

Test Results: Expenditures were coded to cost centers and assigned to services through a cost accounting model.

We reviewed the expenditures, for July 2010 through April 2011, for the Statistical Services Revolving Fund (SSRF) and Communications Revolving Fund (CRF), noting each had been assigned a cost center.

No deviation noted.

Department's Control: Revenues for each service are compared to costs to determine the appropriateness of individual rates.

Tests Performed: Reviewed midyear review, rate forecast, and interviewed staff.

Test Results: Revenues for each service were compared to the costs to determine the appropriateness of the individual rates.

Annually, the Department conducted an analysis of the cost centers in order to forecast the rates for the upcoming fiscal year. Additionally, mid-year the Department conducted a review of the rates to determine appropriateness.

A more implicit review of the revenue and rates were conducted during the Department's Financial/Compliance Audit and the Statewide Single Audit. Significant deficiencies were identified during these audits, which are available on our website at http://www.auditor.illinois.gov.

No deviation noted.

Department's Control: Rates for many services are available in the BCCS Service Catalog.

Tests Performed: Reviewed BCCS Service Catalog and interviewed staff.

Test Results: The BCCS Service Catalog provided rates for many of the services available. However, our review indicated several of the Telecommunication rates listed had not been updated since September 2008.

Several of the Telecommunication rates had not been updated in the catalog and did not accurately reflect current rates.

Department's Control: In order to comply with federal requirements (A-87), an analysis is performed annually to determine the profit/loss for each service.

Tests Performed: Reviewed analysis and interviewed staff.

Test Results: Annually, the Department submitted the State of Illinois Statewide Cost Allocation Plan to the Federal Department of Human Services. The Allocation Plan outlined the Department's analysis of cost and revenue by service center.

According to the Department's analysis, they owed the federal Department of Human Services the following amounts.

Fiscal Year	CRF	SSRF
2009	$1.5 million	$1.7 million
2010	$1.5 million	$5.4 million

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

The Department's current cost allocation methodology caused the Department to accrue significant payback amounts to the federal government.

Objective: Procedures exist to help ensure accurate billings and billing details are provided to entities for which services are provided.

Department's Control: Documented billing practices and procedures are followed to ensure the accuracy of billing statements for both funds.

Tests Performed: Reviewed CRF Billing Overview, SSRF Information Services Division / Information Management System (ISD/IMS) Monthly Billing procedures, and interviewed staff.

Test Results: The Department had documented billing practices and procedures to ensure the accuracy of billing statements for the SSRF and CRF.

The Department had developed the SSRF ISD/IMS Monthly Billing procedure to assist staff with the monthly compilation of the billing. Reports were to be produced and reconciled against each

other to ensure the accuracy of the billings. In addition, an Edit Check was completed to ensure the completeness and accuracy of the monthly billings.

The Department had developed the CRF Billing Overview and Process, to guide staff with the monthly billing process.

Each month vendors or the Department provided data utilized to produce agency telecommunication billing. The CRF Billing Overview and Process provided instructions for the loading and reconciliation of data and billing.

No deviation noted.

Department's Control: Reports are produced and verified against each other and an edit check is completed to help ensure the completeness and accuracy of each billing.

Tests Performed: Reviewed SSRF and CRF monthly billing reports, agency billing detail, and interviewed staff.

Test Results: The Department produced various monthly reports to help verify the accuracy and completeness of each billing. Additionally, the Department completed an Edit Check for the monthly SSRF billing to promote accuracy.

SSRF
We reviewed the various billing reports and the Edit Check for December 2010 and January 2011, noting the Edit Check traced to the various billing reports. However, we did note that a process to ensure the accuracy of source information pertaining to PCs/laptops, servers, and software licenses did not exist.

We reviewed two agencies detailed billing for two months, noting the charges appeared appropriate.

CRF
We reviewed the monthly reconciliation and the tape approval form for December 2010 and January 2011, noting no exceptions.

The Department had a process to help ensure the accuracy of most services; however, a process to ensure billings accurately reflected some services had not been established.

Department's Control: Details on each billing are available on the invoices, through the EMS11 system for CRF billings, and on a SharePoint site for SSRF billings.

Tests Performed: Reviewed invoices, EMS11, SharePoint, and interviewed staff.

Test Results: Agencies monthly billings for the CRF and SSRF contained detailed information. In addition, EMS11 contained information related to the agencies CRF billings. Detailed information related to the agencies SSRF billings were maintained on SharePoint.

No deviation noted.

Objective: The CMS Fiscal Operation Policy ensures the collection of outstanding accounts.

Department's Control: The CMS Fiscal Operation Policy outlines the process for the collection of outstanding accounts.

Tests Performed: Reviewed Fiscal Operation Policy and interviewed staff.

Test Results: The Fiscal Operations Policy outlined the process for the collection of outstanding accounts.

The Policy provided the Department and the respective bureaus guidelines for the collection of accounts past due.

No deviation noted.

Department's Control: Delinquency letters are sent out based on the number of days an invoice is past due. An account aging analysis is sent out on a quarterly basis.

Tests Performed: Reviewed delinquency letters and interviewed staff.

Test Results: The Department sent delinquency notices to the agencies. We reviewed 25 delinquency notices as of May 2, 2011, noting the past due amount agreed to the Department's accounts receivable report.

On a quarterly basis, Administrative and Regulatory (A&R) Shared Services sent a quarterly report indicating the total charges and amount collected to date.

As of May 1, 2011, the Department had outstanding accounts receivable of $26,247,830 and $28,396,037 for the CRF and SSRF, respectively.

No deviation noted.

Objective: Procedures exist to ensure billing discrepancies are reviewed and adjusted as needed.

Department's Control: Requests for billing credits must be submitted in writing, and be properly approved.

Tests Performed: Reviewed Accounts Receivable CR/DR Memorandum (ARCM) Request Form, Fiscal Operations Policy, and interviewed staff.

Test Results: In the event the Department and agency determined an inappropriate charge occurred, a credit would be issued. We reviewed 50 SSRF and CRF issued credits, noting two CRF issued credits had not been properly approved by the Bureau.

Two issued credits were not properly approved.

Department's Control: Approved billing credits are sent to A&R Shared Services for processing and posting via an ARCM request form.

Tests Performed: Reviewed billing credits, fiscal policies, and interviewed staff.

Test Results: Approved billing credits were sent to the A&R Shared Services for processing and posting to agency accounts.

We reviewed 44 SSRF and CRF ARCM request forms sent to A&R Shared Services, noting 13 were not properly approved by accounting.

ARCM request forms were not always properly approved.

OVERALL CONCLUSION

The Department had a process to develop and review billings to user agencies. However, a process to ensure billings accurately reflected some services had not been established. The Department should develop a process to ensure billings accurately reflect services rendered. In addition, the Department should develop an appropriate methodology to reduce the paybacks to the federal government. The Department should also ensure all billing credits are properly approved and update Telecommunication rates in the catalog to reflect current rates.

CHANGE MANAGEMENT

EXISTING ENVIRONMENT

Per the Department's Description of System – "The Department's change management controls the Department managed infrastructure, including hardware and software in the mainframe, and desktop environments, and the State of Illinois Network environment. The change management process does not apply to application changes."

Auditor's Note: Changes in areas not covered by these change management controls, that are relevant to the review, were tested and incorporated in the following areas:

- Accounting Information System
- Central Payroll System
- Central Inventory System
- Central Timekeeping and Attendance System
- LAN Applications
- Web Applications

Objective: Policies exist to provide that only authorized and documented changes are made to the Department's production environment.

Department's Control: The Department's Change Management Policy and the Remedy Change Management Guide describe the change initiation, documentation standards, approval process, and post implementation review process.

Tests Performed: Reviewed the Change Management Policy, Remedy Change Management Guide, and Change Tickets.

Test Results: The Department developed the Change Management Policy (Policy), effective December 15, 2008, and the BCCS Remedy Change Management Guide (Guide), last reviewed December 10, 2010. The Policy and Guide provided guidance on documenting changes and entering/tracking changes in the Remedy Action Request System (System).

According to the Policy, "infrastructure changes for all technology platforms and systems of the CMS/BCCS managed infrastructure and environment" were to follow the Policy. The Policy defined a change as "any alteration to the state or configuration of any production software or hardware under BCCS management and support. This would include adding new functionality, repairing or removing functionality."

The Guide stated the purpose was to "standardize the actions, behaviors and responsibilities related to the processing of Change Requests for utilizing the Remedy Change Management application."

The Guide defined the authorization and approval processes, roles and responsibilities, emergency changes, and user involvement for specified changes. The Guide stated testing plans were only required for high impact changes and the level of testing was the responsibility of the Shared Services Team.

We reviewed 25 Change tickets for the required information, noting no exceptions.

No deviation noted.

Department's Control: Requests for changes (system maintenance and vendor maintenance) follow the Change Management Policy and Guide.

Tests Performed: Interviewed staff.

Test Results: Requests for changes followed the Change Management Policy and Guide.

No deviation noted.

Department's Control: A Request for Change (RFC) is required to be completed for all production changes.

Tests Performed: Reviewed Change Management Guide and interviewed staff.

Test Results: An RFC was required to be completed for production changes.

No deviation noted

Department's Control: The Remedy Action Request System is utilized to track all RFCs to the Department's environment.

Tests Performed: Reviewed the Change Management Policy and interviewed staff.

Test Results: The Department utilized the Remedy Action Request System to track RFCs to the Department's environment.

No deviation noted.

Department's Control: Requests for Change (RFC) are based on the Category, Type and Item (CTI).

Tests Performed: Reviewed Remedy System, change tickets, and interviewed staff.

Test Results: Requests for changes were based on CTI.

We tested 25 tickets, noting each ticket had CTI fields completed.

No deviation noted.

Department's Control: The Remedy Action Request System routed the changes to the appropriate staff based on CTI and documents the approvals and authorizations for the requested changes.

Tests Performed: Reviewed Remedy System, change tickets, and interviewed staff.

Test Results: The Remedy Action Request System routed changes to the appropriate staff based on CTI, and documented approvals and authorizations.

We reviewed 25 change tickets, noting they had been appropriately approved.

No deviation noted.

Department's Control: High Impact Changes require that a test plan be attached to the RFC, if applicable.

Tests Performed: Reviewed Change Management Guide and change tickets.

Test Results: The Change Management Guide required testing documentation for high impact changes be attached to the change ticket. However, the Guide did not document the requirements or required documentation.

High impact changes required a test plan to be attached to the RFC.

We reviewed ten high impact changes, noting each had a test plan attached.

No deviation noted.

Department's Control: High Impact Changes testing documentation is maintained by the applicable area.

Tests Performed: Reviewed Change Management Guide and interviewed staff.

Test Results: The Change Management Guide required testing documentation for high impact changes be attached to the change ticket. However, the Guide did not document the requirements or required documentation. The requirements for the documentation and the depth of testing were the responsibility of the Shared Services Teams which submitted the request.

We reviewed ten high impact changes, noting each had test documentation attached.

We requested from the Shared Services Teams the applicable policies and procedures related to the documentation and testing requirements of changes. However, we noted most Shared Service Teams did not have policies and procedures.

The quality of the documentation was inconsistent due to the lack of established and defined testing and documentation requirements.

Department's Control: Post implementation reviews are conducted on all emergency changes and scheduled changes which cause a major outage.

Tests Performed: Reviewed Change Management Guide, change tickets, and interviewed staff.

Test Results: The Change Management Guide stated a post implementation review was to be conducted on emergency changes and scheduled changes which caused a major outage. The Guide indicated an Incident Form or information from the help desk ticket was to be attached to the change. However, the Guide did not document the information which was to be included or the communication requirements with the business owner.

We reviewed 14 emergency change tickets for post implementation reviews, noting information was documented in the worklog; however since the procedures did not document what information should be included in a post implementation review, we could not assess compliance.

In addition, we reviewed the two scheduled changes which caused a major outage (MORT) during the review period, noting both had a post implementation review documented in the worklog.

The quality of the documentation was inconsistent due to the lack of established and defined post implementation review requirements.

Department's Control: Planned (low, medium, and high impact) changes are reviewed by the technical approver (Shared Services Manager) and both reviewed and scheduled by the business approver (Enterprise Change Management (ECM) Team). In addition, medium and high impact changes are reviewed by the Change Advisory Committee.

Tests Performed: Reviewed Change Management Guide, change tickets, and CAC meeting minutes.

Test Results: The Change Management Guide indicated each level of approval was responsible for reviewing specific items of a request. As each level was approved, Remedy would indicate the next level of approval needed.

Additionally, the Technical and ECM approvers were to review each request to ensure the required documentation was attached.

We reviewed 25 tickets for proper approvals, noting each was appropriately approved.

In addition, we reviewed 25 high, medium and low impact tickets, noting:

- 21 high and medium impact tickets reviewed were in CAC meeting minutes.
- Four low impact tickets were included in the Completed Change Report.

No deviation noted.

Department's Control: Changes are communicated to users via Change Advisory Committee Meetings and reports located on the ECM SharePoint Site.

Tests Performed: Reviewed SharePoint site and meeting minutes.

Test Results: Changes were communicated to users through CAC meetings and reports on the ECM SharePoint site.

The ECM SharePoint site maintained various reports to inform the users:

- Change Advisory Committee Meeting Minutes
- 30 Day Outage Report by Agency
- Change Detail Report (Next 14 Days)
- Enterprise Change Schedule (Next 90 Days)
- Overdue Change Report.

We reviewed the reports and meetings from the ECM SharePoint Site for July 2010 - January 2011, noting information related to changes.

Each agency had access to the SharePoint site to view reports and meeting minutes. Emails were sent to all agencies identifying the changes to be discussed at the upcoming CAC meeting and the email included a link to the SharePoint site.

No deviation noted.

Department's Control: High Impact Changes require a back-out plan be attached to the RFC for use in the event of a disruption.

Tests Performed: Reviewed Change Management Guide and high impact change tickets.

Test Results: The Change Management Guide stated high impact changes required a back-out plan be attached to the RFC. However, the Guide did not document what information should be included in a back-out plan.

We reviewed ten high impact changes, noting each had a back-out plan attached.

The quality of the documentation was inconsistent due to the lack of established and defined back-out plan requirements.

Objective: Procedures exist to provide that emergency changes are documented and authorized timely.

Department's Control: All emergency changes are required to complete the standard documentation outlined in the Change Management Policy and the Remedy Change Management Guide.

Tests Performed: Reviewed the Change Management Policy, Change Management Guide, and emergency change requests.

Tests Results: According to the Change Management Policy, an emergency was defined as "a change that does not present notification to the formal process in advance of implementation." Emergency changes will only be acceptable in the event of a system failure or the discovery of security vulnerability." The Policy also stated "all emergency changes will be reviewed and documented."

The Change Management Guide defined emergency changes as unscheduled changes. Emergency changes were only acceptable in the event of a system failure or the discovery of security vulnerability. Emergency changes were to follow all change management processes except they may be implemented in advance of approval in order to correct the failure in a timely manner.

We reviewed 14 emergency tickets, noting one did not have the appropriate level of approval.

One ticket was not appropriately approved.

Department's Control: All emergency changes are reviewed by the technical and business approver post implementation.

Tests Performed: Reviewed emergency change tickets and interviewed staff.

Test Results: Emergency changes were to be reviewed by the technical and business approvers.

We reviewed 14 emergency change tickets for appropriate approvals, noting one did not have the appropriate level of approvals.

One emergency ticket was not appropriately approved.

Department's Control: Emergency changes are communicated to users post implementation via the Change Advisory Committee Meeting.

Tests Performed: Reviewed CAC meetings minutes.

Test Results: Emergency changes were communicated to users through the CAC meetings.

We reviewed 14 emergency change tickets, noting they were included in the CAC meeting minutes.

No deviation noted.

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:

- Develop guidelines and requirements to promote standardization and consistency in testing, documentation, post implementation reviews, and back-out plans.
- Ensure all tickets are appropriately completed and approved.

CONTINUOUS SERVICE

EXISTING ENVIRONMENT

Objective: The Department has policies and procedures in place to help safeguard the availability of critical Department-managed resources.

Department's Control: A disaster recovery policy exists.

Tests Performed: Reviewed Recovery Action Plan and Recovery Methodology.

Test Results: The Department developed the State of Illinois, CMS/BCCS, Recovery Activation Plan (Plan), with a revision date of March 2, 2011.

The purpose of the Plan was to provide instructions and actions required when recovering CMS/BCCS computing facilities and services." The Plan was limited to events affecting CMS/BCCS computing facilities and services.

The Plan provided guidance regarding the assessment of damage to obtaining the assistance of the recovery services provider.

In addition, the Department developed the State of Illinois, Department of Central Management Services, Bureau of Communication and Computer Services, Recovery Methodology (Methodology), effective January 1, 2010.

The purpose of the Methodology was to provide direction and recommendations to "produce effective and detailed instructions" for the recovery of systems and services.

The Methodology provided guidance to agencies in conducting a Business Impact Analysis, identifying critical applications, and defining recovery time objectives.

The Methodology outlined two criteria for determining the classification of an application; recovery category and recovery stage.

The categories were defined as:

- Category One-Human Safety-applications which have a direct impact on the lives of citizens and employees.
- Category Two-Welfare/Human Safety-applications which have a direct impact on the well-being of citizens and employees.
- Category Three-Non-welfare/Human Services-a human resource service which has a direct impact on the well-being of citizens and employees.
- Category Four-Administrative Functions and Processes-applications which support state processes.
- Category Five-Specific Agency Functions and Processes-maintenance of specific processes.

Additionally, the Methodology identified the recovery time objective (maximum time agencies can be without resources) for each recovery stage.

- 0 to 72 hours -- Stage Zero.
- 72 to 168 hours -- Stage One.
- > 168 hours -- Stage Two.

The Methodology stated all Stage Zero, Category One applications would be recovered first. After the recovery of the Stage Zero applications, all remaining Category One applications would be recovered. In the event there was additional space, Category Two applications would be recovered.

No deviation noted.

Department's Control: Disaster recovery plans are tested periodically for critical IT assets.

Tests Performed: Reviewed Recovery Activation Plan, Recovery Methodology, exercise documentation, critical application listing, and interviewed staff.

Test Results: The Department conducted testing of disaster recovery plans at the alternate recovery data processing facility.

The Department conducted testing of its computing facility and mainframe services at the alternate recovery data processing facility in September 2010.

Our review of exercise documentation indicated four agencies, including the Department, participated in the exercise and tested the recovery of fourteen Stage Zero, Category One applications.

No deviation noted.

Department's Control: The Department has an alternate recovery site.

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

Test Results: The Department had a contract with an out of state disaster recovery service provider to provide recovery services in the event of a major regional disaster with prolonged outages.

According to the contract, the vendor would be required to provide mainframe recovery services, resources, personnel, and other services in order to continue the required processing capabilities.

The contract will expire in December 2011.

The Department had also contracted with a vendor for "highly available alternate data center, failover site services and other services as needed." The contract provided floor space, electricity, security and telecommunication services.

The contract indicated it is the Department's responsibility to provide hardware and software in order to recover.

No deviation noted.

Objective: The Department communicates recovery responsibilities to appropriate users and responsible parties.

Department's Control: The Department periodically conducts meetings and initiates audio conferences to keep appropriate users informed of procedures and the status of support services.

Tests Performed: Reviewed meeting and audio conference agendas and interviewed staff.

Test Results: The Department conducted the Illinois Digital Government Summit and two audio conferences during the review period, which provided information on support services and new trends.

No deviation noted.

Department's Control: A disaster recovery communications portal (SharePoint site) contains relevant information such as standards and templates as well as critically important information during a rehearsal.

Tests Performed: Reviewed portal and interviewed staff.

Test Results: The Department maintained a SharePoint site which contained recovery documentation.

Additionally, specific agencies had access to a secure section, in which they could post their recovery information.

No deviation noted.

Objective: Procedures exist to assist maintaining the integrity of critical data and system backups.

Department's Control: An inventory of backups and their location is maintained.

Tests Performed: Interviewed staff.

Test Results: Library Services maintained an inventory of backup tapes and their respective location.

See the Library Services section for additional information.

No deviation noted.

Department's Control: Backups are stored at an off-site location.

Tests Performed: Reviewed backups maintained off-site and interviewed staff.

Test Results: Backups were stored at an off-site location.

We reviewed a sample of 56 tapes which were to be located at the off-site storage location, noting 11 tapes were actually located at the CCF.

Eleven tapes were not stored in the proper location.

Department's Control: Backups are utilized during the annual recovery testing.

Tests Performed: Reviewed exercise documentation and interviewed staff.

Test Results: The Department conducted its annual recovery testing in September 2010. The agencies which participated in the recovery testing utilized backups for the restoration of their respective applications.

No deviation noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. However, the Department should continue to pursue avenues in providing and improving their recovery capabilities. Additionally, it is imperative the Department continue to work with the user agencies to ensure appropriate recovery services are available.

HELP DESK

EXISTING ENVIRONMENT

Customer Service Center (CSC)

Objective: Policies exist to report and act upon issues and incidents.

Department's Control: The Incident Ticket procedures document the process by which the CSC enters incident calls from customers in Remedy Help Desk Case module.

Tests Performed: Reviewed procedures and Help Desk tickets.

Test Results: The Department had developed the IT Incident Management Processing Incident Tickets procedure, dated April 29, 2010. The procedures provided guidance for the opening, monitoring, and closing of IT help desk tickets into the Remedy System. The procedures also included guidance related to the monitoring and resolving/closing service desk tickets.

We reviewed 25 help desk tickets for completeness, noting they had been completed properly.

No deviation noted.

Department's Control: The Expense Management System (EMS) manual documents the process by which the Telecom Provisioning Unit enters the customer service requests in EMS.

Tests Performed: Reviewed Methods and Procedures and service requests.

Test Results: The Department had developed the EMS Logger and Screener Methods and Procedures, dated August 25, 2009, to provide guidance to users regarding establishing a record in EMS.

EMS allowed the user to establish a record using the Telecommunications Service Request (TSR), Telecommunications Data/Intercity Service Request (TDR), Paging Service Request (PSR), and Wireless Service Request (WSR) Order Forms submitted by an agency and establish an EMS Request number (PO number). The Procedures provided steps for entering data into EMS and the fields required to be populated.

We reviewed 25 service requests in EMS, noting they had been properly completed and approved.

No deviation noted.

Department's Control: The Enterprise Service Request (ESR) procedures for IT MAC (Move/Add/Change) document the process by which the IT Service Desk enters customer service requests in Remedy Change Request module.

