

THIRD PARTY REVIEW

**Department of Central Management Services
Bureau of Communication and
Computer Services**

July 2007

TABLE OF CONTENTS

Report Digest	i
Auditor's Report	1
Report Summary	5
Service Organization - Description of Controls	11
Service Auditor Description of Tests and Operating Effectiveness	63
General Controls	
Chief of Staff	65
Workforce and Development and Logistics	68
Executive Program Management Office.....	71
Agency Relations.....	76
Business Services	79
Technical Strategy.....	82
Network Services.....	84
Business Enterprise Applications – Personal Information Management	91
Enterprise Applications – Quality Assurance.....	93
Workflow.....	99
Service Management	101
Web Services and LAN Application Development	102
End User Computing	107
Vendor Management	109
Enterprise Production Operations Services	112
Enterprise Capacity Performance and Storage - Mainframe.....	116
Systems Programming - Mainframe	118
Database Management - Mainframe.....	124
Infrastructure Services - CCF Tape Library	131
Infrastructure Quality Assurance and Methods.....	134
Infrastructure Services – Data Center Operations	136
Risk Management – Recovery Services	140
Physical Security - BCCS	144
Risk Management – Technical Safeguards	149
Change Management - Mainframe	151
Administrative Safeguards	152
Customer and Account Management.....	155
Service Engineering	162
Illinois Office of Internal Audit	169
Internet Billing System.....	171
Physical Security – Bureau of Property Management.....	179
Application Controls.....	183
Accounting Information System	185
Central Payroll System.....	191
Central Inventory System.....	197
Central Time and Attendance System	203
Appendix A - Complementary User Organization Controls.....	209
Appendix B - List of User Agencies	213
Appendix C – Identified Description of Control Deficiencies	215
Appendix D – Acronym Glossary	217

REPORT DIGEST

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

THIRD PARTY REVIEW

For the Year Ended:
June 30, 2007

Release Date:
July 11, 2007



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