Tests Performed: Reviewed procedures, service requests, ESRs, and ESR Addendums.

Test Results: The Department developed the Customer Service Center Procedures for Processing Centralized ESRs, dated November 20, 2009, to guide the IT MAC process.

The Procedures listed steps for processing ESRs; such as determining the completeness and verifying the appropriate IT Coordinator had submitted the request. Additionally, the Procedures provided guidance for entering all of the information from the ESR or ESR Addendum into Remedy.

We reviewed 34 service requests to ensure the applicable ESR or ESR Addendum was attached, noting no exceptions. Additionally, we reviewed the 34 service requests to ensure they had been appropriately completed noting one service request did not have the region field completed.

In addition, we reviewed 44 ESRs, noting 38 were not properly completed; however all were properly approved. According to the ESR Addendum instructions, the Governor's Procurement Criteria and the Business Justification fields were required to be completed; however, they were not.

Not all service requests and ESRs were completed properly.

Department's Control: The Non-routine procedures document the process by which the Telecom Project Unit enters the request information in Remedy Provisioning module.

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

Test Results: The Non-Routine Provisioning Procedures last reviewed December 2, 2010, provided procedures for processing TSRs for non-routine telecommunication projects.

We reviewed the two non-routine provisioning tickets during the review period, noting one did not have the required attachment.

One non-routine provisioning ticket was not properly completed.

Objective: Policies exist to ensure only authorized requests are made.

Department's Control: Agency management delegates, in writing, an IT and Telecom coordinator(s) authorized to expend funds.

Tests Performed: Reviewed service requests and interviewed staff.

Test Results: Each agency head delegates, in writing, a Telecommunications and IT coordinator(s) authorized to expend funds.

We reviewed the Telecommunication Coordinators from 25 service requests (TSR, TDR, WSR, PSR) and noted all were properly authorized by the respective agency coordinator.

We also reviewed 25 IT Coordinators, noting all were properly authorized by the respective agency coordinator.

No deviation noted.

Department's Control: CSC verifies submitter is authorized.

Tests Performed: Reviewed Telecommunication Requests, ESRs, and interviewed staff.

Test Results: The CSC verified requests were submitted by an authorized coordinator.

We reviewed 25 service requests (TSR, TDR, WSR, PSR) and 44 ESRs, noting they had been submitted by an approved Telecommunication or IT Coordinator.

No deviation noted.

Department's Control: The Telecom Service Desk has documented Methods and Procedures (M&Ps) for voice mail password resets.

Tests Performed: Reviewed Methods and Procedures, Remedy tickets, and interviewed staff.

Test Results: The Telecom Repair: Reset Voice Mail from E-mail Request Methods and Procedures issued December 10, 2010, provided guidance regarding voice mail password resets.

The Procedures stated the Telecommunications Help Desk must receive a request for voicemail resets from an authorized agency Telecommunications Coordinator. Help Desk must then send a follow-up e-mail to the requesting agency Telecommunication coordinator. Additionally, a Remedy ticket was to be created for each request.

We reviewed four Remedy tickets completed after the issuance of the Procedures, noting the requesting email was included and an authorized Telecommunication Coordinator had sent the request.

No deviation noted.

Objective: The Department monitors, logs and tracks calls, incidents and service requests.

Department's Control: The Avaya phone system and its internal functionality provides the tools and means by which the number of customer calls are logged and tracked.

Tests Performed: Interviewed staff.

Test Results: The Avaya Phone system allowed management to monitor the performance of the individuals taking the calls and the calls themselves. Additionally, the manager could monitor how many calls were coming in, how long it took to answer a call, and how many calls were abandoned. Based on this information, the managers could make real-time decisions.

No deviation noted.

Department's Control: The Remedy Help Desk Case Module and its internal functionality provides a system generated Case Number and the tools and means by which customer incidents are logged, tracked, and updated with supporting documentation through resolution.

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

Test Results: The Remedy Help Desk Case Module logged, tracked and maintained documentation. Additionally, Remedy generated a case number for each ticket.

We reviewed 25 help desk tickets, noting each had a case number and contained supporting documentation.

No deviation noted.

Department's Control: The EMS system and its internal functionality provides a system generated Request Number and the tools and means by which all Telecom service requests are logged, tracked, scheduled with external vendors and/or internal teams and updated through completion.

Tests Performed: Reviewed Telecom service requests and interviewed staff.

Test Results: EMS generated a request number, logged, tracked and scheduled requests.

We reviewed 25 service requests in EMS, noting no exceptions.

No deviation noted.

Department's Control: The Remedy Change Request module and its internal functionality provides a system generated Change Request Number and the tools and means by which customer incidents are logged, tracked, scheduled with external vendors and/or internal teams and updated through completion.

Tests Performed: Reviewed service requests and interviewed staff.

Test Results: The Remedy Change Request Module generated a change request number, logged, tracked, and scheduled service requests.

Tasks were created within each ticket and assigned to each individual team that was needed to complete the request in the sequence in which the work was to be done. These tasks were created, assigned, and scheduled by the request owner. Each team updated their own tasks in the individual task work logs.

We reviewed 34 service request tickets, noting 33 had been completed appropriately.

One service request was not completed appropriately.

Department's Control: All Help Desk Cases and Service Requests are to be properly documented and updated through completion detailing resolution steps and work performed.

Tests Performed: Reviewed Help Desk cases, service requests, and interviewed staff.

Test Results: Help Desk cases and service requests were documented and updated as steps were performed.

We reviewed 25 Help Desk tickets and 34 service requests, noting the work conducted had been documented in the work logs.

No deviation noted.

Department's Control: ESRs are assigned tasks for engaging and tracking external vendors and internal teams.

Tests Performed: Interviewed staff.

Test Results: ESRs were assigned tasks in order to engage and track external vendors and internal teams.

Separate tasks were created within each Remedy ticket and assigned to each team that was needed to complete the request in the sequence in which the work must be done. These tasks were created, assigned, and scheduled by the request owner. Each team updated their own tasks in the individual task work logs.

No deviation noted.

Department's Control: The Remedy Provisioning module provides the tools and means by which Non-routine requests are logged, tracked and updated to obtain the necessary procurement approvals.

Tests Performed: Reviewed non-routine requests.

Test Results: The Remedy Provisioning module logged, tracked and updated requests.

We reviewed two non-routine requests, noting one did not have the required attachment.

One non-routine request was not completed appropriately.

Objective: The Department classifies and prioritizes incident calls and new service requests to ensure timely and satisfactory customer service.

Department's Control: The Avaya phone system and its internal functionality provides the ability to classify and prioritize calls via announced menu options, "blind" options, and personnel changes via skill based routing as necessary.

Tests Performed: Reviewed website and interviewed staff.

Test Results: The Avaya phone system provided a means to classify and prioritize calls via menu options.

The Help Desk menu allowed an individual to enter an option based on their needs. Calls were then routed based on the menu selections.

No deviation noted.

Department's Control: The Remedy Help Desk Case module uses category, type and item (CTI) to identify classification and assignment to appropriate individuals/groups.

Tests Performed: Reviewed Help Desk tickets and interviewed staff.

Test Results: The Remedy Help Desk Case Module utilized category, type and item to classify and assign tickets.

We reviewed 25 help desk tickets, noting each had a category, type and item assigned.

No deviation noted.

Department's Control: The priority field in Remedy Help Desk Case identifies the priority of the incident per user agency request.

Tests Performed: Reviewed Help Desk tickets and interviewed staff.

Test Results: The Remedy Help Desk Case identified the priority of the incident based on the user's request.

The priority levels were Urgent, High, Medium, and Low. Urgent tickets would be worked continuously unless otherwise agreed upon. High priority tickets were time sensitive and/or a reoccurring problem that had indirect impact to the end user and an interim solution or workaround was available. Medium priority tickets affected users ability to perform normal

operations, inhibits productivity, but were not time sensitive. Low priority tickets were if users ability to perform normal operations or there was a work around available.

We reviewed 25 Help Desk tickets noting, each had been prioritized.

No deviation noted.

Department's Control: User agencies have the ability to verbally request the level of priority of their reported incident or by designating priority on the Telecom and IT service request forms.

Tests Performed: Interviewed staff.

Test Results: Agencies had the ability to request the priority level, however; the CSC had the ability to reassign the level if they felt that it was unreasonable due to scheduling conflicts or if a vendor needed to be involved. The CSC would work with the agencies regarding the priority levels.

No deviation noted.

Department's Control: CSC obtains customer confirmation/satisfaction before closing incidents.

Tests Performed: Interviewed staff.

Test Results: The IT Help Desk obtained customer confirmation on incidents when a vendor was responsible for resolving a problem. The work log was updated accordingly with the applicable information.

The Telecommunication Help Desk obtained customer confirmation on incidents before closing; except voice mail resets, which were completed via email.

No deviation noted.

Department's Control: IT Service Desk obtains customer confirmation/satisfaction before closing ESRs/addendums.

Tests Performed: Interviewed staff.

Test Results: The IT Service Desk obtained customer confirmation before closing the ESR.

If contact was made with the customer via the phone, the customer's comments were recorded in the work log of the confirmed customer satisfaction task. If contact was made with the customer via email, the reply was copied into the work log of the confirmed customer satisfaction task.

This information was reviewed by management only when there were problems. If the customer stated the ESR was not properly worked or completed, a new task was created for the work that

was not properly completed. The confirm customer satisfaction task was closed as unsuccessful, and a new task was created.

No deviation noted.

Objective: The Department communicates information regarding services to user agencies.

Department's Control: User agencies have the ability to call back for updates on incidents by referencing the assigned Remedy Case Number provided by the CSC when reporting an incident, or they can track current status if they have Remedy access.

Tests Performed: Interviewed staff.

Test Results: Agencies had the ability to call the CSC regarding an incident. The agency would need the Remedy case number when requesting an update.

Additionally, agencies, with access, could track the status of the incident via Remedy.

No deviation noted.

Department's Control: Telecom user agencies have the ability to call back for updates on service requests referencing the EMS Request Number or their agency assigned control number, or they can track current status if they have EMS access.

Tests Performed: Interviewed staff.

Test Results: The agencies had the ability to contact the Help Desk to obtain the status of their service request. The agency would need the EMS Request Number or the assigned control number.

Additionally, agencies, with access, could track the status of the request, via EMS.

No deviation noted.

Department's Control: IT user agencies have the ability to call back for updates on service requests referencing the assigned Remedy Change Request Number or they can track current status if they have Remedy access.

Tests Performed: Interviewed staff.

Test Results: IT user agencies had the ability to call the Help Desk to obtain an update on the status of the request. The Help Desk would request the assigned Remedy Change Request Number.

Additionally, agencies, with access, could track the status of the request, via Remedy.

No deviation noted.

Department's Control: If IT user agency has Remedy access, the Change Request Number and status updates are automatically sent to customer upon CSC entering their request, during status changes of the request, and at resolution.

Tests Performed: Interviewed staff.

Test Results: IT user agencies were sent the change request number and automatic updates until resolution.

No deviation noted.

Objective: Procedures exist to escalate unresolved incidents.

Department's Control: The CSC has Methods and Procedures (M&Ps) for CSC incidents based on specified criteria defined by management.

Tests Performed: Reviewed procedures.

Test Results: The Management Escalation Procedure CSC Telecommunications Service Desk dated March 17, 2008, provided guidance based on criteria related to extensive system failure and critical calls from the Governor's office, Director's office, impact on public safety, or contact from one of the listed critical agencies.

Department management would determine if the incident was significant enough to warrant contacting the Department's Emergency Management Coordinator.

No deviation noted.

Department's Control: The IT Service Desk has M&Ps for management and Very Important Person (VIP) ticket escalations and MORT (Major Outage Response Team) procedures.

Tests Performed: Reviewed procedures.

Test Results: The VIP Remedy Procedures, dated July 10, 2009, and the Management Escalation Procedures, dated July 7, 2009, provided guidance to IT Service Desk staff on the handling of calls.

The VIP Remedy Procedures provided steps for handling tickets by verifying the VIP information, prioritizing the tickets as High/Urgent; depending on situation, notifying the Shared Service team manager and keeping track of the ticket until resolution.

According to the Management Escalation Procedures, they were to be used for the escalation of problems. The Procedures listed the criteria for an escalation that affected a business critical application.

Also listed were the responsible party, which group to contact, initial notification, incident updates and resolution and emergency management criteria.

No deviation noted.

Objective: External vendors and internal team performance are monitored.

Department's Control: Monthly reports are generated from Remedy and EMS to track and monitor vendor performance for Telecom Services.

Tests Performed: Reviewed vendor performance reports and interviewed staff.

Test Results: Monthly reports were generated from Remedy and EMS in order to reconcile vendor performance.

No deviation noted.

Department's Control: For Telecom Services, the Department and vendors reconcile misses against contractual intervals. Based on reconciliation, penalty amounts are calculated and deducted from the monthly maintenance invoice in accordance with the contract specifications.

Tests Performed: Reviewed vendor performance reports and interviewed staff.

Test Results: The Department and the vendors reconciled missed targets against contractual intervals. Penalties were calculated based on response time, depending on the contract language.

We reviewed the vendor performance reports for July through December 2010, noting the reports tracked the total repairs missed, the percent of repairs completed, and the repairs by priority; urgent, high, medium, and low. There were also penalty calculations for missed targets, if it was part of the contract with the respective vendor.

No deviation noted.

Objective: Trends and recurring problems are monitored.

Department's Control: The Telecom Help Desk staff asks all callers if the reported incident is chronic. If identified as a chronic issue, procedures exist to pull history report and escalation.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: The Customer Service Center, Telecom Methods & Procedures: Report- All Repair Locating Remedy Tickets Methods and Procedures, dated January 26, 2011 provided guidance for "checking of possible chronic problems, duplicate tickets and/or historical reports."

Management demonstrated in Remedy how to pull a history report by pulling up a ticket and selecting the related items tab and then selecting the search criteria from the drop down box, this would show related tickets and associated history.

Management stated escalating a chronic issue would follow the Abridged Remedy Help Desk Procedures.

No deviation noted.

Department's Control: The IT Service Desk managers review multiple reporting sources (Remedy metrics, Avaya phone metrics) from the CSC Quality Assurance Team to identify spikes in service demands, call volumes, and ticket counts. Corrective actions and resource allocations are implemented as needed at the IT Service Desk.

Tests Performed: Interviewed staff.

Test Results: The IT Service Desk managers reviewed reports from various sources to identify spikes in service demands, call volumes, and ticket counts.

The Avaya Phone system allowed management to view the performance of the individuals taking the calls and the calls themselves. Calls could be monitored in real-time. The information that could be reviewed was who was on a call, how long the call was taking and who was away from their workstation and the reason, etc. Managers could also determine how many calls come in, how long it takes to answer a call, how many calls were abandoned, etc. Managers, also could make real-time decisions based on call volumes/trends/problems.

According to Management, trends were watched not only for the type of calls but also for the trends in the individuals taking the calls.

For resource allocation Remedy reports were to determine current workloads in areas such as pending asset updates, customer satisfaction tasks, and ESRs. Avaya would send alerts to management when specific call queue activity was reached. Management was then able to make staff reassignments appropriately to re-distribute staff assignments.

Reports on workloads also helped to monitor acceptable levels so that tasking assignments could be distributed between service desk agents with the highest available times. Weekly and monthly reports were also run to track trends in call volumes and activities and staff assignments were adjusted accordingly.

No deviation noted.

Customer Management Center (CMC)

Objective: Procedures exist to report and act upon issues and incidents.

Department's Control: Methods and procedures are available to assist staff members in providing support and resolving network issues.

Tests Performed: Reviewed procedures.

Test Results: The CMC: Remedy Ticket Procedure, last reviewed October 2008, provided guidance to CMC staff on "entering and working Illinois Century Network (ICN) Remedy tickets." The Procedures provided the staff with a script to follow when answering an issue and entering the issue into ICN Remedy.

No deviation noted.

Objective: The Department monitors, logs and tracks calls, incidents and service requests.

Department's Control: CMC staff use Remedy to document incidents and service requests.

Tests Performed: Reviewed CMS Remedy tickets and ICN Remedy tickets.

Test Results: The CMC staff utilized CMS Remedy and ICN Remedy to document incidents and service requests.

We reviewed 25 CMS Remedy Help Desk tickets noting they had been properly completed.

In addition, we reviewed 25 ICN Remedy tickets, noting the tickets were generally completed.

No deviation noted.

Department's Control: Remedy ticket logs are used to document the incident and actions taken to bring the incident to resolve.

Tests Performed: Reviewed ICN Remedy tickets.

Test Results: Remedy ticket logs were used to document incidents and actions taken to resolve an issue.

We reviewed 25 ICN Remedy tickets, noting the work logs had appropriate information regarding the incident.

No deviation noted.

Objective: Procedures exist to escalate unresolved incidents.

Department's Control: The CMC has established procedures for managing the escalation of incidents.

Tests Performed: Reviewed procedures.

Test Results: The CMC Methods and Procedures: Managing Escalations and Carriers, dated May 20, 2010, provided procedures for escalating incidents.

According to the Procedures, an escalation would occur when there was either no significant level of progress on an issue or "per the hourly matrix based on the business rules."

The Procedures documented the priority levels; low, medium, high, urgent and chronic, along with the action to be taken.

No deviation 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 ensure all help desk tickets, service requests, ESRs, ESR Addendums, and provisioning tickets are properly completed.

INFORMATION ASSURANCE

EXISTING ENVIRONMENT

Objective: The Department defines and documents IT policies for security.

Department's Control: The Department's security policies have been established and posted to the publically accessible web site http://bccs.illinois.gov/it_policies.htm.

Tests Performed: Reviewed policies, procedures, standards, memos, Business Reference Model (BRM), background checks, revocation requests, laptops, inventory listing, Remedy Asset System, and interviewed staff.

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

Information Technology Policies

- Data Classification Policy, revised January 1, 2010
- Enterprise Desktop/Laptop Policy, effective December 15, 2008
- General Security for Statewide IT Resources Policy, revised January 1, 2010
- General Security for Statewide Network Resources Policy, revised January 1, 2010
- IT (Information Technology) Recovery Policy, effective October 1, 2009
- Recovery Methodology, effective January 1, 2010
- IT Resource Access Policy, effective December 1, 2007
- Laptop Data Encryption Policy, revised January 1, 2010
- Midrange Backup Policy (TSM Shared Services), effective December 1, 2007
- Statewide CMS/BCCS Facility Access Policy, revised January 1, 2010

General Policies

- Change Management Policy, Effective December 15, 2008
- Data Breach Notification Policy, revised January 1, 2010
- Action Plan for Notification of a Security Breach, effective August 31, 2007
- Electronically Stored Information Retention Policy, effective February 15, 2009
- IT Governance Policy, effective December 15, 2008
- Mobile Device Security Policy, effective October 1, 2009
- Wireless Communication Device Policy, revised January 1, 2010

We reviewed the policies and implementation practices and found the following:

- The policies contained sections requiring the designation of responsibility to implement, monitor, audit, track, and validate compliance with the policies and procedures; however, we found implementation and monitoring processes at the Department to be lacking.
- The Data Classification Policy provided guidelines for data owners to classify their data into one of three categories; Public, Official Use Only, or Confidential. However, the Department had not classified its own applications or data.

- The Laptop Data Encryption Policy required all laptops deployed after the effective date of the Policy be equipped with full disk encryption; however, the Department had deployed several laptops without full disk encryption software.
- The Statewide CMS/BCCS Facility Access Policy stated it was applicable to "any individual requiring physical access privileges to a CMS/BCCS facility located anywhere in Illinois." The Policy stated, "a security screening review (background check) will be conducted on any individual requesting unescorted physical access to CMS/BCCS facilities. Access will be delayed until the review is completed." During the review period, the Bureau had three new employees. We requested the background checks, noting two of the three individuals did not have background checks completed before employment began and access was granted.

According to Department management, the Department's Security & Compliance Solutions staff lacked the authority to require the Department's other divisions to comply with the various security policies.

We requested from the Department the procedures and assigned personnel for implementing the various policies. According to Department management, they were responsible for informing and publishing the policies; however, each user agency must develop their own procedures and ensure compliance.

Upon identification of the security weaknesses, we discussed the results of our testing and the security effects with Department management. Department management indicated that many of the deficiencies were the result of a lack of staff. Over the past four fiscal years the Department had lost approximately 26.8% of their staff.

Additionally, the Department stated they were in the process of installing encryption software on the laptops in question. As for the classifying their data as outlined in the Data Classification Policy, the Department believed "it is not realistic to be in compliance with the policy in the near future. This policy therefore is under review."

Although the Department had developed policies and procedures designed to provide a security strategy and framework, all provisions had not been effectively developed or implemented.

Objective: The Department communicates security obligations to users and responsible parties.

Department's Control: Security summits are hosted by the Department to share relevant cyber security topics of interest to State government security professionals and other IT professionals.

Tests Performed: Reviewed agendas, proclamation, and interviewed staff.

Test Results: On October 27, 2010, the Department hosted a Cyber Security Summit, which addressed several security topics. The Summit was available to Agency CIOs, IT Managers, Security Officers and Agency staff.

No deviation noted.

Department's Control: Security awareness month educational materials are distributed to user agency IT management.

Tests Performed: Reviewed security awareness materials, memos, and interviewed staff.

Test Results: The Department distributed security awareness material to user agencies.

No deviation noted.

Department's Control: Public facing website disseminates awareness and educational information and is accessible at http://bccs.illinois.gov/security/awareness.htm.

Tests Performed: Reviewed website and interviewed staff.

Test Results: The Department's website contained security awareness and educational information.

We reviewed the website noting it contained posters relating to:

- Keyboard Hands Security,
- Security Survivor,
- Global Security, and
- Strong Passwords.

No deviation noted.

Department's Control: Notification of newly published or significantly modified cyber security policies is achieved through inter-office email notifications coordinated by Agency Relations.

Tests Performed: Interviewed staff.

Test Results: Notification of new or modified cyber security policies were to be communicated by Agency Relations to user agencies.

During the review period, there were no new or modified policies which required notification.

No deviation noted.

Department's Control: Pertinent information is disseminated to appropriate parties and posted when appropriate on Department repositories such as IL-ISAC (Illinois - Information Sharing and Analysis Center) and the Department's Web portal.

Tests Performed: Reviewed security communications and interviewed staff.

Test Results: Information was disseminated to appropriate parties and posted to Department repositories.

No deviation noted.

Objective: The Department has procedures in place to implement policy requirements.

Department's Control: System security account activity reports are generated and procedures have been developed to investigate system security violations.

Tests Performed: Reviewed Mainframe Security Procedures, violation reports and interviewed staff.

Test Results: The Department had developed the Mainframe Security Procedures (Procedure), effective January 1, 2010 to "serves as a technical reference on RACF security policies, reporting, and procedures."

According to the Procedure, violation reports were to be reviewed and analyzed by Technical Support staff on a daily basis. The intent of reviewing the reports daily was to catch any problems with password use, password resets, or access attempts before any problems arise.

The Daily Reports documented invalid attempts (and number of attempts), password resets (and by whom), and IDs which had attempted to access data without the appropriate authorization. Department staff were to take action if invalid attempts had exceeded five times and the dataset access listing indicated an "abundance" number of tries and the ID did not have update authority.

During our review, we noted accounts which had failed logon password entry of more than five times, without indication of follow up. Additionally, there was no indication of review regarding "abundance of update tries" or review to ensure password resets were completed by an authorized individual.

In addition, per Department management, violations reports were not being routinely reviewed.

According to the Procedures, if a user needed their password reset, the Security Support staff would "confirm identity by receiving the prerecorded name or response to the prompt question." However, the Help Desk and the Security and Compliance security staff did not always confirm the individual's identity.

Upon discussion with Department management, they indicated a project was underway to collect and use the security question and answer in order to verify the identity of owner for a password reset. In addition, on June 16, 2011, the Department distributed a memorandum outlining a new process for password resets and verification as an interim process until the security question process was implemented.

Additionally, the Procedures included a listing of additional security reports which were to be generated and reviewed. However, we noted the Department was not generating and reviewing the reports.

The Department had not generated or reviewed security violation reports. Additionally, the Department did not require the verification of an individual's identity before resetting of passwords.

Department's Control: Critical Incident Response procedures exist that establish responsibility for responding to and reporting of cyber incidents that threaten Department cyber assets.

Tests Performed: Reviewed Critical Incident Response procedures, Critical Incident Response Team (CIRT) reports. and interviewed staff.

Test Results: The Department had established the Critical Incident Response Procedures, last revised January 1, 2011 to respond and report on cyber incidents. The Procedures "established responsibility for responding to and reporting all information technology security incidents."

The Procedures required a CIRT Report to be completed for each incident. The Report was to document the incident, actions taken and the lessons learned.

We reviewed four CIRT reports, noting no exceptions.

No deviation noted.

Objective: The Department monitors their systems and policies.

Department's Control: Scans on IT resources are conducted and logs are produced by the Technical Safeguards staff to detect operating system and Web application vulnerabilities, unauthorized software, potential intrusion activity, and/or to identify mission software patches when operationally appropriate or when other circumstances warrant.

Tests Performed: Reviewed security assessments and interviewed staff.

Test Results: The Technical Safeguards Unit conducted 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 the review period, the Department had conducted nine assessments. We reviewed the assessments, noting numerous vulnerabilities were identified.

Each month the Department compiled a report documenting the scans completed, the issues identified and action taken to address the issues. We reviewed the report for February 2011, which addressed testing conducted from February 2010 to January 2011. Based on our review of the reports, it did not appear that the Department was taking action to remedy security vulnerabilities classified as high risk in a timely manner.

Although a framework for conducting security assessments existed, the Department did not have a process to ensure the timely remediation of security vulnerabilities classified as high risk.

Department's Control: Department employees must acknowledge acceptance of security policies which is monitored by the Department's Personnel Liaisons.

Tests Performed: Reviewed the General Security For Statewide IT Resources Policy and interviewed staff.

Test Results: According to the General Security For Statewide IT Resources Policy, revised January 1, 2010, "new employees are required to participate in employee orientation to include certifying that they have completed any required security awareness training and agree to comply with this General Security for Statewide IT Resources."

Additionally, "current employees shall, at each annual performance evaluation, certify that they have completed any required security awareness training and agree to comply with this General Security for Statewide IT Resources."

During the review period the Department had three new employees. We requested the acknowledgments for them; however, the Department indicated they had not been completed. In addition, the Department did not require current employees to acknowledge acceptance of the policies at their annual performance evaluation.

The Department did not require employees to acknowledge acceptance of security policies.

Department's Control: Evidentiary discovery tasks are initiated by cyber security specialists when requested by law enforcement or cyber security professionals and findings are reported to authorized parties.

Tests Performed: Interviewed staff.

Test Results: When requested by law enforcement or cyber security professionals, evidentiary discovery tasks would be initiated and reported to the appropriate parties.

During the review period, there were no requests.

No deviation noted.

OVERALL CONCLUSION

Based on the test results described above, the controls (with the exceptions of controls over verifying the identity of an individual prior to resetting their password) were operating with sufficient effectiveness to achieve the control objective.

Although the Department has developed policies and procedures designed to provide an overall security strategy and framework, all provisions had not been effectively developed or implemented.

It is incumbent upon the Department to ensure mechanisms have been developed to effectively implement, monitor, audit, track, and validate compliance with the policies and procedures.

To promote compliance with the policies and procedures throughout State Government, the Department should ensure it is complying with all necessary provisions in its own environment.

Specifically, the Department should:

- Ensure the identity of the owner is verified before resetting passwords.
- Develop a process to ensure implementation of appropriate policies and procedures internally.
- Ensure the timely remediation of security vulnerabilities and issues classified as high risk.
- Review requirements outlined in all security documents to ensure they meet Department needs.
- Ensure the violation reports are reviewed and properly analyzed.

INTERNET-ENABLED WEB APPLICATIONS

EXISTING ENVIRONMENT

Objective: A structured software development methodology is utilized to manage any new software developments and enhancements to existing code, and to ensure that only authorized, tested and documented changes are made to the application.

Department's Control: All application development changes are controlled in accordance with the Application Systems Development Methodology Manual.

Tests Performed: Reviewed the Application Systems Development (ASD) Methodology, project documentation, and interviewed staff.

Test Results: The Web Application Development Unit utilized the Application Systems Development Methodology (also known as the EAA Systems Development Methodology), dated August 2005, for application developments.

For new developments, the Department utilized the Rapid Application Development (RAD) process outlined in the ASD Methodology. The RAD process allowed exceptions to the sequential processes of the Methodology to utilize iterative and prototyping development technologies.

The RAD process provided the same information as the sequential Methodology process, except the deliverables were grouped differently.

There was one new development during the review period. An online survey strategy system was developed to promote compliance with the Disabled Hiring Initiative law. We tested the new development, noting that there was general compliance with the Methodology. However, emails were provided to support user approval rather than actual user sign-offs as required by the Methodology. In addition, although testing was completed, documentation related to testing was incomplete.

User approvals did not meet Methodology requirements and the test documentation was incomplete.

Department's Control: New developments and enhancements are documented through the use of an Enterprise Service Request (ESR) and documented in the Remedy System.

Tests Performed: Reviewed Remedy Tickets, Enterprise Service Requests, and interviewed staff.

Test Results: New developments and enhancements were documented via an ESR and Remedy.

We reviewed five Remedy Change tickets for the required fields, noting no exceptions. In addition, we reviewed five ESRs for appropriate approvals and completeness, noting no exceptions.

No deviation noted.

Department's Control: New developments and enhancements are approved and tested before implementation into the production environment.

Tests Performed: Reviewed project documentation and interviewed staff.

Test Results: New developments and enhancements were approved and tested before implementation.

The Web Applications Unit made the changes and moved to a Quality Assurance environment for the user to view and approve. Each application had a business owner which approved the changes that were to be made.

We reviewed the testing documentation for the new development, noting the test plans were incomplete and documentation to support the resolution of all problems did not exist. However, documentation to support user testing and approval existed.

Test and problem resolution documentation was incomplete.

Department's Control: New developments, as well as enhancements, are moved into production by Information Services Division (ISD) Midrange and require an approved ESR to execute changes requested by Enterprise Application and Architecture (EAA) Application Development staff.

Tests Performed: Reviewed ESRs, moves to production, and interviewed staff.

Test Results: New developments and enhancements were moved to production by the ISD Midrange group. In addition, an approved ESR was required to execute the change.

For moves to production, the Web Applications Unit submitted an ESR to have the change moved to production. When the lead developer submitted an ESR, the manager was required to approve the request. The actual move to production was done by the ISD Midrange Group, after they received an approved ESR through the Remedy System.

We reviewed four ESRs for appropriateness, noting no exceptions. In addition, we reviewed the four changes to ensure appropriate segregation of duties, noting no exceptions.

No deviation noted.

Department's Control: Affected program documentation is updated as part of system developments or enhancements that are required to comply with the Information Technology Governance (ITG) process.

Tests Performed: Reviewed IT Policy, ITG documents, and interviewed staff.

Test Results: Documentation was updated as required to comply with the ITG process.

The Web Applications Unit utilized the IT Governance process and the IT Governance Policy for projects that were required to complete the process.

During the review period, there was one project which was required to complete the IT Governance process. We reviewed the project documentation, noting it complied with the ITG requirements and approvals.

No deviation noted.

Objective: The following System Security controls provide reasonable assurance that adequate measures are employed to ensure overall system security.

Department's Control: Application Development security is controlled by Security Groups which ensure that the individual developing the application does not have the authority to move the changes into the production environment.

Tests Performed: Reviewed moves to production and interviewed staff.

Test Results: Individuals which developed applications did not have the authority to move the changes into the production environment.

The Web Applications Unit submitted an ESR to have the change code moved to the production environment. When the lead developer submitted an ESR, the manager was required to approve the request. The actual move to production was done by ISD Midrange Group, after they received an approved ESR through the Remedy System.

We reviewed four changes which were moved to production during the review period, noting an appropriate segregation of duties.

No deviation 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 ensure user approval and testing documentation is maintained as required by the Methodology.

LAN APPLICATIONS

EXISTING ENVIRONMENT

Objective: A structured software development methodology is utilized to manage any new software developments and enhancements to existing code, and to ensure that only authorized, tested and documented changes are made to the application.

Department's Control: All application development changes are controlled in accordance with the Application Systems Development Methodology Manual.

Tests Performed: Reviewed the Application Systems Development (ASD) Methodology and interviewed staff.

Test Results: The LAN Application Development Unit utilized the Application Systems Development Methodology (also known as the EAA Systems Development Methodology), dated August 2005, for changes and new developments.

For new developments, the Department utilized the Rapid Application Development (RAD) process in the ASD Methodology. The RAD process allowed exceptions to the sequential processes of the Methodology to utilize iterative and prototyping development technologies.

The RAD process provided the same information as the sequential Methodology process, except the deliverables were grouped differently.

There were no new developments during the review period.

No deviation noted.

Department's Control: New software developments and enhancements, and changes are documented through the use of the Remedy Change Module (Enterprise Service Requests (ESR)) or Enterprise Program Management (EPM) Portal.

Tests Performed: Reviewed change tickets, ESRs, and interviewed staff.

Test Results: New software developments and enhancements and changes were documented in Remedy or the EPM Portal.

Requests which were documented in the Remedy Change Management module were either categorized as "changes" or "service requests". If the request was categorized as a change, then the Remedy Change Management Guide was followed. If the request was categorized as a service request, then the Remedy User Guide was followed.

Department management stated if the request was a problem/issue it was categorized as a "service request" and if the request was a change to an application or an enhancement it was categorized as a "change". However, the Department had not formally defined categorization types.

We reviewed two requests which were categorized as "change" for the required fields noting no exceptions. In addition, we reviewed them for the proper approvals, noting no exceptions.

We also reviewed three requests which were categorized as "service request" for the required fields and proper approvals, noting all of the fields were completed.

There were no new developments during the review period. In addition, there were no projects which were required to go through the EPM Portal.

No deviation noted.

Department's Control: New developments, enhancements, and changes are approved and tested before implementation into the production environment.

Tests Performed: Reviewed requests documentation and interviewed staff.

Test Results: New developments, enhancements and changes were to be approved and tested prior to implementation.

The LAN Application Unit completed the change; then notified the user to test the change. After approval was received from the user, the change was moved to the production environment.

We reviewed six "maintenance" requests and found general compliance with procedures. However, the Remedy User Guide did not include detailed procedures to promote consistency in documentation requirements for all change types.

There were no new developments during the review period.

No deviation noted.

Department's Control: New developments, enhancements, and changes are approved through Remedy Change Management Module process.

Tests Performed: Reviewed requests and interviewed staff.

Test Results: New developments, enhancements and changes were approved through the Remedy Change Management process.

We reviewed six requests for the required fields and proper approvals, noting all of the fields were completed. However, one request was approved by a supervisor who was not included on the IT Coordinator list as required.

There were no new developments during the review period.

The approval of one service request did not meet requirements.

Department's Control: Affected program documentation is updated as part of system developments or enhancements required to comply with the Information Technology Governance (ITG) process.

Tests Performed: Reviewed IT Policy, ITG documents, and interviewed staff.

Test Results: Documentation was updated as required to comply with the ITG process.

The LAN Applications Unit utilized the IT Governance process and the IT Governance Policy for projects that were required to complete the process.

During the review period, there were no system developments or enhancements which required documentation to be updated.

No deviation noted.

Objective: Processes exist to restrict access to LAN applications.

Department's Control: Development security is controlled by Access Security Groups which, along with Drive Mapping, ensures that only authorized users are allowed access to the application.

Tests Performed: Reviewed Remedy worklogs and interviewed staff.

Test Results: Development security was controlled via Access Security Groups. Access Groups were assigned to allow individuals access to specific folders.

No deviation 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 ensure all appropriate requirements to control changes are followed.

LAN SERVICES

EXISTING ENVIRONMENT

Objective: Policies exist to document the Department's standard/template for the LAN network settings.

Department's Control: The LAN Services Standards for Hardware Configuration and Development document the Department's configuration standards.

Test Performed: Reviewed network topologies, devices configurations, hardware and software vendor websites, configuration standards, 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.

To assist in the configuration of Agency LAN infrastructure devices, LAN Services maintained the CMS/BCCS LAN Services Standards for Hardware Configuration and Development document. To ensure conformance with the defined standards, LAN Services implemented a procedure in February 2011 to periodically perform informal reviews of device configurations.

Upon review of the standards we noted they, for the most part, provided for appropriate baseline settings; however, we did note instances where configurations established within the standards could be enhanced. Additionally, upon review of the configurations, we noted instances where the configurations deviated from the standards.

We reviewed the current electronic configurations of the devices, which contained software version levels and fully documented high-level rule base descriptions. Upon review it appeared the configurations were, for the most part, appropriately configured; however, we did note instances where configurations could be enhanced.

We noted some standards and parameters which should be reviewed to ensure security issues are appropriately addressed.

Department's Control: Individual network topology maps are maintained for each network segment.

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

Test Results: To document its network architecture, LAN Services maintained individual network topology maps for each of the agency network segments it maintained.

We reviewed the maps depicting network segments utilized by the Department and each of the consolidated agencies. Upon review and discussion with staff, maps provided appeared to be, for the most part, accurate and complete.

Additionally, during our review of the maps and configurations we determined devices were placed in suitable logical positions.

No deviation noted.

Objective: Procedures exist to monitor against unauthorized access to system resources.

Department's Control: SolarWinds and NCM are utilized to monitor the network and ensure configurations are appropriately backed up. Events are logged daily and reviewed by LAN Services.

Test Performed: Reviewed SolarWinds, vendor website, and interviewed staff.

Test Results: SolarWinds Orion was utilized and consisted of two separate modules: Network Configuration Manager (NCM) and Network Performance Manager (NPM). NCM was utilized for configuration backups, making configuration changes to multiple devices at a time, and policy reporting purposes. NPM was utilized to monitor performance related issues such as up/down status of devices, bandwidth utilization, CPU utilization, etc.

Both NCM and NPM were capable of sending alerts to administrators as deemed appropriate. Up/down status and high processor events were the primary events in which NPM sent alerts to administrators; however, other events were logged as well and all events were logged to a database server.

Configuration backups were handled by NCM. We reviewed the reports for a five day period, noting configurations were successfully backed-up on a routine basis.

No deviation noted.

Department's Control: Tools are utilized to monitor the network and early identification of potential security breaches. Incident logs are monitored and evaluated by LAN Services. The Security Solution Team is notified of any breaches.

Test Performed: Reviewed spreadsheets, device configurations, and interviewed staff.

Test Results: LAN Services had configured two servers to function as the primary external logging servers for the firewalls, routers and switches it maintained.

To monitor the log files for potential issues, an individual had been assigned the responsibility of reviewing the logs daily and tracking the review and any noted issues in a spreadsheet. If necessary, the Security and Compliance Solutions team would be contacted to address any issues identified during the review.

No deviation noted.

Department's Control: TACACS is utilized to ensure only authorized individuals have access. Access is granted based upon team assignment within LAN Services.

Test Performed: Reviewed access rights, account parameters, device configurations, vendor website, and interviewed staff.

Test Results: Two authentications servers were utilized to provide authorized access to the firewalls, routers, and switches maintained by LAN Services. Per review of the vendor website, the servers appeared to be current vendor recommended release.

We reviewed accounts with administrative privileges to ensure appropriate access restrictions and appropriate user assignment for the State Agency network firewalls, routers and switches maintained by LAN Services, noting no exceptions.

No deviation noted.

Department's Control: An authorization request form is sent to the LAN Services Data Center Supervisor by the employees supervisor authorizing access. An authorization request form is sent to the LAN Services Data Center Supervisor by the employees supervisor requesting access to be removed when appropriate.

Test Performed: Reviewed authorization request form and interviewed staff.

Test Results: At the end of calendar year 2010, LAN Services implemented a new procedure which included an access request form to document authorization of requests for new access and revocation of access no longer necessary. Per management, there had been no new requests for access or revocation of access since the form was implemented.

No deviation noted.

Department's Control: LAN Services periodically monitors access rights.

Test Performed: Interviewed staff.

Test Results: With the implementation of the authorization request form at the end of calendar year 2010, managers were advised to start reviewing the assignment of IDs and associated access privileges on a periodic basis; however, such reviews would have been informal and documentation was not maintained.

No deviation noted.

Department's Control: McAfee Smartfilter internet filtering service to consolidated agencies (AGR, CEO, CMS, DHS, DPH, DNR, FPR and REV)

Test Performed: Reviewed diagrams, access rights, vendor websites, and interviewed staff.

Test Results: To manage and monitor Internet usage for the Department and several other agencies (including but not limited to AGR, DCEO, DCMS, DES, DOT, DFPR, EPA, HFS, DHS, DNR, DPH, and REV), the Department had deployed an Internet filtering and monitoring solution: McAfee SmartFilter and Web Reporter.

We reviewed the software versions for the authentication, filtering and reporting modules, noting software appeared to be at current vendor recommended versions.

No deviation noted.

Objective: Procedures exist to provide that only authorized, tested and documented changes are made to the infrastructure.

Department's Control: Changes to the infrastructure follow the Department's Change Management process.

Test Performed: Interviewed staff.

Test Results: Agency network infrastructure changes followed the Department's Change Management process to ensure changes were tracked and appropriately approved. See the Change Management section for detailed testing of changes.

No deviation noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. However, the complexity of the agency networks necessitates continual review and analysis to ensure security controls meet the Department's standards. To enhance controls, the Department should:

- Continually review standards and security parameters to ensure security issues are adequately addressed.
- Ensure established configuration standards (and associated templates) are consistently applied (where possible) to all devices.

LIBRARY SERVICES

EXISTING ENVIRONMENT

Objective: Agency standards and policies

Department's Control: CMS, DHS, HFS sets the standards and policies for their respective agencies which would include document approvals, forms to use and the responsibilities for each step of the process. This documentation is available on SharePoint. DOT requests are set up using historical knowledge, past practice and agency contact when necessary. There is no set standard in place for all agencies as they each have their own unique process to follow. These processes allow Library Services to navigate through the mainframe and/or browse the Mobius reports to ensure the integrity of the media and libraries, using the most current security software available.

Tests Performed: Reviewed SharePoint site and interviewed staff.

Test Results: The Department of Central Management Services (CMS or Department), Department of Human Services (DHS), and the Department of Healthcare and Family Services (DHFS) sets standards and policies for their respective agencies which included document approvals, forms to use, and the responsibilities for each step of the process. Additionally, the Department of Transportation (DOT) requests were set up based on historical knowledge, past practices, and agency contacts.

Library Services personnel stated they were working with the agencies to update standards and policies and to establish documentation on a SharePoint site.

Library Services conducted their duties based on job experience and documentation provided by agencies, whereas no formal internal procedures had been established.

Policies and procedures were informal.

Department's Control: Checking reports online using Mobius and checking all library jobs in CA-Scheduler for successful completion of assigned tasks and schedules assist staff members to identify and correct any hardware or software issues to keep all system impacts to a minimum.

Tests Performed: Reviewed Mobius and interviewed staff.

Test Results: Online Reports via Mobius were utilized to verify the status of all library jobs in CA-Scheduler for successful completion of assigned tasks and schedules to assist staff members in identifying and correcting any hardware or software issues to keep all system impacts to a minimum. Library Support staff stated they checked reports online to ensure that library jobs were completed. The staff verified the generation, volume, and the JCL condition codes. The process was utilized for daily, weekly, and monthly backups. The most typical hardware problems were with carts and the most typical software problems were abends. Library Support staff corrected problems where necessary if they were part of the duties for Library Services (non-

programmatic), otherwise problem resolution would be up to the programmer for the respective agency to fix.

Policies and procedures were informal.

Objective: The Library Support unit communicates the procedures to the users

Department's Control: All email requests contains agency, library and member information necessary for the Library Support staff to complete their tasks.

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

Test Results: All email requests contained agency, library, and member information necessary for the Library Support staff to complete their tasks.

We reviewed 25 moves to production, noting that one move was not appropriately authorized. We also reviewed 19 production libraries for appropriateness, noting no exceptions.

One move to production was not appropriately authorized.

Objective: The Library Services section monitors compliance with policies

Department's Control: Processes and reports exists to control and track media to provide accurate data as follows:

- TGS (automated Tape Generating System) for DHS and HFS.
- Manual system for legacy Mental Health systems.
- Manual system for DOT.

Tests Performed: Reviewed Mobius reports and interviewed staff.

Test Results: Processes and reports existed to control and track media to provide accurate data. TGS and manually produced reports were used to document tape activities for DHS, DHFS, DHS Mental Health 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. However, Department staff stated the use of the TGS reports was decreasing as more agencies were migrating to virtual storage, high density, or FTP.

During our review, we reviewed the Discrepancies (402) and Tape Statistics (403) reports for DHS and HFS for May 19, 2011, noting that the 403 reports were used for the tracking of tapes. The 402 reports showed if there were any discrepancies associated with the carts.

We reviewed the DHS and DHS' Mental Health 3011 reports for May 24, 2011, noting it documented when the carts needed to be discarded. We also reviewed the 6011 report which was printed daily and showed carts forwarded to the Regional Vault.

No deviation noted.

Department's Control: The following processes exist to identify and correct hardware and software issues to keep system impacts to a minimum:

- Checking TGS reports.
- Check for successfully completed jobs.

Tests Performed: Reviewed Mobius and interviewed staff.

Test Results: Checking TGS reports and checking for successfully completed jobs existed to identify and correct hardware and software issues to keep system impacts to a minimum.

If there were problems encountered during the backup or move to production processes, Library Support staff would take appropriate action to resolve the problem. For problems that would occur during the day they would be automatically logged in the job history of CA-Scheduler. For problems that would occur during the nightly cycle they would be included in the Daily Shift reports by the Input Unit. Library Support staff would know that the problem was resolved because the job would complete.

Library Support would check the reports online to ensure that library jobs were completed. Library Support staff stated they verified the generation, volume and the JCL condition codes. This was the same process for daily, weekly, and monthly backups. The most typical hardware problems were with carts and software would be abends. Library Support staff stated they would correct problems if they were part of the duties for Library Services, otherwise it would be up to the programmer for the respective agency to fix the problems encountered.

No deviation noted.

Department's Control: Automated software is used to control and track media for easy accessibility.

Tests Performed: Reviewed tapes on-site and at the Regional Vault and interviewed staff.

Test Results: Automated software was utilized to control and track media for easy accessibility.

During our review, we obtained a listing of tapes generated and their specific location. We reviewed 50 tapes located at the CCF, and confirmed all tapes were located as indicated.

We also selected 91 tapes listed as located at the Regional Vault, noting 11 (12.08%) of the tapes were not located at the Regional Vault but were located at the CCF.

In addition, Department staff stated backup tapes were not encrypted to protect personal or confidential data.

Some tapes were not at the location indicated and backup tapes were not encrypted.

Department's Control: Reports are used to inventory media to keep inventories current.

Tests Performed: Reviewed TMS reports and interviewed staff.

Test Results: Reports were used to inventory media in order to maintain current inventories.

The Tape Library used various reports for inventory such as the inventory listing, TMS report and Automated Cartridge System (ACS) report. Tape Library staff stated inventories were conducted in April 2010 and December 2010. We obtained and reviewed documentation of the inventories and how the inventory was balanced by reconciling the reports, noting no exceptions.

No deviation noted.

Department's Control: Authorization lists, forms and/or broadcasts are used to control the release and receipt of media for security purposes.

Tests Performed: Reviewed Media Transmittal Forms and interviewed staff.

Test Results: Authorization lists, forms and/or broadcasts were utilized to control the release and receipt of media for security purposes. Agencies were responsible for sending a request to release/receive media, which required a Media Transmittal Form or a broadcast via e-mail to the Media library staff. The forms listed the tape media volumes the agencies requested to have moved from the vault to the CCF library or vice versa.

When a transmittal form was received, the individual requesting the move was verified against the authorization list.

We reviewed the transmittal forms for January 27, 2011, noting no exceptions.

No deviation noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. However, to strengthen the controls, we recommend the Department:

- Develop standards and policies for Library Service activities, moves to productions, and verifying backups.
- Ensure that moves to production are authorized.
- Ensure the backup tape locations are properly documented.
- Ensure personal and confidential data on backup tapes is adequately protected from unauthorized disclosure.

NETWORK SERVICES

EXISTING ENVIRONMENT

Objective: Policies exist to document the network settings.

Department's Control: The Basic MPLS Common Connectivity Model document settings.

Test Performed: Reviewed Basic Multiprotocol Label Switching (MPLS) Common Connectivity Model and interviewed staff.

Test Results: Network Operations maintained the Basic MPLS Common Connectivity Model. The Model depicted the basic architectural layout, including points of redundancy, for agencies connecting to the Statewide network.

No deviation noted.

Department's Control: The Agency WAN Redundancy standard document settings.

Test Performed: Reviewed Agency Wide Area Network (WAN) Redundancy Standard and interviewed staff.

Test Results: Enterprise Network Support (ENS) maintained the Agency WAN Redundancy Standard. The Standard provided router redundancy configurations by establishing baseline configurations which defined primary and secondary routers using two different protocols.

No deviation noted.

Department's Control: Created configuration templates for core and distribution routers.

Test Performed: Reviewed network topologies, device configurations, hardware and software vendor websites, configuration templates, and interviewed staff.

Test Results: Network Services, which consisted of two teams (Network Operations and Enterprise Network Support), was tasked with maintaining the State's primary network consisting of core, distribution and agency access routers; as well as firewalls and egress routers.

To assist in the configuration of core and distribution routers, Network Operations maintained two configuration templates; one for core routers and one for distribution routers. Upon review of the templates we noted they, for the most part, provided for appropriate baseline settings; however, we did note instance where configurations established within the templates could be enhanced. Additionally, upon review of the configurations, we noted instances where the configurations deviated from the standards.

We reviewed the current electronic configurations of the devices, which contained software version levels and fully documented high-level rule base descriptions. Upon review it appeared the configurations were, for the most part, appropriately configured; however, we did note instances where configurations could be enhanced.

We noted some standards and parameters which should be reviewed to ensure security issues are appropriately addressed.

Department's Control: Utilizes Cisco Advanced Services quarterly reports.

- To keep network in-line with Cisco best practices recommendations.
- Reviewed by Cisco and Network Operations.

Test Performed: Reviewed reports and interviewed staff.

Test Results: To keep the network aligned with Cisco best practices and recommendations, Cisco performed reviews and provided Network Services with reports titled Best Practice Configuration Analysis Report. During the review period, we noted reports were provided to Network Services for the quarters ending December 2010 and March 2011; however, a report was not provided for the quarter ending September 2010.

Upon review of the Executive Summary in the reports provided, we noted no major issues had been identified. Additionally, the reviewer cited progress was being made to resolve management and security related issues identified in prior reports.

The reports also made recommendations regarding hardware and software upgrade needs; as well as, configuration enhancements to increase network security, efficiency, and redundancy.

No deviation noted.

Department's Control: Network diagrams are maintained.

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

Test Results: To document its network architecture, Network Services maintained network diagrams depicting the placement of the core distribution, access and egress routers maintained.

Upon review and discussion with staff, network diagrams provided for the segments of the network maintained by Network Services 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.

No deviation noted.

Department's Control: Illinois Century Network (ICN) Remedy and Expense Management System (EMS) 11 are utilized to inventory current data circuits.

Test Performed: Reviewed procedures and interviewed staff.

Test Results: The Department utilized ICN Remedy and EMS 11 to maintain an inventory of data circuits.

Network Services utilized methods and procedures established by Field Operations to inventory circuits in ICN Remedy: ICN Remedy Use Case Procedures and ICN Remedy Circuits and Hardware Procedures. Upon review of the procedures it appeared Network Services had procedures depicting methods and procedures utilized to enter circuit and hardware orders and installations.

The Department utilized the Telecommunications Data/Intercity Service Request (TDR) for requesting and recording of data circuits into EMS11.

No deviation noted.

Objective: Procedures exist to monitor against unauthorized access to system resources.

Department's Control: Authentication servers are utilized to control access and ensure only properly authenticated individuals are granted access to devices for configuration management and maintenance.

- This is done via Cisco Tacacs+ system.
- Granting access requires management approval.

Test Performed: Reviewed access rights, account parameters, device configurations, vendor website, and interviewed staff.

Test Results: Three authentications servers were utilized to provide authorized access to the firewalls, routers, and switches maintained by Network Services. Per review of the vendor website, the servers appeared to be current vendor recommended release.

Management indicated access required management approval and IDs were periodically reviewed; however, such approvals and reviews were informal and documentation was not maintained. We reviewed accounts with administrative privileges to ensure appropriate access restrictions and appropriate user assignment for the core, distribution, and access segments of the network, noting access generally appeared to be appropriately restricted and assigned.

Documentation was not maintained showing approval of access rights.

Department's Control: SolarWinds Orion is utilized to monitor the network.

- SolarWinds is monitoring the backbone core, distribution, and customer access routers. The devices are being monitored with icmp for up/down status. Device CPU, memory,

and interface bandwidth utilization and error data is also collected and stored in the database.
- Monitored device results are under constant 24/7 review by the Customer Management Center (CMC).
- Monitored, failed devices are attended to by CMC and the applicable NetOps group.
- Notification is escalated to management level if applicable.

Test Performed: Reviewed SolarWinds, vendor website, and interviewed staff.

Test Results: SolarWinds Orion was utilized and consisted of two separate modules: Network Configuration Manager (NCM) and Network Performance Manager (NPM). NCM was utilized for configuration backups, making configuration changes to multiple devices at a time, and policy reporting purposes. NPM was utilized to monitor performance related issues such as up/down status of devices, bandwidth utilization, CPU utilization, etc.

Both NCM and NPM were capable of sending alerts to administrators as deemed appropriate. The CMC was primarily responsible for monitoring (on a 24x7 basis) the status of the devices; however, Network Services may monitor the alerts as a part of their normal daily activities. When CMC became aware of a problem, they would open a Remedy ticket and escalate as necessary to Network Services for corrective action.

No deviation noted.

Department's Control: ICN Remedy and CMS Remedy are utilized for trouble ticketing and tracking problem resolution.

Test Performed: Reviewed ICN Remedy tickets, CMS Remedy tickets, and interviewed staff.

Test Results: Network Services utilized ICN Remedy and CMS Remedy for trouble ticketing and tracking problem resolution.

We obtained and reviewed trouble tickets generated from ICN and CMS Remedy, noting no exceptions.

See the Help Desk section for detailed testing of help desk and ICN Remedy tickets.

No deviation noted.

Objective: Procedures exist to provide for the completeness, accuracy and timeliness of backups.

Department's Control: Firewall, router, and switch configurations are backed up via two methods.
- Method 1:
    - A server is used to gather configurations.

    - An archive file (tar) of all the configurations is created on the server.
    - The archive file is retrieved by the Data Center Storage team.
    - The retrieved file is backed up in accordance with the Data Center Storage team's defined backup strategy.
- Method 2:
    - An Orion, SolarWinds server is used to gather the configurations.
    - The configurations are stored locally on the server.
    - The configurations are backed up periodically.

Test Performed: Reviewed SolarWinds, reports, and interviewed staff.

Test Results: Firewall, router and switch configurations were backed up via two independent processes.

The first method of backing up device configurations utilized a backup server maintained by Network Services. The server utilized an automated process to retrieve configurations from devices on a daily basis. Files were then encrypted and stored on the server for the Enterprise Storage and Backup (ESB) team to backup and rotate off-site. We reviewed a report detailing the completion of backups for a five day period, noting no exceptions.

The second method of backing up device configurations utilized the NCM module of SolarWinds. Daily, NCM pulled configurations and placed a copy of the configurations on a local database server. Once configurations were backed-up, NCM sent email reports to administrators informing them of the devices which were not successfully backed-up during the cycle. Upon discussion with staff and review of the reports for one day, we noted configurations were generally being backed-up on a routine basis.

No deviation noted.

Objective: Procedures exist to provide that only authorized, tested and documented changes are made to the infrastructure.

Department's Control: Changes to the infrastructure follow the Department's Change Management process.

Test Performed: Interviewed staff.

Test Results: The Department utilized the Remedy Change Management application and followed the Department's Change Management process for approving and documenting changes made to the Network infrastructure.

See the Change Management section for detailed testing of changes.

No deviation noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. However, the complexity of the statewide network necessitates continual review and analysis to ensure security controls meet the Department's standards. To enhance the controls, the Department should:

- Continually review security standards and parameters to ensure security issues are appropriately addressed.
- Ensure established configuration templates are consistently applied (where possible) to all devices.
- Develop procedures to ensure appropriate documentation is maintained for granting/modifying/revoking access to networking resources.

OUTPUT PRODUCTION

EXISTING ENVIRONMENT

Objective: Distribution of output is restricted to authorized individuals.

Department's Control: The Focal System contains a listing of individuals authorized to pickup print jobs.

Tests Performed: Reviewed Report Distribution Logs and interviewed staff.

Test Results: The Focal application contained a listing of individuals authorized to pick up reports.

We reviewed 25 individuals from the Report Distribution Logs from the weeks of November 29, 2010 and January 24, 2011 to determine if only authorized individuals picked up reports, noting no exceptions.

No deviation noted.

Department's Control: Individuals are required to provide identification and/or verified by Revenue staff and sign the Report Distribution Log for each pickup.

Tests Performed: Reviewed Report Distribution Logs, observed pickup process, and interviewed staff.

Test Results: Individuals were required to provide identification in order for the Revenue staff to verify. In addition, the individual was required to sign the Report Distribution Log for each pickup.

We reviewed Report Distribution Logs from the weeks of November 29, 2010 and January 24, 2011, noting they were generally completed.

No deviation noted.

Department's Control: Central Management Services (CMS)/Healthcare and Family Services (HFS)/Department of Human Services (DHS) print jobs are maintained in the secure print shops.

Tests Performed: Interviewed staff.

Test Results: The CMS, HFS and DHS print jobs were maintained in the secure print shops until they were picked up. The print jobs were picked up at the loading dock each morning by the agencies messenger. The messenger would pull up to the dock, call the guard's desk, and identify themselves. The guards would have a listing of authorized individual and then notify the print shop of the agency waiting for pickup. The print shop staff then took the print jobs to the loading

dock. The documents were loaded onto the truck. The messenger would then sign the Report Distribution Log.

No deviation noted.

Department's Control: During business hours, the remaining agencies print jobs are maintained in the distribution room. After hours, the print jobs are maintained in the secure print shop.

Tests Performed: Observed pickup process and interviewed staff.

Test Results: During business hours, agencies print jobs were maintained in the distribution room. After hours, the print jobs were maintained in the print shop.

No deviation noted.

Department's Control: All payroll jobs or any job with Social Security numbers and names are sealed.

Tests Performed: Observed reports and interviewed staff.

Test Results: Payroll jobs or any job with confidential information including Social Security numbers and names were sealed.

We observed a pick up on April 6, 2011, noting the report was sealed as were the reports in the distribution room.

No deviation noted.

Objective: Measures to maintain the printing equipment have been implemented.

Department's Control: Preventive maintenance agreements are in place.

Tests Performed: Reviewed preventive maintenance agreements and interviewed staff.

Test Results: The Department maintained maintenance agreements over the printers.

We reviewed the preventive maintenance agreements for 12 selected printers. However, in our testing of maintenance agreement, we were only provided agreements for eight of 12 printers.

All maintenance agreements were not available for review.

Department's Control: Any printer down time is recorded in the Down-time Log.

Tests Performed: Reviewed Down-time Logs and interviewed staff.

Test Results: When problems with a printer occurred a service call was placed. In addition, the information was recorded in the Down-time Logs. At the end of each month the total down time was recorded for each printer.

We reviewed the Down-time Logs for December 2010 and February 2011, noting a majority of the downtime was related to jams, problems with paper trays, broken rollers, faded pages, imaging problems, part ordering, and replacement.

No deviation noted.

Department's Control: Monthly status reports are maintained which document the number of reports produced and the printer meter readings.

Tests Performed: Reviewed monthly status reports.

Test Results: Monthly status reports were maintained which documented the number of reports produced and printer meter readings.

We reviewed the printer monthly status reports for December 2010 and February 2011, noting the reports had a break down for: usage (printer meter readings), performance (number of reports produced), downtime, average response time, and the number of calls for each printer and shift performance.

No deviation noted.

Department's Control: Printer configurations are backed-up weekly and stored in Revenue's tape library. However, DHFS is responsible for the backup of the printer they utilize. It is backed-up weekly and stored at Revenue's tape library.

Tests Performed: Observation and interviewed staff.

Test Results: Printer configurations were backed up and stored in Revenue's tape library. DHFS was responsible for the backup of the printer which they utilized.

We observed the printer configuration backup tapes in the library.

No deviation noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. However, to strengthen the controls, we recommend the Department verify that all printers are covered under preventive maintenance agreements.

PHYSICAL SECURITY

EXISTING ENVIRONMENT

Central Computer Facility (CCF) and the Communications Building

Objective: Procedures exist to restrict physical access.

Department's Control: Physical access to facilities is restricted to authorized individuals by a card key system. Proximity card readers also restrict access to areas within the facilities.

Tests Performed: Toured facilities and interviewed staff.

Test Results: The card key system was utilized to control and restrict access to the CCF and Communications Building. Proximity card readers were installed on the building's exterior doors and strategically throughout the interior of each building.

In addition to other sensitive areas, at the CCF, the card key system controlled and restricted access to the Data Center hosting the Tape Library, tape cleaning room, Systems Operations Center, Public Key Infrastructure (PKI) room, and telecommunications room.

In addition to other sensitive areas, at the Communications Building, the card key system controlled and restricted access to the ICN network room, server and telecommunications rooms, and Network Control Center (NCC) Technical Safeguards lab.

No deviation noted.

Department's Description of Control: Absentee limits and restrictions on employee pass-back are activated to help control physical access to buildings.

Tests Performed: Reviewed procedures, card key system, toured facilities, and interviewed staff.

Test Results: The Badge Information Document and the Access Information Document outlined the requirements for access cards to be set with an absentee limit. We reviewed the card key system, noting absentee limits were established to disable access cards after a period of inactivity.

In addition, upon review of the card key system and observations of staff, we noted the Department had implemented pass-back technology to help prevent individuals from following ("piggy backing") others into the CCF and Communications Building.

No deviation noted.

Department's Control: In order to obtain an access badge:

- Privileges must be approved by an appropriate authority and are subject to modification or revocation by same.

- All employees and contractors of the CMS Bureau of Communication and Computer Services (BCCS) will be issued a photo card credential subject to the confirmation of CMS employment or contractual relationship, a screening for outstanding warrants and criminal history.
- Presentation of one of the following identity source documents: State issued Driver's License, State issued State ID card, a U.S. Government photo ID if not a U.S. citizen.

Tests Performed: Reviewed policies and procedures, email approvals, and interviewed staff.

Test Results: During our review, we were provided four documents, which outlined differing requirements for obtaining an access badge.

- Statewide CMS/BCCS Facility Access Policy, effective December 15, 2008,
- IT Resource Access Policy, effective December 1, 2007,
- Badge Information Document, and
- Access Information Document.

However, we determined the Department did not comply with the requirements outlined in these documents. Department management stated the process used for obtaining an access badge was the receipt of an email requesting access. This process did not utilize the formal procedures outlined in the four documents. For example, the following processes were not followed:

- The Statewide CMS/BCCS Facility Access Policy stated background checks were to be conducted on all individuals requiring unescorted access. Access would be delayed until the background was reviewed.
- According to the Badge Information Document, all workforce credential requested for BCCS must originate through their Personnel Liaison.
- According to the Access Information Document, all employees and contractors of BCCS would be issued a photo card credential subject to:
    - Confirmation of CMS employment or contractual relationship.
    - Appearance in person before a trusted agent.

During the review period, the Department had nine new employees. We requested the email approvals for three new employees, noting the emails had been sent to the BOPM Security Administrator by various individuals within the Department.

In the event, access privileges needed to be revised, Department management emailed the BOPM Security Administrator of the required changes.

Additionally, there was not a formal mechanism in place to ensure the BOPM Security Administrator was notified of departing individuals to ensure timely revocation of access rights.

The Department did not have adequate controls over the granting, modifying, or revoking access badges.

Department's Control: Physical access cards are managed by BOPM Security Administrator.

Tests Performed: Reviewed card key system, departed employee listing, access rights, and interviewed staff.

Test Results: The BOPM Security Administrator was responsible for the management of the access cards.

Upon authorization for the creation of an access card, the individual had to meet (staff in remote locations could email information) with the BOPM Security Administrator. At that time, the BOPM Security Administrator would create the access card with the applicable access rights.

We reviewed 18 individuals, who had left the employment of the Department, noting:

- 9 badges were deactivated on their last day, or within 24 hours,
- 7 badges were deactivated within two weeks of their last day, and
- 2 badges were deactivated more than two weeks after their last day.

We also reviewed the appropriateness of access for 81 individuals, noting 23 (28%) of those access rights should have been revoked. Upon notification, the Department revoked the access rights.

In the event an access badge was lost, the guards notified the BOPM Security Administrator who in turn disabled the badge.

The Department did not have adequate controls to ensure the timely deactivation of access badges.

Department's Control: Access is logged, maintained and reviewed by BOPM Security Administrator.

Tests Performed: Reviewed card key system documentation and interviewed staff.

Test Results: The card key system had the capabilities to create various reports. Reporting capabilities included, reports documenting location and time an access card was utilized, as well as who had access to the facilities and various location within.

However, according to the BOPM Security Administrator, reports were not routinely generated or reviewed. Reports were only generated when a request from management was received.

The Department did not routinely review access logs.

Department's Control: Supervisor or Manager is responsible for collection and return of ID Badge's upon employee or contractor discharge, separation or card expiration.

Tests Performed: Reviewed policies and procedures and interviewed staff.

Test Results: The individual's supervisor or manager was responsible for the collection and return of badges upon departure.

However, during our review, we also noted that badges could be collected by the security guards on the individuals last day.

Once collected, the badges were to be sent to the BOPM Security Administrator for destruction.

Records to support the receipt and destruction of badges did not exist.

We were unable to verify the receipt and destruction of badges.

Department's Control: Processes exist for issuing and maintaining real property keys.

- The Facility Managers or designee determines the need of an employee and/or contractor to be issued a facility key and to keep to a minimum the number of keys issued.
- Employees are to report a lost key to the issuer (Manager) immediately.
- Key(s) are to be returned at the end of State employment, contractual obligation or upon issuer's request.

Tests Performed: Reviewed key logs, departed employee listing, toured facilities, and interviewed staff.

Test Results: Each facility manager was responsible for issuing and maintaining real property keys. Keys were issued to individuals upon supervisory request. A key log was maintained of individuals issued keys.

Upon review of the real property key listings for the CCF and Communications Building we noted deficiencies in the tracking and maintenance of real property keys. The key listing did not accurately reflect who had been issued keys. In fact, our review indicated 18 (50%) of the 36 master keys to the CCF and Communications Building had been lost, not found, or assigned to a former employee.

Adequate controls were not in place to track and maintain real property keys.

Department's Control: The Department has a contract with a security firm.

Tests Performed: Reviewed contract and interviewed staff.

Test Results: Effective September 25, 2009, the Department entered into a contract with a security firm to provide security guard services to select facilities, including the CCF and Communications Building. The contract required at least one guard be on duty 24/7 at both buildings and outlined the security guards duties and responsibilities associated with patrolling, incident response/reporting, and access control.

No deviation noted.

Department's Control: Security guards staff facilities 24/7.

Tests Performed: Reviewed contract, shift reports, and interviewed staff.

Test Results: The contract required at least one guard to be on duty 24/7 at both buildings.

Based on observations and review of reports, the CCF and Communications Building were protected by security guards 24/7.

No deviation noted.

Department's Control: Security guards patrol the interior and exterior of the facilities.

Tests Performed: Reviewed contract, shift reports, and interviewed staff.

Test Results: Based on observations and review of reports, the guards at the CCF and Communications Building patrolled the interior and exterior of the facilities.

No deviation noted.

Department's Control: Security guards document their daily shift activities.

Tests Performed: Reviewed post orders, daily activity reports, and interviewed staff.

Test Results: The Site Specific Post Orders directed the security guards to log their daily activity on the Daily Activity Report.

We reviewed the Daily Activity Reports for the CCF and Communications Building for the weeks of December 20, 2010 and February 14, 2011, noting they had been completed and no significant issues were noted.

No deviation noted.

Department's Control: Security Guards issue temporary badges (with limited access rights) to visitors, and to employees who forget their assigned access card.

Tests Performed: Reviewed temporary badges and interviewed staff.

Test Results: The Department maintained temporary badges with varying levels of access privileges; 15 types of badges for the CCF and 12 types of badges for the Communications Building. Depending on the type of access rights previously defined within the card key system for the individual, security guards issued the appropriate temporary badge. A visitor (V) badge, which contained no access rights, was maintained for both buildings.

No deviation noted.

Department's Control: Those issued a temporary badge must sign the Building Admittance Register.

Tests Performed: Reviewed Building Admittance Registers, card key system, and interviewed staff.

Test Results: Individuals receiving a temporary badge were required to sign the Building Admittance Register prior to receiving a temporary badge from the security guard. We reviewed the Building Admittance Registers for the week of February 14, 2011 for the CCF and Communications Building, noting the registers contained name and badge number for each entry.

Additionally, for the same week, we selected 24 individuals issued temporary badges at the CCF and 24 individuals issued temporary badges at the Communications Building and compared them to the access privilege defined in the card key system, noting all appeared to have been issued the appropriate badge.

No deviation noted.

Department's Control: Security guards inventory the temporary badges at the start of each shift.

Tests Performed: Reviewed Badge Inventory sheets, card key system, and interviewed staff.

Test Results: Security guards were to inventory temporary badges at the start of each shift and document the results on the respective buildings Badge Inventory sheets. We reviewed the Badge Inventory sheets for the week of March 27, 2011 for the CCF and Communications Building, noting the sheets were being completed and no significant exceptions were noted.

No deviation noted.

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

Tests Performed: Toured facilities and interviewed staff.

Test Results: Video cameras were strategically placed throughout the interior and surrounding the exterior of both the CCF and Communications Building. Video feeds were monitored at a console located at the security guard desks. We viewed the digital video feeds, noting cameras were generally positioned to allow for clear unobstructed views and images were generally clear.

In addition, since the system was connected to both the CCF and Communications Building, security guards at each facility had the ability to review cameras at their facility and the other facility. The Physical Security Coordinator also had the capability to remotely view the cameras. Video was saved to a Network Video Recorder located in the CCF Data Center.

No deviation noted.

Objective: Procedures exist for the identification and escalation of physical security breaches.

Department's Control: Post orders and emergency evacuation procedures are at every guard desk.

Tests Performed: Reviewed post orders, emergency evacuation procedures, and interviewed staff.

Test Results: The guards at the CCF and the Communications Building maintained Site Specific Post Orders. The Orders provided general guidance and instructions.

In addition, the guards at the CCF and the Communications Building maintained the Illinois Department of Central Management Services-Bureau of Communication and Computer Services-Occupant Evacuation Response Team Members (OERT), updated April 7, 2010.

The OERT was part of a packet which included a series of emails related to emergency procedures.

During our review, we noted the Department had developed emergency evacuation procedures, which had been provided to employees. However, the guards had not been provided the procedures.

The guards had not been provided the Department's emergency evacuation procedures.

Objective: Measures to prevent or mitigate threats have been implemented.

Department's Control: Controlled areas are protected against fire using smoke detectors and fire suppression systems. The smoke detectors and fire suppression system are tested periodically.

Tests Performed: Toured facilities and interviewed staff.

Test Results: The CCF third floor computer room contained fire suppression and detection systems that were Underwriter Laboratory approved and utilized an environmentally friendly gaseous agent, FM-200. Upon review, we noted the system was last inspected in February 2011.

The Communications Building contained a fire detection and suppression system throughout the entire facility. Upon review, we noted the system was last inspected in April 2011.

Additionally, we noted the fire extinguishers for both facilities were inspected during the review period.

No deviation noted.

Department's Control: Water detectors are installed within the raised floor area.

Tests Performed: Toured facilities and interviewed staff.

Test Results: Water detectors were installed within the raised floor area of the CCF. In the event sensors became damp, an alarm would sound in the Command Center.

No deviation noted.

Department's Control: The Central Computer Facility is supplied by two different power sources.

Tests Performed: Interviewed staff.

Test Results: The CCF was supplied by two different power sources.

No deviation noted.

Department's Control: The Central Computer Facility is equipped with an uninterruptible power supply (UPS).

Tests Performed: Toured facilities and interviewed staff.

Test Results: The CCF was equipped with a UPS. In the event of a power failure, the UPS would engage immediately drawing power from the battery farm and generators.

No deviation noted.

Willard Ice Building

Department's Description of Control: Procedures exist to restrict physical access over the Willard Ice Building:

- Security guards staff facilities 24/7.
- Proximity card readers that require unique access codes are located in the interior of the buildings to control and restrict access to controlled areas.
- Controlled areas are protected against fire using smoke detectors and fire suppression systems.
- The smoke detectors and fire suppression system are tested periodically.
- Controlled areas temperature and humidity are controlled and monitored.
- Controlled areas are protected with uninterruptible power supplies.
- Preventive maintenance agreements are in place.

Tests Performed: Toured facility and interviewed staff.

Test Results: On November 19, 2010, the Department moved the print shop to the Department of Revenue's Willard Ice Building.

We reviewed the security controls over the Willard Ice Building, noting:

- Security guards staffed the facility 24/7.
- Proximity card readers required unique access codes were located in the interior to control and restrict access to controlled areas.
- Controlled areas were protected against fire using smoke detectors and fire suppression systems.
- Controlled areas temperature and humidity were recorded, however we did note that there was no official use of the recorded readings.

Controlled areas were protected with uninterruptible power supplies and tested several times a year.

No deviation noted.

Clinton Facility

Department's Description of Control: Physical security controls over the Clinton Facility include:

- Security guards,
- Video cameras strategically located inside and outside the building,
- Proximity card readers requiring an active Access Card to allow entry, and
- Alarm System.

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 of Central Management Services.

The entrance to the building was unlocked during work hours. All employees were provided with an employee badge to permit access to the facility. A security guard monitored the entrance to the facility a few hours before and after work hours. The guard verified that employees were displaying their badge and required that visitors sign-in and were escorted by an employee. While a proximity key card system was present on the wall, it did not work. A second guard patrolled the facility during work hours.

After work hours the facility was locked. The facility was also equipped with an alarm system.

The facility was equipped with external cameras at the loading dock and front entrance, and internal cameras at the loading dock and fire alarm exits. These cameras were not working at the time of the tour.

The card reader and video cameras were not working properly.

Harris Facility

Department's Description of Control: Physical security controls over 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.

Tests Performed: Toured facility and interviewed staff.

Test Results: The Harris Facility computer room was located within a building occupied by the Department of Human Service (DHS). During our review, we found the following physical security controls were established to safeguard the Harris Facility:

- Security guards were on duty a few hours before and after work hours,
- Multiple video cameras were located inside and outside the building to provide viewable images for security guards and all were viewable by security guards, and
- Proximity card readers required an active access card for entry to restricted areas and were located throughout the facility.

No deviation noted.

OVERALL CONCLUSION

Based on the test results described above, the controls (with the exceptions of controls over granting, modifying, or revoking access badges) were operating with sufficient effectiveness to achieve the control objective.

To enhance controls, the Department should:

- Review all policies and procedures associated with granting, modifying and revoking physical access rights, as well as the collection of access cards and assignment and collection of real property keys. Specifically, the Department should:
    - Ensure proper accounting for real-property keys, in particular master keys.
    - Develop a mechanism to locate and account for all master keys currently unaccounted for.
    - Ensure policies and procedures provide for a consistent, repeatable, and timely process.
    - Ensure the defined process aligns with management's intentions and are in the best interest of all parties involved.
    - Ensure the defined process includes routinely reviewing the appropriateness of individual's access rights and keys assigned.
    - Ensure the defined process includes procedures specific to contractors and their assigned access rights and keys.
    - Ensure the defined process outlines documentation necessary to provide for an adequate audit trail.

    - Ensure policies and procedures are approved and distributed to all appropriate individuals.
- Ensure all access badges are deactivated in a timely manner.
- Ensure all access badges are collected upon departure and documentation is maintained.
- Develop a listing of individual who are authorized to approve access badges.
- Ensure information to assist in the performance of security guard duties is available and current.
- Ensure all card readers and cameras are properly working.

PRODUCTION CONTROL AND INPUT UNITS

EXISTING ENVIRONMENT

Objective: The Department has computer operations and job scheduling procedures which document procedures and instructions.

Department's Control: Production Control staff utilizes agency procedures to determine and define all batch processing schedules and to assist with problem determination and resolution.

Tests Performed: Reviewed SharePoint site, procedure acceptance forms, and interviewed staff.

Test Results: The Production Control staff utilized the agencies procedures to determine and define batch processing schedules and to assist with problem determinations and resolutions.

Department staff stated comprehensive and standardized production control policies and procedures had not been developed.

It was the responsibility of the agency to submit all the criteria, conditions, along with other supporting documentation, such as the Job Control Language (JCL) for a job to be run (agencies procedures).

Troubleshooting information would be provided by an agency and would be included in the JCL or the flowchart created by the Production Control Unit for after hours processing.

When the agency submitted a new job or a change to an existing job, a Proc Acceptance Form was submitted.

We reviewed 25 acceptance forms, noting the Department did not maintain a listing of individuals authorized to submit the forms.

In addition, we reviewed three new procedures requested during the review period, noting not all documentation was maintained. Additionally, the Department did not maintain a listing of individuals authorized to submit new procedures.

The Department had not standardized production control policies and procedures. In addition, the Department did not maintain all documentation and did not maintain a listing of individuals authorized to submit procedure acceptance forms.

Department's Control: The Computer Operations unit can use Visio flowcharting, historical data and or agency provided documentation to determine the job flow of batch processing scheduled by the Production Control unit.

Tests Performed: Reviewed flowcharts and interviewed staff.

Test Results: The Computer Operations unit utilized Visio flowcharts, historical data and agency documentation to determine the job flow of a batch processing scheduled by the Production Control Unit.

Flowcharts were created by the Production Control Unit for use during after-hours processing. Flowcharts were based on the information that was provided by the agency, which indicated the production process (jobs) and who to contact if a job would abend.

We reviewed the flowcharts for two agencies noting they contained the production process, timing of the job, and who to contact if the job would abend.

No deviation noted.

Department's Control: The Reporting Unit is responsible for setting up and maintaining reports produced from the agencies and placing them in Mobius for electronic viewing, archival and retrieval.

Tests Performed: Reviewed Mobius and interviewed staff.

Test Results: The Reporting Unit was responsible for setting up and maintaining agency-produced reports in Mobius.

Security software restricted the ability to view or print 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.

The Reporting Unit would change access rights to Mobius for an employee when an agency sent a request for the change. However, the Department did not maintain a listing of individuals who were authorized to request or change access rights.

The Department did not maintain a listing of individuals who were authorized to request or change access rights.

Department's Control: Production Control staff monitors the JCL of scheduled batch processing for any abnormal conditions and modifies as necessary before programs are processed, reran or set up for the next schedule.

Tests Performed: Interviewed staff.

Test Results: Production Control staff monitored the JCL of scheduled batch processing for abnormal conditions. Additionally, staff made modifications as necessary before programs were processed, rerun, or scheduled.

No deviation noted.

Objective: The Department provides a batch job monitoring and problem resolution service to the CMS, DHS, DOT, EPA, HFS and IDOR agencies.

Department's Control: Production Control utilizes automated scheduling system CA-Scheduler to control and schedule the batch processing for assigned agencies.

Tests Performed: Reviewed CA-Scheduler and interviewed staff.

Test Results: Production Control utilized CA-Scheduler to control and schedule batch processing for the Department, DHS, DOT, EPA and HFS.

The staff would monitor the jobs for the respective agencies and if a problem or abend would occur, then staff would contact the agencies from the call list.

No deviation noted.

Department's Control: Input Control utilizes the automated scheduling system, Zeke to control and schedule Department of Revenue batch processing.

Tests Performed: Reviewed Zeke and interviewed staff.

Test Results: Input Control utilized Zeke to control and monitor the Department of Revenue's batch processing.

Input Unit staff would utilize ZEKE to view and monitor the input and output queues, users, jobs, and tape drives. If there were problems or abends then staff would notify the individual assigned to the job.

No deviation noted.

Department's Control: The Bluezone emulation software is utilized to monitor all assigned processing.

Tests Performed: Reviewed Bluezone and interviewed staff.

Test Results: The Department utilized Bluezone emulation software to monitor assigned processing.

Input Control staff monitored the mainframe productions system utilizing Bluezone. Security software restricted access to Bluezone software.

No deviation noted.

Department's Control: Emergency (after-hours) program migrations from test to production status are performed at the request of agencies. These requests are forwarded to the Production Control unit for follow-up and to ensure documentation is accurately updated.

Tests Performed: Reviewed email and interviewed staff.

Test Results: The Production Control Unit would migrate programs from test to production during the day. After hours, the Input Control Unit would migrate programs from test to production.

The Input Control Unit would notify the Production Control Unit via email of any after hours migration.

No deviation noted.

Department's Control: Agency processing schedules and requests are submitted through shared e-mail addresses.

Tests Performed: Interviewed staff.

Test Results: Agency processing schedules and requests were submitted through a shared email address.

The Department had set up shared email addresses for the different groups within Production Control. The individuals that had access to the shared account were the supervisor of the group and staff members.

No deviation noted.

Department's Control: Production Control staff contact lists for problem resolution are maintained and available in SharePoint, e-mail and hardcopy.

Tests Performed: Reviewed contact list and interviewed staff.

Test Results: The Production Control staff contact lists were maintained and available on SharePoint, email, and hardcopy.

We reviewed the contact listing on SharePoint, noting staff names and contact numbers. Department staff stated email contact information was available via the email directory.

No deviation noted.

Department's Control: Problems are logged on daily shift reports and reviewed by supervisors, management and staff.

Tests Performed: Reviewed shift reports and interviewed staff.

Test Results: Problems were logged on the daily shift report. The supervisors, managers and staff reviewed the shift reports to ensure all appropriate action was taken, including follow up with an agency to determine if solutions to problems met their expectations.

We reviewed the daily shift reports for April 20, 2011, noting that not all jobs that had an abend had a contact listed. Department staff stated it was the responsibility of the submitting agency to provide the appropriate contacts for submitted jobs.

No deviation noted.

Department's Control: Shift reports are available to the agencies on SharePoint and the agency then controls internal access to these reports.

Tests Performed: Reviewed shift reports and interviewed staff.

Test Results: Shift reports were available to agencies via SharePoint. Access to the reports was the responsibility of the applicable agency.

We reviewed the SharePoint site for the daily shift reports for April 20, 2011, noting the site contained the reports.

No deviation noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. However, to strengthen the controls, we recommend the Department

- Develop standardized production control policies and procedures for use by all agencies.
- Develop a list of individuals authorized to submit job requests.
- Develop a list of individuals authorized to request updates to access rights to view or print jobs.

SECURITY SOFTWARE

EXISTING ENVIRONMENT

Objective: Procedures exist to restrict access to defined systems.

Department's Control: Access to the defined systems is granted to an authenticated user.

Tests Performed: Reviewed security reports, system options, security profiles, and interviewed staff.

Test Results: Access to the defined systems was granted to an authenticated user.

Resource Access Control Facility (RACF) security software was implemented to restrict access to defined systems. User IDs and passwords were used to identify and authenticate users and were key control mechanisms within RACF. RACF protected access and enforced user accountability over data and system resources by positively verifying the user's authority to utilize that data or system resource, and by logging the user's actions if a violation occurred.

No deviation noted.

Department's Control: Creation, reassignment or granting access to an ID requires the Enterprise Service Request (ESR) process.

Tests Performed: Interviewed staff.

Test Results: Creation, reassignment, or granting access to an ID required the ESR process.

No deviation noted.

Department's Control: Users are required to have a password and ID in order to gain access to the systems.

Tests Performed: Reviewed access listings and interviewed staff.

Test Results: Users were required to have an ID and valid password prior to gaining access to system resources.

We obtained a listing of IDs assigned to Department personnel and confirmed that a valid RACF ID and password was required before access was allowed.

No deviation noted.

Department's Control: All IDs have a default unit.

Tests Performed: Reviewed security profiles and interviewed staff.

Test Results: All IDs had a default unit. During our review of access privileges, we confirmed IDs (user profile) had a default group (unit).

No deviation noted.

Department's Control: Use of group or shared IDs are not permitted.

Tests Performed: Reviewed security ID listing for Department users and interviewed staff.

Test Results: Based on our review, it appeared that each user was assigned a unique ID. However, we identified some additional special purpose IDs that were not uniquely assigned to an individual. Department staff stated that due to turnover, some IDs that had been assigned to departed staff members (who were not replaced) were assigned to certain functional areas to allow the performance of special purpose functions.

Some special purpose IDs were not individually assigned.

Department's Control: Passwords are complex and require a specific syntax.

Tests Performed: Reviewed security reports, system options, and interviewed staff.

Test Results: Passwords were complex and required specific syntax.

On September 28, 2010, the Department issued a memorandum to agency users stating a new password standard was being established and was effective November 1, 2010.

No deviation noted.

Department's Control: Security configuration parameters force passwords to be changed in defined intervals.

Tests Performed: Reviewed system options and interviewed staff.

Test Results: Security configuration parameters forced passwords to be changed in defined intervals.

No deviation noted.

Department's Control: IDs are disabled after a defined number of unsuccessful login attempts.

Tests Performed: Reviewed system options.

Test Results: Security configuration forced IDs to be disabled after a defined number of unsuccessful login attempts.

No deviation noted.

Department's Control: Invalid access attempts are logged.

Tests Performed: Reviewed violation reports and interviewed staff.

Test Results: Invalid access attempts were logged.

No deviation noted.

Department's Control: Access violations are reviewed and investigated.

Tests Performed: Reviewed violation reports and interviewed staff.

Test Results: Department staff stated access violations were reviewed. See the Information Assurance section for additional information.

No deviation noted.

Department's Control: The ability to establish, modify or delete a user, or user access privileges, is limited to Security Administrators.

Tests Performed: Reviewed security reports and interviewed staff.

Test Results: The ability to establish, modify or delete a user, or user access privileges, was limited to Security Administrators.

No deviation noted.

Department's Control: The ability to establish, modify or delete an Admin account, or privileges, is limited to Security Administrators.

Tests Performed: Reviewed security reports and interviewed staff.

Test Results: The ability to establish, modify or delete an Administrator account, or privileges, was limited to Security Administrators.

No deviation noted.

Department's Control: Access to superuser functionality and sensitive system functions is restricted to authorized staff.

Tests Performed: Reviewed security profiles, security reports, and interviewed staff.

Test Results: Access to superuser functionality and sensitive system functions was restricted to authorized staff.

No deviation noted.

Department's Control: Access to data and system resources is based on the ID and role-based units.

Tests Performed: Reviewed individual and group security profiles and interviewed staff.

Test Results: Access to data and system resources was based on the ID and role-based units.

No deviation noted.

Department's Control: IP activity is limited to those IDs with an identifier field on both the ID and the IDs default unit.

Tests Performed: Reviewed security reports, security profiles, and interviewed staff.

Test Results: IP activity was limited to those IDs having an identifier field on both the ID and the IDs default unit.

No deviation noted.

Department's Control: Production and Test data is protected by a general profile or specific profile.

Tests Performed: Reviewed security profiles and interviewed staff.

Test Results: Production and test data was protected by a security profile.

No deviation noted.

Department's Control: Verification is sent to the agencies on a semi-annual basis for the verification of agency RACF coordinators.

Tests Performed: Reviewed security verification memorandum and interviewed staff.

Test Results: A Security Authorization List Updates memorandum was sent to user agencies on May 15, 2011. The previous update memorandum was sent to user agencies in March 2010.

The verification of RACF Coordinators was performed annually rather than semi-annually.

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:

- Ensure the verification of RACF Coordinators is distributed and verified semi-annually.
- Ensure all IDs are individually assigned to promote accountability and eliminate sharing.

SERVICE COMMUNICATIONS

EXISTING ENVIRONMENT

Objective: The Department and User Agencies are provided with access to information regarding the Department and the services it provides.

Department's Control: Periodic meetings are held with the User Agencies to share information regarding the Department and the services it provides.

Tests Performed: Reviewed agendas and interviewed staff.

Test Results: Periodic meetings were held to share information regarding the Department and services.

No deviation noted.

Department's Control: The BCCS Service Catalog is available online and outlines information on most available services and rates.

Tests Performed: Reviewed BCCS Service Catalog.

Test Results: The BCCS Service Catalog was available on the Department's website. The Catalog provided information related to five categories of service, along with specific services available for each category.

The BCCS Service Catalog also provided a listing of rates for several of the Department's services.

No deviation noted.

Department's Control: The BCCS website serves as a central location for communicating information about available services, policies and procedures, contact information, forms and guides for requesting services, announcements/bulletins, and a variety of other information to the Department and its User Agencies.

Tests Performed: Reviewed website and interviewed staff.

Test Results: The Department's website provided a central location for communicating information related to available services, policies and procedures, contact information, forms and guides for requesting services, announcements, and other information.

No deviation noted.

Department's Control: Quarterly newsletters, memos and bulletins regarding Department changes, updates and notifications are produced and distributed to the Department and its User Agencies.

Tests Performed: Reviewed newsletters, bulletins, notifications, and interviewed staff.

Test Results: The Department distributed various communications to the Department's staff and its users. In addition, the Department posted newsletters, bulletins and memos on the website.

No deviation noted.

Objective: The Department provides avenues for User Agencies to submit and receive information on incidents, service requests and changes.

Department's Control: User Agencies can submit incidents and service requests via e-mail or phone for processing and tracking by the Department. The Department provides and maintains status information via the Remedy Service Desk System as well as by offering additional ad-hoc reporting capabilities to User Agencies.

Tests Performed: Reviewed Remedy and interviewed staff.

Test Results: User agencies could submit incidents and service request via email or phone for processing.

The Remedy system logged, tracked, and monitored tickets.

No deviation noted.

Department's Control: An Enterprise Change Management (ECM) website is maintained to provide an updated listing of scheduled changes, stakeholders, and affected parties.

Tests Performed: Reviewed SharePoint site and meeting minutes.

Test Results: Changes were communicated to users through Change Advisory Committee (CAC) meetings and reports on the ECM SharePoint site.

The ECM SharePoint site maintained various reports to inform the users:

- Change Advisory Committee Meeting Minutes
- 30 Day Outage Report by Agency
- Change Detail Report (Next 14 Days)
- Enterprise Change Schedule (Next 90 Days)
- Overdue Change Report.

We reviewed the reports and meetings from the ECM SharePoint Site for July 2010 - January 2011, noting information related to changes.

Each agency had access to the SharePoint site to view reports and meeting minutes. Emails were sent to all agencies identifying the changes to be discussed at the upcoming CAC meeting and the email included a link to the SharePoint site.

No deviation noted.

Objective: The Department and select User Agencies are provided with access to data and reports related to service delivery and performance.

Department's Control: Various reporting systems that provide service delivery and performance monitoring capabilities are available to select User Agencies and Department managers.

Tests Performed: Reviewed reports and interviewed staff.

Test Results: The Department provided selected agencies access to various reports in order to monitor services.

The Department maintained reports for management and agencies to monitor.

- IT Shared Services Open Ticket Report,
- BCCS Performance Reports, and
- Various report from Remedy related to Change Management and Help Desk.

No deviation noted.

Department's Control: The Enterprise Program Management (EPM) system is used to track and provide status on ongoing service related projects, initiatives, and reporting.

Tests Performed: Reviewed EPM documentation and interviewed staff.

Test Results: The Department utilized the EPM system to track and monitor service related projects, initiatives, and reporting.

No deviation noted.

Objective: User Agencies are provided a means to discuss and resolve issues regarding the services the Department provides.

Department's Control: Periodic meetings are held with User Agency Telecom Coordinators to share information and to address User Agency service concerns.

Tests Performed: Interviewed staff.

Test Results: The Department held a meeting during the review period in which they provided information to the Telecom Coordinators.

No deviation noted.

Department's Control: Meetings are held upon request of the User Agency to discuss and resolve service related issues.

Tests Performed: Reviewed meeting agendas, minutes, summit agendas, calendars, and interviewed staff.

Test Results: The Department held meetings with agencies to discuss issues.

We reviewed the Priority Meeting and BCCS Leadership meeting minutes, noting meetings were held to discuss issues.

No deviation noted.

Department's Control: E-mail boxes are available that allow User Agencies to submit service related questions or concerns. In addition, User Agencies may also contact the Customer Service Center (CSC) with any service questions or concerns.

Tests Performed: Interviewed staff.

Test Results: The Department made email boxes available to agencies for the submittal of service related questions or concerns. In addition, the agencies could contact the CSC with any questions.

No deviation noted.

OVERALL CONCLUSION

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

STORAGE AND BACKUP

EXISTING ENVIRONMENT

Objective: Procedures are in place to restrict access to resources.

Department's Control: RACF administrator assigns a RACF ID after receiving approval from staff supervisor.

Test Performed: Reviewed security reports and interviewed staff.

Test Results: To obtain a RACF ID, a Mainframe Request form was completed and submitted through the Enterprise Service Request (ESR) process. The form was assigned to the Enterprise Storage & Backup's (ESB) RACF Coordinator to grant and remove access to ESB resources. Department staff stated there had been no new staff during the review period.

No deviation noted.

Department's Control: Resources are secure utilizing RACF.

Test Performed: Reviewed security profiles and interviewed staff.

Test Results: RACF security software was utilized to secure systems and resources. To access systems and resources, users were required to have a valid RACF User ID and password.

No deviation noted.

Department's Control: Access to offline storage, backup data, systems and media is limited to authorized staff.

Test Performed: Reviewed security profiles and interviewed staff.

Test Results: We reviewed the security profiles of ESB staff members to determine if access was reasonable, noting no exceptions.

No deviation noted.

Objective: Procedures are in place to guide storage activities.

Department's Control: System automation is utilized to control and monitor storage levels.

Test Performed: Reviewed email alerts and interviewed staff.

Test Results: System automation was utilized to control and monitor storage levels. ESB staff managed and maintained both shared and private storage pools. System automation was utilized to monitor the performance and availability of storage pools.

No deviation noted.

Department's Control: Thresholds are included in Storage Pool listings.

Test Performed: Reviewed listing of storage pools, storage pool capacity, and interviewed staff.

Test Results: ESB maintained a listing of storage pools maintained. The list identified the pools by system, and whether the pool was a shared or private storage pool.

To monitor current capacity levels for storage pools, ESB staff reviewed online reports showing current capacity levels for each storage pool. Management indicated they reviewed these reports daily and identified pools which were at utilization rates of 90% or more.

No deviation noted.

Department's Control: The Command Center monitors thresholds after hours and notifies ESB staff if thresholds exceed limits.

Test Performed: Reviewed shift reports and interviewed staff.

Test Results: The Command Center staff monitored the capacities of storage pools after hours and notified ESB staff when thresholds exceeded limits.

No deviation noted.

Department's Control: Users are notified by ESB staff if thresholds are exceeded.

Test Performed: Interviewed staff.

Test Results: When a storage capacity threshold was exceeded, ESB staff would contact the agency to alert them to current capacity levels.

No deviation noted.

Department's Control: Users complete an Enterprise Service Request which initiates the completion of a Request For Change to request additional disk space. Additional disk space is allocated by ESB staff utilizing documented instructions.

Test Performed: Reviewed procedures, ESR tickets, and interviewed staff.

Test Results: ESB staff was responsible for allocating additional disk space. To allocate additional disk space, ESB staff utilized procedures which documented detailed steps for disk addition and required the completion of the DASD Addition Checklist.

When additional disk space was necessary, users opened an ESR ticket. After a ticket was opened, an email was automatically generated and sent to the ESB team member assigned to the task.

We reviewed four ESR tickets for adding disk space in a three month period, noting no exceptions.

No deviation noted.

Department's Control: Users complete an Enterprise Service Request which initiates the completion of a Request for Change to request deletion of disk space by ESB. Deletion of disk space is performed by ESB staff utilizing documented instructions.

Test Performed: Reviewed procedures, ESR tickets, and interviewed staff.

Test Results: ESB was responsible for removing disk space. To remove disk space, ESB staff utilized procedures which documented detailed steps to return DASD to spare status and required the completion of the DASD Removal Checklist.

When removal of disk space was necessary, users opened an ESR. After a ticket was opened, an email was automatically generated and sent to the ESB team member assigned to the task.

We reviewed the one ESR ticket for removing disk pace in a three month period, noting no exceptions.

No deviation noted.

Objective: Procedures are in place to guide backup activities.

Department's Control: Automated software is utilized to control and schedule backups.

Test Performed: Reviewed backup schedules and interviewed staff.

Test Results: ESB staff utilized CA-Scheduler to control and schedule backups. All systems were scheduled within CA-Scheduler to be backed up on a routine basis.

No deviation noted.

Department's Control: Actual backup schedules are reviewed against the defined backup schedule.

Test Performed: Reviewed procedures, backup schedules, and interviewed staff.

Test Results: ESB was responsible for reviewing defined backup schedules and ensuring that backups ran as scheduled.

To document backup jobs scheduled in CA-Scheduler and assist with verifying that all backups were successful, ESB staff reviewed and maintained the CA-Scheduler Verify Backups document.

No deviation noted.

Department's Control: Backups are tracked through CA-Scheduler.

Test Performed: Reviewed backup logs and interviewed staff.

Test Results: Backups were tracked through CA-Scheduler backup logs. The logs detailed the backup jobs submitted via CA-Scheduler for processing and identified jobs, via condition codes, that processed successfully and jobs which had problems.

No deviation noted.

Objective: Procedures are in place to control verification of backups.

Department's Control: ESB Staff monitors successful completion of backups by utilizing documented instructions.

Test Performed: Reviewed procedures and interviewed staff.

Test Results: To assist in monitoring the successful completion of backups, ESB staff maintained the procedures, which documented detailed steps to be performed to ensure the successful completion of backup jobs.

No deviation noted.

Department's Control: ESB staff is notified of failed backups.

Test Performed: Reviewed procedures, shift reports, and interviewed staff.

Test Results: ESB staff monitored CA-Scheduler daily for any issues related to the scheduled backups. ESB staff would identify any failed backups during the review of the history log.

No deviation noted.

Department's Control: Users are notified of failed backups.

Test Performed: Reviewed procedures and interviewed staff.

Test Results: Instructions documented the procedure to notify user agencies of failed backups.

No deviation noted.

Department's Control: ESB uses restoration procedures after receiving a Help Desk Ticket requesting the restoration of data.

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

Test Results: ESB staff was responsible for restoring disk space. To restore disk space, ESB staff utilized the procedures which documented detailed steps for restores.

We reviewed the one Help Desk ticket for restoring disk space in a three month period, noting no exceptions.

No deviation noted.

OVERALL CONCLUSION

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

STRATEGIC PLANNING

EXISTING ENVIRONMENT

Objective: Defined goals are required to properly align the Bureau's strategic plan with the mission and objectives of the State, Department and user entities.

Department's Control: Management has periodic meetings with the State CIO and Department senior management to define direction and objectives.

Tests Performed: Reviewed meeting agendas, minutes, calendars, and interviewed staff.

Test Results: Management and other leaders held regular meetings to define direction and objectives.

We reviewed the Priority Meeting and Bureau Leadership meeting agendas, noting meetings were held to review strategies, directions, and objectives.

No deviation noted.

Department's Control: Management conducts periodic meetings with consolidated agencies, Illinois State Police, Department of Children and Family Services, and the Department of Corrections to provide updates on technology initiatives, discuss technology needs, issues, and strategic plans.

Tests Performed: Reviewed meeting agendas, minutes, summit agendas, calendars, and interviewed staff.

Test Results: Management held regular meetings to discuss technology needs, issues, and strategic plans with state agencies.

We reviewed the Priority Meeting and Bureau Leadership meeting agendas, noting meetings were held to discuss technology needs, issues, and strategic plans.

In addition, the Department was actively involved in the Illinois Digital Government Summit (September 2010) and the Cyber Security Summit (October 2010) that provided an avenue to present updates on technology initiatives, technology issues, and strategic plans to agency management throughout state government.

No deviation noted.

Department's Control: Management conducts periodic meetings with State Agency CIOs and Senior IT managers to share information and solicit discussion on broad issues that may affect the use of technology in Illinois Government. Agendas are provided and handout materials are

distributed as is warranted. Management meets frequently with individual user entities to discuss various topics including direction and objectives.

Tests Performed: Reviewed meeting agendas, minutes, summit agendas, calendars, and interviewed staff.

Test Results: Management and other leaders held regular meetings to discuss technology issues.

We reviewed the Priority Meeting and Bureau Leadership meeting agendas, noting meetings were held to discuss technology issues.

In addition, the Department was actively involved in the Illinois Digital Government Summit (September 2010) and the Cyber Security Summit (October 2010) that provided an avenue to present updates on technology initiatives, discuss technology needs, issues, and strategic plans to agency management throughout state government.

No deviation noted.

Department's Control: BCCS determines its goals by analyzing the needs of user agencies, changes in technology and trends in the industry, and the direction given by Department management and the Governor's Office.

Tests Performed: Reviewed Strategic Priorities Initiative Summary and interviewed staff.

Test Results: A draft version of the Strategic Priorities Initiative Summary (Summary) was developed in December 2010. The draft Summary contained the following section:

Bureau Strategic Goals:

- Cost Savings - Reduce ongoing information Technology and Telecommunications related operational costs and expand revenue sources.
- Innovation & Transformation - Transform and mature BCCS service delivery capabilities by promoting innovation and standardization of technology-enabled business solutions to create sustainable business value.
- Optimization - Optimize business processes and best practices to create operational efficiencies and provide high quality, low cost IT and Telecommunication services.
- Service - Ensure access to and delivery of secure, available, and reliable IT and Telecommunication services and technology solutions to the State of Illinois.

The Acting Deputy Director of the Bureau stated the draft Summary was being used as a general guide.

No deviation noted.

Objective: Research and information regarding technology and trends in Government and the industry is utilized in setting goals.

Department's Control: Management and technical subject matter experts meet and request information on a regular basis from existing vendors, other technology providers, and industry experts to monitor technology trends.

Tests Performed: Reviewed meeting agendas, minutes, summit agendas, calendars, Gartner subscription, and interviewed staff.

Test Results: We reviewed the Priority Meeting and Bureau Leadership meeting agendas, noting meetings were held to discuss technology issues.

In addition, the Illinois Digital Government Summit and the Cyber Security Summit included presentations from vendors and industry experts.

The Gartner subscription provided: executive programs research reports; access to all Gartner for IT executives role web portals; teleconferences; access to Gartner core research; access to Gartner for IT leaders content and role pages; and the talking technology series.

No deviation noted.

Department's Control: Management receives information on technology options through the Request for Information and procurement processes.

Tests Performed: Reviewed the Illinois Procurement Bulletin.

Test Results: The Illinois Procurement Bulletin had multiple solicitations and notices that contained information on technology options.

No deviation noted.

Objective: Management monitors progress of specific projects and activities that arise from the strategic plan.

Department's Control: Processes exist for management to track the progression of all priority projects and procurements through the Enterprise Project Management (EPM) Portal.

Tests Performed: Reviewed EPM brochure, workflow diagram, and reports.

Test Results: We found that processes existed for management to track the progression of all priority projects and procurements through the EPM Portal. In addition, reports regarding priority projects were available from the EPM portal.

No deviation noted.

Department's Control: Management holds priority project meetings on a regular basis to track and discuss the progression of all priority projects and procurements using reports from the EPM portal.

Tests Performed: Reviewed meeting agendas, minutes, summit agendas, calendars, EPM reports, and interviewed staff.

Test Results: We reviewed the Priority Meeting and Bureau Leadership meeting agendas, noting meetings were held to discuss priority projects and procurements.

In addition, reports regarding priority projects were available from the EPM portal.

No deviation noted.

Department's Control: Management holds executive leadership meetings and manager meetings to discuss activities and progress toward goals.

Tests Performed: Reviewed meeting agendas, minutes, calendars, and interviewed staff.

Test Results: Management and other leaders held regular meetings to discuss activities and progress toward goals.

We reviewed the Priority Meeting and Bureau Leadership meeting agendas, noting meetings were held to discuss activities and progress toward goals.

No deviation noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance the controls, the Department should formally approve and publish the Summary. In addition, the Summary should be reviewed and updated at least annually.

SYSTEM SOFTWARE

The Department provides mainframe hosting environments for agencies and other entities. System software includes:

- z/OS (Zero Downtime Operating System)
- z/VM (Zero Downtime Virtual Machine)
- CICS (Customer Information Control System)
- DB2 (Database 2)
- IMS (Information Management System)
- IDMS/R – Integrated Database Management System/Relational

EXISTING ENVIRONMENT

Objective: Procedures exist to maintain system components consistent with defined system policies.

Department's Control: An up-to-date listing of all software and their respective level, version and patch is maintained.

Tests Performed: Reviewed a listing of software utilized and interviewed staff.

Test Results: An updated listing of all software and their respective level, version and patch was maintained.

No deviation noted.

Department's Control: Changes to the environment follow the Department's Change Management Process.

Tests Performed: Reviewed a listing of system software changes and interviewed staff.

Test Results: The Department utilized the Remedy Change Management application and followed the Department's Change Management process for approving and documenting changes made within the IMS environment.

We obtained and reviewed listings of changes generated from the Remedy Change Management application, noting no exceptions.

No deviation noted.

Department's Control: The assigned CMS technician is responsible for ensuring all software is maintained at latest version/level/patch.

Tests Performed: Reviewed software version levels, vendor's website, and interviewed staff.

Test Results: The assigned CMS technician was responsible for ensuring all software was maintained at latest version/level/patch. We confirmed that the current versions of software were listed as a supported product on the vendor's website.

No deviation noted.

Objective: Procedures exist to protect against unauthorized access to system resources.

Department's Control: System logs are utilized to monitor the environment.

Tests Performed: Reviewed reports, logs, and interviewed staff.

Test Results: Department staff reviewed logs and reports for performance monitoring system software.

We reviewed several reports and logs utilized for performance monitoring of system software.

No deviation noted.

Department's Control: Success/failure events are logged.

Tests Performed: Reviewed logs and interviewed staff.

Test Results: We reviewed several logs that contained information on system activity, transaction processes, and system use.

No deviation noted.

Department's Control: The Chief Security Officer is notified of potential security issues/breaches.

Tests Performed: Reviewed security procedures, breach notification procedures, and interviewed staff.

Test Results: Procedures existed to notify the Chief Security Officer of potential security issues/breaches. Per Department staff, no security breaches were identified during the review period that required notification.

No deviation noted.

Objective: Procedures exist to restrict access to resources.

Department's Control: Security software is used to control access to systems and resources.

Tests Performed: Reviewed security profiles, system options, and interviewed staff.

Test Results: System software integrated with Resource Access Control Facility (RACF) security software. Users must have a valid RACF ID and password before they could gain access to resources.

No deviation noted.

Department's Control: The Enterprise Service Request (ESR) is used to request access to systems and resources.

Tests Performed: Interviewed staff.

Test Results: Department staff stated they would utilize the ESR process for approving and documenting access requests.

We noted there had been no requests for access to system software resources and no additions to system software staff during the review period.

No deviation noted.

Objective: The Department's mainframe environment availability and performance is monitored and reviewed.

Department's Control: Automated tools are utilized in monitoring the performance and availability of the environment.

Tests Performed: Reviewed reports, logs, tools, and interviewed staff.

Test Results: Department staff reviewed logs, reports, and diagnostic tools to monitor availability and performance of system software.

No deviation noted.

Department's Control: Events are logged and reviewed by the assigned CMS technician.

Tests Performed: Reviewed logs and interviewed staff.

Test Results: We reviewed internal and external system logs, accounting logs, and system logs and noted the logs contained data to diagnose problems that occur in the system, and transaction processing.

No deviation noted.

Department's Control: System performance, availability, and capacity requirements are monitored and reviewed by CMS management.

Tests Performed: Reviewed reports, logs, support levels, and interviewed staff.

Test Results: System performance, availability, and capacity requirements were monitored and reviewed by management.

No deviation noted.

OVERALL CONCLUSION

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

This Page Intentionally Left Blank

APPLICATION CONTROLS

Application controls are the methods, policies, and procedures adopted by an organization to ensure all transactions are entered, processed, and reported correctly. Application controls ensure data being entered, processed, and stored are complete and accurate. They ensure the output from the computer application is timely and accurate.

Application controls can be grouped into three areas: input; processing; and output. Input controls ensure the data entered into the system are authorized and accurate. These controls include both manual and computerized techniques. Processing controls are those that are coded into the software program. Manual procedures often supplement the programmed controls to verify that all processing has taken place as intended. Output controls govern the printing and distribution of reports. Specific control objectives are imbedded in the Department's Description of System.

The Department has developed several applications for use by State agencies. As part of the Service Organization 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.

The **Accounting Information System** (AIS) is an automated expenditure control and invoice voucher processing system utilized by State agencies. Appropriation, obligation, cash and vendor processing functions support the invoice processing. AIS allocates invoice amounts into sub accounts and allows users to track cost centers. Vouchers are created in AIS according to the Comptroller's Statewide Accounting Management System (SAMS) procedures. AIS was utilized by 56 entities. (See page 140 for a list of user agencies).

The **Central Payroll System** (CPS) CPS was designed to provide assistance in preparing payrolls for state agencies. 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 was utilized by 77 entities. (See page 146 for a list of user agencies).

The **Central Inventory System** (CIS) is an automated asset inventory control system which also allows the user agency to track depreciation if they request. 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 was utilized by 22 entities. (See page 152 for a list of user agencies).

The **Central Time and Attendance System** (CTAS) The CTAS is an online system used to maintain "available benefit time". CTAS provides for attendance information to be recorded using either the positive or exception method. CTAS was utilized by 35 entities. (See page 157 for a list of user agencies).

ACCOUNTING INFORMATION SYSTEM (AIS)

EXISTING ENVIRONMENT

Objective: Structured software development methodology is utilized to manage any new developments or enhancements to existing software code to ensure that only authorized, tested and documented developments and enhancements are made to the application.

Department's Control: All application developments and enhancements are controlled in accordance with the Application Systems Development Methodology Manual.

Tests Performed: Reviewed the Application Systems Development (ASD) Methodology Manual (Methodology) and interviewed staff.

Test Results: The Methodology, revised August 2005, was "created to provide a structured process for the design, development and implementation of new systems, enhancements and maintenance to existing systems and for development of ad hoc requests."

No deviation noted.

Department's Control: New application developments and enhancements are documented through the use of a Service Request Form (SR) and are documented in the Service Request Registration System (SRRS).

Tests Performed: Reviewed Application System Development Methodology Manual, Service Requests, and interviewed staff.

Test Results: The Department utilized the Service Request Registration System and Service Request Form to document new developments and enhancements.

According to management, there were no application developments or enhancements to AIS during the review period.

No deviation noted.

Department's Control: New application developments and enhancements are approved and tested before implementation into the production environment.

Tests Performed: Reviewed Application Systems Development Methodology Manual and interviewed staff.

Test Results: The Application Systems Development Methodology Manual required developments and enhancements to be approved and tested before implementation into the production environment.

According to management, there were no application developments or enhancements to AIS during the review period.

No deviation noted.

Department's Control: New developments, enhancements, and changes are moved into production by the Library Control Group.

Tests Performed: Reviewed service requests, Program Library Procedures and interviewed staff.

Test Results: The Program Library Procedures outlined the requirements utilized for new programs and modification to existing programs.

We reviewed the docuemnation supporting the two maintanence changes, noting no exceptions.

No deviation noted.

Department's Control: Affected program documentation is updated as part of system developments or enhancements required to comply with the Information Technology Governance (ITG) process.

Tests Performed: Reviewed service requests and interviewed staff.

Test Results: As part of the process, system documentation was to be reviewed and updated as applicable.

During the review period, there were no system developments or enhancements that required updates to system documentation.

No deviation noted.

Department's Control: System Users are informed when an application development or enhancement will affect them.

Tests Performed: Reviewed communication and interviewed staff.

Test Results: Communications regarding changes which affect users were sent via email.

According to management, there were no application developments or enhancements to AIS during the review period. However, the Department sent one email communication regarding the purge of old data.

No deviation noted.

Objective: Quality Assurance procedures monitor compliance with system development and change processes.

Department's Control: A technical verification is conducted to ensure the quality and completeness of each new application development or enhancement.

Tests Performed: Reviewed EBAS Quality Assurance procedures and interviewed staff.

Test Results: The Quality Assurance 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 review period were required to follow the QA procedures.

No deviation noted.

Objective: Processes exist to restrict logical access to AIS.

Department's Control: A checklist with the necessary security tasks is completed when new user agencies are added.

Tests Performed: Reviewed AIS Agency Setup Task list and interviewed staff.

Test Results: When a new agency was added as a user to AIS, the AIS Agency Setup Task list was completed.

There was one new agency added during the review period. We reviewed the AIS Agency Setup Task list, noting it had been completed.

No deviation noted.

Department's Control: Each AIS user agency has a Security Administrator who is responsible for adding new users. That process is the responsibility of the user agency.

Tests Performed: Interviewed staff.

Test Results: Assignment and authorization of access rights were the responsibility of each agency's security administrator.

No deviation noted.

Department's Control: Security software is used to control access.

Tests Performed: Reviewed the Mainframe Security Procedures, appropriateness of individuals with access to AIS, AIS User Manual, sign-on process, and interviewed staff.

Test Results: Access to AIS was controlled through security software (Resource Access Control Facility (RACF)). Users must have a properly authorized security software user ID and password to gain access to the operating environment.

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 Department staff members to AIS, noting no exceptions. However, an access rights list of Department staff members contained the names of seven staff members who were no longer employed by the Department.

The access rights list was not periodically reviewed and updated.

Department's Control: AIS internal security is used to enable and limit user capabilities.

Tests Performed: Reviewed the AIS User Manual, sign-on process, and interviewed staff.

Test Results: Once access to the operating environment was obtained, users must use a separate application user ID and password to gain access to AIS.

No deviation noted.

Department's Control: Assignment and authorization of access rights are the responsibility of the user agency.

Tests Performed: Interviewed staff.

Test Results: Assignment and authorization of access rights were the responsibility of each agency's security administrator.

No deviation noted.

Objective: The AIS User Manual outlines the procedures related to completeness, accuracy, timeliness and authorization of transactions.

Department's Control: Data requirements exist to force correction of errors and completion of critical fields before a transaction is accepted.

Tests Performed: Reviewed AIS User Manual, system edits, agency data, and interviewed staff.

Test Results: Data entered into the system was the responsibility of the user agency. AIS 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.

The accuracy and reconciliation of data was the responsibility of the user agency.

We reviewed three specific edits, noting no exceptions.

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 66,927 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 deviation noted.

Department's Control: AIS provides various reports to assist the users in verifying and balancing transactions.

Tests Performed: Reviewed AIS User Manual, AIS reports, and interviewed staff.

Test Results: The AIS User Manual provided a listing of various online and batch reports.

We reviewed a sample of daily, weekly, monthly, and other reports, noting no exceptions.

No deviation noted.

Department's Control: Entry, authorization and integrity of data are the responsibility of the user agency.

Tests Performed: Interviewed staff.

Test Results: Entry, authorization, and integrity of data were the responsibility of the user agency.

No deviation noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance the controls, the Department should periodically review access rights to AIS, ensure access is appropriate, and update the access rights list.

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 Insurance
9. Department of Labor
10. Department of Juvenile Justice
11. Department of Military Affairs
12. Department of Natural Resources
13. Department of Public Health
14. Department of Revenue
15. Department on Aging
16. Department of Veterans' Affairs
17. Environmental Protection Agency
18. General Assembly Retirement System
19. Guardianship and Advocacy Commission
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 Emergency Management Agency
30. Illinois Gaming Board
31. Illinois Labor Relations Board
32. Illinois Law Enforcement Training and Standards Board
33. Illinois Office of the State's Attorneys Appellate Prosecutor
34. Illinois Power Agency
35. Illinois Prisoner Review Board
36. Illinois Procurement Policy Board
37. Illinois Racing Board
38. Illinois Student Assistance Commission
39. Illinois Violence Prevention Authority
40. Illinois Workers' Compensation Commission
41. Judges' Retirement System
42. Judicial Inquiry Board
43. Office of Management and Budget
44. Office of the Attorney General
45. Office of the Auditor General
46. Office of the Executive Inspector General
47. Office of the Governor
48. Office of the Lieutenant Governor
49. Office of the State Appellate Defender
50. Office of the State Fire Marshal
51. Property Tax Appeal Board
52. State Board of Elections
53. State Employees' Retirement System
54. State Police Merit Board
55. State Universities Civil Service System
56. Supreme Court of Illinois

CENTRAL PAYROLL SYSTEM (CPS)

EXISTING ENVIRONMENT

Objective: A structured software development methodology is utilized to manage any new developments, any enhancements and maintenance to existing code to ensure only authorized, tested and documented developments and changes are made to the application.

Department's Control: Changes are logged, tracked, and approved through the EPM process.

Tests Performed: Reviewed EPM process and interviewed staff.

Test Results: The Department utilized the Enterprise Project Management (EPM) process for logging and tracking changes. In addition, since updates to EPM were restricted to managers, the information for a particular change was in effect approved by the manager updating the record.

The Department had a process to log and track changes at an overview level.

No deviation noted.

Department's Control: New developments, enhancements, and changes are approved and tested before implementation into the production environment.

Tests Performed: Reviewed changes and interviewed staff.

Test Results: According to management, there were no major changes to CPS during the review period. The Department did have one change request for routine maintenance (updates related to union contract provisions, tax laws, and employee benefit choices) during the review period.

No deviation noted.

Department's Control: New developments, enhancements, and changes are moved into production by the Library Control Group.

Tests Performed: Reviewed changes, Program Library Procedures, and interviewed staff.

Test Results: The Program Library Procedures outlined the requirements utilized for new programs, and modifications to existing programs.

We reviewed the documentation supporting the routine maintenance change, noting no exceptions.

No deviation noted.

Department's Control: Affected program documentation is updated as part of system developments or enhancements required to comply with the Information Technology Governance (ITG) process.

Tests Performed: Reviewed changes and interviewed staff.

Test Results: As part of the process, system documentation was to be reviewed and updated as applicable.

During the review period, there were no system developments or enhancements that required updates to system documentation.

No deviation noted.

Department's Control: System Users are informed when a system development or enhancement will affect them.

Tests Performed: Reviewed communications and interviewed staff.

Test Results: Communications regarding changes which affect users were sent via email.

The Department sent two email communications regarding fiscal year end changes and calendar year end changes to users.

No deviation noted.

Objective: Processes exist to restrict logical access to CPS.

Department's Control: A checklist with the necessary security tasks is completed when new user agencies are added.

Tests Performed: Reviewed Central Payroll Agency Information Sheet and interviewed staff.

Test Results: When a new agency was added as a user of the Central Payroll system, the Central Payroll Agency Information Sheet was completed. The Sheet documented the agency's payroll clerk and who was authorized to pickup payroll reports.

There were no agencies added during the review period.

No deviation noted.

Department's Control: Each CPS user agency has a Security Administrator who is responsible for adding new users. That process is the responsibility of the user agency.

Tests Performed: Interviewed staff.

Test Results: Assignment and authorization of access rights were the responsibility of each agency's security administrator.

No deviation noted.

Department's Control: Security software is used to control access.

Tests Performed: Reviewed the Mainframe Security Procedures, appropriateness of individuals with access to CPS, CPS User Manual, sign-on process, and interviewed staff.

Test Results: Access to CPS was controlled through security software (Resource Access Control Facility (RACF)). Users must have a properly authorized security software user ID and password to gain access to the operating environment.

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 Department employee access rights, noting no exceptions.

No deviation noted.

Department's Control: CPS internal security is used to enable and limit user capabilities.

Tests Performed: Reviewed the CPS User Manual, sign-on process, and interviewed staff.

Test Results: Once access to the operating environment was obtained, users must use a separate application user ID and password to gain access to CPS.

No deviation noted.

Department's Control: Assignment and authorization of access rights are the responsibility of the user agency.

Tests Performed: Interviewed staff.

Test Results: Assignment and authorization of access rights were the responsibility of each agency's security administrator.

No deviation noted.

Objective: The CPS User Manual outlines the procedures related to completeness, accuracy, timeliness, and authorization of transactions.

Department's Control: Data requirements exist to force correction of errors and completion of critical fields before a transaction is accepted.

Tests Performed: Reviewed CPS User Manual, system edits, 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.

The online data entry function had error codes and corresponding messages, which were displayed online when an error occurred, and the field that had the error in it was highlighted. Although the error messages were not discussed directly in the CPS Manual, the messages were understandable, and the CPS Manual identified acceptable values for the field.

After the data is entered successfully, the CPS staff executed a Gross-to-Net program, which processed the batch transactions for any errors and generated a Tentative Vouchers Report. If no errors occurred, a copy of the Tentative Vouchers Report was forwarded to the agencies for approval prior to being submitted to the Comptroller's Office for warrant generation. If an error occurred, it was identified on the report, which also contained payroll totals and statistics. The totals and statistics were used by CPS staff to ensure that all payrolls had been processed. If an error occurred and could be fixed, the CPS staff would fix the error, reschedule another voucher and complete a Payroll Adjustment form. The Payroll Adjustment forms were used to notify the agency of the error/correction.

We reviewed 13 specific edits, noting no exceptions.

During our review, we selected two agencies' CPS data and tested employee identification numbers, voucher numbers, warrant amounts, furlough information and date fields for proper input, edits, and compliance with date standards. We determined that the 39,261 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 deviation noted.

Department's Control: CPS provides various reports to assist in verifying and balancing transactions.

Tests Performed: Reviewed CPS Manual and interviewed staff.

Test Results: Each pay period, the following standard payroll reports were provided to agencies:

- Personal Services Expenditure,
- Personal Services Expenditure/With Insurance,
- Employer Retirement Pick-Up,
- University Retirement Report,
- Group Insurance Salary Refund Report,
- Payroll/Group Insurance Discrepancy Report, and
- Position Occupied Report.

No deviation noted.

OVERALL CONCLUSION

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

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 Insurance
13. Department of Juvenile Justice
14. Department of Labor
15. Department of Military Affairs
16. Department of Natural Resources
17. Department of Public Health
18. Department of Revenue
19. Department of Veterans' Affairs
20. Department on Aging
21. East St. Louis Financial Advisory Authority*
22. Emergency Management Agency
23. Environmental Protection Agency
24. Executive Ethics Commission
25. Guardianship and Advocacy Commission
26. House of Representatives
27. Human Rights Commission
28. Illinois Arts Council
29. Illinois Civil Service Commission
30. Illinois Commerce Commission
31. Illinois Community College Board
32. Illinois Council on Developmental Disabilities
33. Illinois Criminal Justice Information Authority
34. Illinois Deaf and Hard of Hearing Commission
35. Illinois Educational Labor Relations Board
36. Illinois Gaming Board
37. Illinois Labor Relations Board
38. Illinois Law Enforcement Training and Standards Board
39. Illinois Math and Science Academy
40. Illinois Office of the State's Attorneys Appellate Prosecutor
41. Illinois Power Agency
42. Illinois Prisoner Review Board
43. Illinois Procurement Policy Board
44. Illinois Racing Board
45. Illinois State Board of Investment *
46. Illinois State Police
47. Illinois Student Assistance Commission
48. Illinois Violence Prevention Authority
49. Illinois Workers' Compensation Commission
50. Joint Committee on Administrative Rules
51. Judges' Retirement System
52. Judicial Inquiry Board
53. Legislative Audit Commission
54. Legislative Ethics Commission
55. Legislative Information System
56. Legislative Printing Unit
57. Legislative Reference Bureau
58. Legislative Research Unit
59. Office of Management and Budget
60. Office of the Architect of the Capitol
61. Office of the Attorney General
62. Office of the Auditor General
63. Office of the Executive Inspector General
64. Office of the Governor
65. Office of the Lieutenant Governor
66. Office of the Secretary of State
67. Office of the State Appellate Defender
68. Office of the State Fire Marshal
69. Office of the Treasurer
70. Property Tax Appeal Board
71. State Board of Education
72. State Board of Elections
73. State Employees' Retirement System
74. State of Illinois Comprehensive Health Insurance Board
75. State Police Merit Board
76. State Universities Civil Service System
77. Teachers' Retirement System of the State of Illinois

* Agency payroll information was entered into the system by CPS staff.

CENTRAL INVENTORY SYSTEM (CIS)

EXISTING ENVIRONMENT

Objective: The structured software development methodology is utilized to manage any new developments, any enhancements and maintenance to existing code to ensure only authorized, tested and documented developments and changes are made to the application.

Department's Control: All application development changes are controlled in accordance with the Application Systems Development Methodology Manual.

Tests Performed: Reviewed the Application Systems Development (ASD) Methodology Manual (Methodology) and interviewed staff.

Test Results: The Methodology, revised August 2005, was "created to provide a structured process for the design, development and implementation of new systems, enhancements and maintenance to existing systems and for development of ad hoc requests."

No deviation noted.

Department's Control: New developments, enhancements, and changes are documented through the use of a Service Request Form (SR) and documented in the Service Request Registration System (SRRS).

Tests Performed: Reviewed Application System Development Methodology Manual and interviewed staff.

Test Results: The Department utilized the Service Request Registration System and Service Request Form to document new developments and enhancements.

According to management, there were no application developments, enhancements, or changes to CIS during the review period.

No deviation noted.

Department's Control: New developments, enhancements, and changes are approved and tested before implementation into the production environment.

Tests Performed: Reviewed Application Systems Development Methodology Manual, and interviewed staff.

Test Results: The Application Systems Development Methodology Manual required developments, enhancements, and changes to be approved and tested before implementation into the production environment.

According to management, there were no application developments, enhancements, or changes to CIS during the review period.

No deviation noted.

Department's Control: New developments, enhancements, and changes are moved into production by the Library Control Group.

Tests Performed: Reviewed Program Library Procedures and interviewed staff.

Test Results: The Program Library Procedures outlined the requirements utilized for new programs and modification to existing programs.

According to management, there were no application developments, enhancements, or changes to CIS during the review period.

No deviation noted.

Department's Control: Affected program documentation is updated as part of system developments or enhancements required to comply with the Information Technology Governance (ITG) process.

Tests Performed: Interviewed staff.

Test Results: As part of the process, system documentation was to be reviewed and updated as applicable.

During the review period, there were no system developments or enhancements that required updated to system documentation.

No deviation noted.

Department's Control: System Users are informed when an application development or enhancement will affect them.

Tests Performed: Interviewed staff.

Test Results: Communications regarding changes which affect users were sent via email.

The Department did not have a system development or enhancement which required communications to users during the review period.

No deviation noted.

Objective: Quality Assurance procedures monitor compliance with system development and change processes.

Department's Control: A technical verification is conducted to ensure the quality and completeness of each new application development or enhancement.

Tests Performed: Reviewed EBAS Quality Assurance procedures and interviewed staff.

Test Results: The Quality Assurance 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.

According to management, there were no application developments, enhancements, or changes to CIS during the review period.

No deviation noted.

Objective: Processes exist to restrict logical access to CIS.

Department's Control: A checklist with the necessary security tasks is completed when new user agencies are added.

Tests Performed: Reviewed CIS Security checklist and interviewed staff.

Test Results: When a new agency was added as a user to CIS, the CIS Security checklist is completed.

According to management, there were no new user agencies during the review period.

No deviation noted.

Department's Control: Each CIS user agency has a Security Administrator who is responsible for adding new users. That process is the responsibility of the user agency.

Tests Performed: Interviewed staff.

Test Results: Assignment and authorization of access rights were the responsibility of each agency's security administrator.

No deviation noted.

Department's Control: Security software is used to control access.

Tests Performed: Reviewed the Mainframe Security Procedures, appropriateness of individuals with access to CIS, CIS User Manual, sign-on process, and interviewed staff.

Test Results: Access to CIS was controlled through security software (Resource Access Control Facility (RACF)). Users must have a properly authorized security software user ID and password to gain access to the operating environment.

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 seven Department staff members to CIS, noting no exceptions.

No deviation noted.

Department's Control: CIS internal security is used to enable and limit user capabilities.

Tests Performed: Reviewed the CIS User Manual, sign-on process, and interviewed staff.

Test Results: Once access to the operating environment was obtained, users must use a separate application user ID and password to gain access to CIS.

No deviation noted.

Department's Control: Assignment and authorization of access rights are the responsibility of the user agency.

Tests Performed: Interviewed staff.

Test Results: Assignment and authorization of access rights were the responsibility of each agency's security administrator.

No deviation noted.

Objective: The CIS User Manual outlines the procedures related to completeness, accuracy, timeliness and authorization of transactions.

Department's Control: Data requirements exist to force correction of errors and completion of critical fields before a transaction is accepted.

Tests Performed: Reviewed CIS User Manual, system edits, agency data, and interviewed staff.

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 corrected data. Data was entered online by user agencies and errors must be corrected before the transaction was accepted.

We reviewed three specific edits, noting no exceptions.

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 119,188 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 deviation noted.

Department's Control: CIS provides various reports to assist the users in verifying and balancing transactions.

Tests Performed: Reviewed CIS User Manual, CIS reports, and interviewed staff.

Test Results: The CIS User Manual provided a listing of various online and batch reports.

We reviewed a sample of transaction and inventory reports, noting no exceptions.

No deviation noted.

Department's Control: Entry, authorization and integrity of data are the responsibility of the user agency.

Tests Performed: Interviewed staff.

Test Results: Entry, authorization, and integrity of data were the responsibility of the user agency.

No deviation noted.

OVERALL CONCLUSION

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

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 Finance and Professional Regulations
6. Department of Human Rights
7. Department of Military Affairs
8. Department of Natural Resources
9. Department of Public Health
10. Department of Transportation
11. Department of Veterans' Affairs
12. Department on Aging
13. Environmental Protection Agency
14. Illinois Arts Council
15. Illinois Deaf and Hard of Hearing Commission
16. Illinois Law Enforcement Training and Standards Board
17. Illinois Office of the State's Attorneys Appellate Prosecutor
18. Illinois Violence Prevention Authority
19. Office of Management and Budget
20. Office of the Attorney General
21. Office of the Governor
22. Office of the Lieutenant Governor

CENTRAL TIME AND ATTENDANCE SYSTEM (CTAS)

EXISTING ENVIRONMENT

Objective: A structured software development methodology is utilized to manage any new developments, any enhancements and maintenance to existing code to ensure only authorized, tested and documented developments and changes are made to the application.

Department's Control: Changes are logged, tracked, and approved through the EPM process.

Tests Performed: Reviewed EPM process and interviewed staff.

Test Results: The Department utilized the Enterprise Project Management (EPM) process for logging and tracking changes. In addition, since changes to EPM were restricted to managers, the information for a particular change was in effect approved by the functional manager updating the record.

The Department had a process to log and track changes at an overview level.

No deviation noted.

Department's Control: New developments, enhancements, and changes are approved and tested before implementation into the production environment.

Tests Performed: Reviewed changes and interviewed staff.

Test Results: According to management, there were no changes to CTAS during the review period.

No deviation noted.

Department's Control: New developments, enhancements, and changes are moved into production by the Library Control Group.

Tests Performed: Reviewed changes, Program Library Procedures, and interviewed staff.

Test Results: The Program Library Procedures outlined the requirements utilized for new programs, and modifications to existing programs.

According to the Department, there were no changes to CTAS during the review period.

No deviation noted.

Department's Control: Affected program documentation is updated as part of system developments or enhancements required to comply with the Information Technology Governance (ITG) process.

Tests Performed: Interviewed staff.

Test Results: As part of the process, system documentation was to be reviewed and updated as applicable.

During the review period, there were no system developments or enhancements that required updates to system documentation.

No deviation noted.

Department's Control: System Users are informed when an application development or enhancement will affect them.

Tests Performed: Interviewed staff.

Test Results: Communications regarding changes which affect users would be sent via email.

The Department did not have a system development or enhancement which required communications to users during the review period.

No deviation noted.

Objective: Processes exist to restrict logical access to CTAS.

Department's Control: A checklist with the necessary security tasks is completed when new user agencies are added.

Tests Performed: Reviewed CTAS New Agency Procedures and interviewed staff.

Test Results: When a new agency was added as a user of the CTAS, the CTAS New Agency Procedures was completed. The Procedures documented the information needed to establish the new agency on the system.

There were no agencies added during the review period.

No deviation noted.

Department's Control: Each CTAS user agency has a security administrator who is responsible for adding new users. That process is the responsibility of the user agency.

Tests Performed: Interviewed staff.

Test Results: Assignment and authorization of access rights were the responsibility of each agency's security administrator.

No deviation noted.

Department's Control: Security software is used to control access.

Tests Performed: Reviewed the Mainframe Security Procedures, appropriateness of individuals with access to CTAS, CTAS User Manual, sign-on process, and interviewed staff.

Test Results: Access to CTAS was controlled through security software (Resource Access Control Facility (RACF)). Users must have a properly authorized security software user ID and password to gain access to the operating environment.

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 Department staff members to CTAS. An access rights list of Department staff members contained the names of 12 staff members who did not require access.

The access rights list was not periodically reviewed and updated.

Department's Control: CTAS internal security is used to enable and limit user capabilities.

Tests Performed: Reviewed the CTAS User Manual, sign on process, and interviewed staff.

Test Results: Once access to the operating environment was obtained, users must use a separate application user ID and password to gain access to CTAS.

No deviation noted.

Department's Control: Assignment and authorization of access rights are the responsibility of the user agency.

Tests Performed: Interviewed staff.

Test Results: Assignment and authorization of access rights were the responsibility of each agency's security administrator.

No deviation noted.

Objective: The CTAS User Manual outlines the procedures related to completeness, accuracy, timeliness and authorization of transactions.

Department's Control: Data requirements exist to force correction of errors and completion of critical fields before a transaction is accepted.

Tests Performed: Reviewed CTAS Manual and agency data.

Test Results: Data entered into the system was the responsibility of the user agency. CTAS contained 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 employee identification numbers for proper input, edits, and compliance with date standards. We determined that the 4,171 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 deviation noted.

Department's Control: CTAS provides various reports to assist in verifying and balancing transactions.

Tests Performed: Reviewed CTAS User Manual, CTAS reports, and interviewed staff.

Test Results: During the "close" process, 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.

We reviewed a sample of closed and supplementary reports, noting no exceptions.

No deviation noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance the controls, the Department should periodically review access rights to CTAS, ensure access is appropriate, and update the access rights list.

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 Corrections
6. Department of Financial and Professional Regulation
7. Department of Human Rights
8. Department of Insurance
9. Department of Labor
10. Department of Natural Resources
11. Department of Public Health
12. Department of Revenue
13. Department of Veterans' Affairs
14. Department on Aging
15. Environmental Protection Agency
16. Guardianship and Advocacy Commission
17. Human Rights Commission
18. Illinois Civil Service Commission
19. Illinois Comprehensive Health Insurance Plans
20. Illinois Deaf and Hard of Hearing Commission
21. Illinois Educational Labor Relations Board
22. Illinois Gaming Board
23. Illinois Law Enforcement Training and Standards Board
24. Illinois Planning Council on Developmental Disabilities
25. Illinois Procurement Policy Board
26. Illinois Racing Board
27. Illinois State Police
28. Illinois Workers' Compensation Commission
29. Office of the Attorney General
30. Office of the Executive Inspector General
31. Office of the Governor
32. Office of the Lt. Governor
33. Office of the State Fire Marshal
34. Property Tax Appeal Board
35. State Board of Elections

This Page Intentionally Left Blank

OTHER INFORMATION PROVIDED BY THE DEPARTMENT OF CENTRAL MANAGEMENT SERVICES BUREAU OF COMMUNICATIONS AND COMPUTER SERVICES THAT IS NOT COVERED BY THE SERVICE AUDITOR'S REPORT (NOT EXAMINED)

The Department provided information in the following areas:

- Summary of Services
- User Organization Controls
- Action Plan to Address Security Deficiencies
- Staffing Trends

SUMMARY OF SERVICES

The Department of Central Management Services' Bureau of Communications 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 of Central Management Services operates the Central Computer Facility (CCF), the Communications Center, and branch facilities.

The Department of Central Management Services 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 Bureau of Communications and Computer Services' mission is to provide competitive statewide technology services to meet the needs of State agencies, boards and commissions and other constituents including local governments, public safety agencies, schools, libraries and hospitals.

The Bureau of Communications and Computer Services:

- Oversees the planning, procurement, managing, maintaining, and delivering of voice, data, wireless, video, Internet, and telecommunications services to all state government agencies, boards, and commissions, and state supported institutions of higher education in Illinois, as well as other governmental and some non-governmental entities. As part of the Information Technology and Telecommunications Rationalization, BCCS centralized infrastructure functions previously devolved in certain agencies.
- Operates the Central Computer Facility, which provides mainframe processing systems and support for most state agencies and midrange application hosting for many agencies.
- Manages the Illinois Century Network, a service that creates and maintains high speed telecommunications networks providing reliable communication links to and among Illinois schools, institutions of higher education, libraries, museums, research institutions, state agencies, units of local government, and other local entities providing services to Illinois citizens.

The Bureau of Communications and Computer Services provides voice, data, wireless, video, Internet, and telecommunications services to all state government agencies, boards, and commissions, as well as many schools and universities, libraries, hospitals and local governmental bodies across Illinois. The Bureau also manages high-speed radio and wireless computer networks for use by Illinois public safety agencies.

The Bureau of Communications and Computer Services has made significant progress in its multi-year effort to "rationalize" the State's Information Technology infrastructure - to coordinate and streamline the myriad of IT communications systems used by State agencies.

The Bureau of Communications and Computer Services functions as a service organization providing computing and telecommunication resources for State agencies' and other entities' use. The following is a summary of services:

Strategic Planning
Strategic planning is used to align IT and telecommunication resources and guide activities toward the support of the mission and objectives of the State, Department, and the entities it serves.

Continuous Service
The Department provides IT recovery services to user agencies in the form of coordination, rehearsal assistance, infrastructure support, and contract establishment.

Service Communications
The Department provides its User Agencies with the ability to access information regarding the services it provides. It monitors and reports on service delivery and performance. It communicates with User Agencies regarding incidents, changes, service requests, issues and new developments that may affect service. It also provides a means for User Agencies to discuss and resolve service related issues.

Billing
The Department is statutorily authorized to provide IT and telecommunication services to governmental and other entities, to bill for these services and to accept payments in the Statistical Services Revolving Fund (SSRF) and the Communications Revolving Fund (CRF).

Output Production
On November 15, 2010, the print shop utilized by State agencies was moved from the Harris facility to the Willard Ice Building. Additionally, controls over the operation were transferred from the Department to the Department of Revenue.

The process of scheduling jobs and picking up the print jobs remained the same.

Library Services
Library Services unit is comprised of the Library Support unit and the Tape administration unit. Library support in responsible for program migrations, responsible for ensuring all libraries, carts and datasets used by each of the following respective agencies is within the standards and guidelines:

DHS Standards & Policies
HFS Standards & Policies
CMS Standards & Policies
DOT Standards & Policies

The Library Support unit constantly monitors libraries checking on generations allowed and retentions used using the reports listed in Mobius and using commands on the mainframe through Bluezone to check on space available.

The Tape Administration unit ensures all carts to be used within a specific timeframe are ready for use according to security standards, or determines they need to be disposed of using the following methods:

RACF
TMS
TGS Systems for DHS & HFS
HFS and DHS Standards
CMS Tape Library procedures are followed to dispose of media

Library Support and the Tape Administration units work with each other to schedule jobs using CA-Scheduler to process on the A, D and H systems of the mainframe for DHS, HFS, CMS and IDOT. These jobs are set up to execute within their respective schedules for after-hours processing. The Production Control unit runs the TGS jobs for DHS and HFS which the Tape Administration unit uses the output and online entries to complete their duties the next day.

Help Desk

Customer Service Center (CSC)
The CSC provides Tier 1 support of the Telecommunications (excluding Illinois Century Network and Radio) and IT products and service offerings managed by the Department.

The CSC IT Service Desk provides Tier 1 IT technical and end user support to the consolidated agencies as well as multiple boards, commissions and Department managed agencies. 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 Department of Healthcare and Family Services and the Department of Human Services.

The CSC Telecom Service Desk provides maintenance and provisioning of voice, video, data and wireless systems and services for all State agencies, departments, constitutional officers, commissions, and boards, excluding ICN and Internet calls which are routed directly to the Customer Management Center (CMC). Universities may elect to procure Telecom services through the CSC. The Telecom service Desk is staffed during normal business hours Monday thru Friday 8 am to 5 pm. All telecommunications service calls outside regular business hours and on Holidays are handled by the CMC.

Customer Management Center (CMC)
The CMC provides 24/7 network support for the State of Illinois. Additionally, after 5 pm and during non-business hours, the CMC provides support for voice, wireless and data services.

Network Services

Network Services provide telecommunications/network services to a variety of agencies, boards and commissions, educational institutions, and other governmental and non-profit entities.

Change Management

Infrastructure changes

The Department's change management controls Department managed infrastructure, including hardware and software in the mainframe, and desktop environments, and the State of Illinois Network environment. The change management process does not apply to application changes.

Application changes

Agencies that manage and maintain their own applications and have the administrative rights to move their own agency application changes into production:

- Windows Environment: All agencies have administrative rights to their legacy environment and some agencies (REV, AGR, DOT, and FPR) have limited rights to Illinois.gov environment to move changes into production; therefore, follow the respective agencies change management process.
- Unix/Websphere: The following agencies (AGR and REV plus select applications at CMS, HFS, DHS, and DPH) have administrative rights to move changes into production; therefore, follow the respective agencies change management process.

The remaining environments and agencies may utilize the ESR/RFC process at their discretion.

Information Assurance

The Department provides information assurance services to user agencies that:

- Communicate security principles through issuance of policy and hosting education opportunities.
- Alert users to known occurrences or potential imminent threats that could cause risk to cyber resources.
- Notify appropriate parties of non-compliance instances of system security software.
- Develop enterprise strategies and policy statements to assist the Department with compliance to applicable rules and regulations.

LAN Services

LAN Services installs, configures, and supports the Department's LAN networking infrastructure, including: switches, routers, hubs, firewalls, wireless switches and inside cabling. LAN Services also provides internet filtering services for specific agencies.

System Security Software

Security software is utilized to protect resources and data found on the Department's systems, including all subsystems that incorporate interfaces to the security software.

Storage and Backup

Enterprise Storage and Backup (ESB) provide the allocation, backup and removal of storage for the Department's mainframe systems. ESB manages both SMS Pools and Private Pools.

System Software
The Department provides mainframe hosting environments for agencies and other entities. System software includes:

- z/OS (Zero Downtime Operating System)
- z/VM (Zero Downtime Virtual Machine)
- CICS (Customer Information Control System)
- DB2 (Database 2)
- IMS (Information Management System)
- IDMS/R – Integrated Database Management System/Relational

Physical Security
The Department's Bureau of Property Management (BoPM) implements and maintains all physical security systems and services at facilities which house the Department's Bureau employees and equipment.

LAN Application
The LAN Application Development develops and maintains LAN based applications which agencies utilize.

Internet-Enabled Web Applications
The Department provides a variety of internal and external web-enabled Applications that agencies use to communicate and share information with both public and private sectors. These Web applications, in contrast to Web Content Management (WCM) sites, typically contain custom business logic and databases.

Accounting Information System
AIS is an automated expenditure control and invoice voucher processing system utilized by State agencies. Appropriation, obligation, cash and vendor processing functions support the invoice processing. AIS allocates invoice amounts into sub accounts and allows users to track cost centers. Vouchers are created in AIS according to the Comptroller's Statewide Accounting Management System (SAMS) procedures.

Central Inventory System
CIS is an automated asset inventory control system, which also allows the user agency to track depreciation. 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.

Central Time and Attendance System
The CTAS is an online system used to maintain "available benefit time". CTAS provides for attendance information to be recorded using either the positive or exception method.

Central Payroll System
CPS was designed to provide assistance in preparing payrolls for state agencies. 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.

USER ORGANIZATION CONTROLS

Users of the State of Illinois Information Technology Environment are responsible for complying with prescribed requirements and for using available security mechanisms to protect the security and integrity of their data. The Department has identified several areas of user agency responsibility that should be reviewed by user agencies.

Bills for computer services
User agencies should monitor the monthly billing to ensure charges are correct. Additionally, all user agencies should submit payment in a timely manner.

Continuous Service
- User agencies should develop and maintain appropriate and viable business continuity plans, application recovery scripts, designated application information updates to the BRM, recovery exercise procedures and schedules, and ongoing communications with CMS/BCCS.
- User agencies should establish procedures and assign responsibility to specific agency personnel, such as an IT Recovery Coordinator to achieve policy compliance.
- User agencies should understanding the IT Recovery Policy and the CMS/BCCS IT Recovery Methodology, determine the appropriate criticality and RTO classification of their applications, communicate the criticality and RTO classification to CMS/BCCS, and actively participate in local and regional exercises as business needs dictate.

Help Desk
To ensure that controls are functional at the agency level:
- User agencies should review and monitor their monthly billings to ensure Telecom provisioning and repair charges are accurate.
- User agencies should review EMS and monthly billings to monitor usage and submit change requests based on evaluation and eliminate paid services with non-usage.
- User agencies should engage CSC Projects Unit to assist in the evaluation of telecommunications options to reduce costs and/or improve efficiencies as needed.

Information Assurance
To ensure that controls are functional at the agency level:
- User agencies should ensure they have reviewed the security polices located on the Department's website.
- User agencies should communicate to the Department their specific security requirements.

Internet-Enabled Web Applications
To ensure that controls are functional at the agency level, user agencies should:
- Verify only accurate and authorized data are entered into the web applications. 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 web applications to ensure access authorized is appropriate.

LAN Applications

To ensure that controls are functional at the agency level, user agencies should:

- Verify only accurate and authorized data are entered into LAN applications. 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 LAN Applications to ensure access authorized is appropriate.

LAN Services

To ensure that controls are functional at the agency level:

- Users should ensure the Department is aware of their specific security requirements.
- Users should ensure the Department has implemented the appropriate internet filtering controls. Additionally, the Department should monitor the internet filtering logs.

Library Services

To ensure that controls are functional at the agency level, user agencies should ensure security lists are reviewed, updated, approved, and returned to the Department on a bi-annual basis to ensure the most up-to-date lists are in place which minimizes any security breach.

Network Services

To ensure controls are fully implemented and functional at the agency level, user agencies should:

- Ensure the Department is aware of their specific security requirements.
- Ensure the Department is aware of their specific Wide Area Network requirements.

Output Production

To ensure controls are implemented, user agencies should ensure the security authorization listing is updated to reflect authorized individuals.

Production Control and Input Units

To ensure that controls are functional at the agency level, user agencies should ensure:

- Daily schedules are supplied to the after-hours Input unit for CMS, DHS, HFS and DOT by the Production Control unit with access through a EPOS (Enterprise Production Operation Services) SharePoint site. IDOR sends a schedule copy to the Input unit shared email site.
- For problem resolution, HFS (except the Medical unit) allows access to database TSO.Info.Clist listing primary, secondary and supervisor contacts.
- The HFS Medical unit supplies resolution information.
- DHS provides a Microsoft Access database for problem contacts.

- DOT has an in-house SharePoint site for problem resolution to maintain and grant access to Input personnel.
- EPA uses a mainframe – accessible file.
- IDOR provides emails and call-lists for resolution.

Physical Security
To ensure that controls are functional at the agency level, user agencies should ensure security authorization lists are reviewed, updated, approved, and returned to the Department on a bi-annual basis.

Security Software
To ensure that controls are functional at the agency level, user 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 ID's and delete ID's 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.

Service Communications
To ensure that controls are functional at the agency level, agencies should:
- Review service delivery and performance information made available by the Department.
- Notify the Department of any service issues they have.

Strategic Planning
User agencies should ensure their priorities related to Department services are effectively communicated to Department management by participating in the group meetings, requesting individual meetings and contacting the Bureau and Department management regarding issues important to their agency.

Storage and Backup
To ensure that controls are functional at the agency level, agencies should ensure:
- Users utilize an Enterprise Service Request through the Help Desk to request additional storage.
- Users open an ESR through the Help Desk to request the deletion of storage.
- Users open a Help Desk Ticket through the Help Desk for the restoration of data.

System Software
To ensure that controls are functional at the agency level, agencies should ensure appropriate protection over their defined resources.

Accounting Information Systems (AIS) use should be reviewed.
To ensure 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.

Central Payroll System (CPS) use should be reviewed.
To ensure 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.
- 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.
To ensure 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.

Central Time and Attendance System (CTAS) use should be reviewed.
To ensure 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.
- Regularly review those authorized to pick up timekeeping reports, and inform appropriate CTAS personnel of changes timely.

ACTION PLAN TO ADDRESS SECURITY DEFICIENCIES

Department of Central Management Services
Bureau of Communications and Computer Services

The following are action items the Department has undertaken to address control deficiencies that were detailed in the Office of the Auditor General's FY11 Service Organization Report. These deficiencies were deemed to be significant both to the Auditors and to Department Management. Therefore, the Department took immediate action to compensate for the one deficiency. Following are the details:

Control Area: Mainframe password resets
Deficiency: According to the Procedures, a control existed to confirm the identity of an individual requesting their password be reset. Based on their testing, the OAG found that Department staff was not routinely following the procedures and thus not confirming the identity of the users.

Resolution: A control was implemented on June 16, 2011 that required all users to e-mail certain information to the Department's Service Desk in order to request the password reset. Once received and verified, the Service Desk would call the individual at the phone number provided via e-mail and supply a temporary password. We have also developed a prototype of a new automated password reset tool and are currently testing it within the Bureau.

Control Area: Granting, modifying and revoking physical access badges
Deficiency: The Statewide CMS/BCCS Facility Access Policy outlined procedures governing the handling of physical access badges. The OAG found that these procedures were not always being followed.

Resolution: Prior to the audit period, the controls over the physical access process had been assigned to a separate bureau within the Department. As a result, the procedures outlined in the Policy were not followed. However, the Department has the following compensating controls in place:

- All access cards have a 35 day absentee limit.
- All Department facilities are staffed with security guards.
- Sensitive areas are monitored by security cameras.

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
BUREAU OF COMMUNICATIONS AND COMPUTER SERVICES
STAFFING TRENDS
(NOT EXAMINED)

The following tables reflect staff separations and staff hires, and the associated experience gained or lost during the last 5 fiscal years. As outlined in the 3rd table, the Bureau has experienced a significant loss in both the number of staff and experience. The Net loss of staff from FY 2007 through FY 2011* has been 142, with an associated net loss of 3,697 years of experience.

Staff Separations and Total Years of Experience Lost by Fiscal Year.

Fiscal year	Number of Separations	Years of Experience Lost
FY 07	57	759
FY 08	49	744
FY 09	38	755
FY 10	47	997
FY 11*	36	853
Totals	227	4,108

Staff Hires and Total Years of Experience Gained by Fiscal Year.

Fiscal year	Number of Hires	Years of Experience Gained
FY 07	39	254
FY 08	12	89
FY 09	23	68
FY 10	9	0
FY 11*	2	0
Totals	89	428

Net Loss of Staff and Experience by Fiscal Year.

Fiscal year	Net Staff Loss	Net Years of Experience Lost
FY 07	18	505
FY 08	37	655
FY 09	15	687
FY 10	38	997
FY 11*	34	853
Totals	142	3,697

* FY 11 data is through April, 2011

Additionally, the Bureau provided copies of documents that contained statements regarding necessary staffing levels and technical expertise and the risks of not receiving these resources. These documents show a diligent effort by the Bureau to notify relevant parties of the importance of proper staffing and the risks of not providing such. Below are some excerpts from statements made by the Department/Bureau to the Governor's Office Management and Budget on May 2, 2011 related to staffing requests.

> *Security vulnerability remediation personnel are needed to fix critical security flaws in numerous critical computer systems. They provide specific expertise and knowledge related to identifying and correcting vulnerabilities such as weak system settings, newly identified vulnerabilities in systems and software products, virus activities, and correcting issues related to Payment Card Industry (PC) compliance. Not filling these positions could result in an increase in the number of successful intrusions into State computer systems, and could cost the State millions of dollars in costs related to required notification to affected parties, system downtime, increased overtime, and reduced systems availability statewide.*
>
> *The CMS/BCCS mainframes run numerous critical agency business systems including, Medicaid, TANF, Unemployment Benefits just to name a few. As a result of recent retirements, the staffing is down by over 30%+. Another 15% are expected to retire this year. If the positions are not filled in a timely manner, adequate support and knowledge of the environment is at risk.*
>
> *Manager of Mainframe position is responsible for managing the State's mainframe computer system which runs numerous critical agency systems including; Medicaid, TANF, Unemployment Benefits, etc. If this position is not filled planning for necessary upgrades of hardware and software will be impacted as well as day to day operations and management of staff. If necessary software upgrades are not performed, security of the systems could be impacted as well as support of the software products by the vendors due to not maintaining current levels of software. The resulting computer systems outage would have a major impact to the State of Illinois.*

The Executive Dashboard, a document that is generated by the Bureau EPMO staff, reviewed by the Deputy Director and submitted to the Agency Director's Office frequently had statements regarding staffing. Examples are listed below:

> *The inability to fill several key positions in BCCS has put us at risk of being unable to address our resource deficiencies and operational needs.*
>
> *Without specialized technical services that contractual resources can provide, BCCS will not be able to complete the requisite projects by their mandated due dates, thus putting the State in a position of non-compliance with State and Federal law.*
>
> *The inability to fill several key positions in BCCS has put us at risk of being unable to address our resource deficiencies and operational needs.*

This Page Intentionally Left Blank

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 Insurance
17. Department of Juvenile Justice
18. Department of Labor
19. Department of Military Affairs
20. Department of Natural Resources
21. Department of Public Health
22. Department of Revenue
23. Department of Transportation
24. Department of Veterans' Affairs
25. Department on Aging
26. East St. Louis Financial Advisory Authority
27. Eastern Illinois University
28. Emergency Management Agency
29. Environmental Protection Agency
30. Executive Ethics Commission
31. General Assembly Retirement System
32. Governors State University
33. Guardianship and Advocacy Commission
34. Historic Preservation Agency
35. House of Representatives
36. Human Rights Commission
37. Illinois Arts Council
38. Illinois Civil Service Commission
39. Illinois Commerce Commission
40. Illinois Community College Board
41. Illinois Council on Developmental Disabilities
42. Illinois Criminal Justice Information Authority
43. Illinois Deaf and Hard of Hearing Commission
44. Illinois Educational Labor Relations Board
45. Illinois Finance Authority
46. Illinois Gaming Board
47. Illinois Housing Development Authority
48. Illinois Labor Relations Board
49. Illinois Law Enforcement Training and Standards Board
50. Illinois Math and Science Academy
51. Illinois Medical District Commission

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

ACRONYM GLOSSARY

ACL – Access Control List

ACS – Automated Cartridge System

AGR – Department of Agriculture

AIM – Acquisition and Inventory Management

AIS – Accounting Information System

AOC – Automated Operations Control

AR – Agency Relations

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

BOSSAP – Bureau of Strategic Sourcing and Procurement

BRM – Business Reference Model

Bureau – Bureau of Communication and Computer Services

CA – Computer Associates

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 – Communications 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

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

HIPAA – Health Insurance Portability and Accountability Act

HMC – Hardware Management Console

HSM – Hierarchical Storage Management

H/V – Hirsch Velocity

IBM – International Business Machines

ICN – Illinois Century Network

ID – Identification

IDOT – Illinois Department of Transportation

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

LSM – Library Storage Manager

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

PC – Personal Computer

PCF – Property Control Form

PIM – Program Information Management or Personal Information Management

PIR – Post-Implementation review

PKI – Public Key Infrastructure

POP – Point Of Presence

PROC – Procedures

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

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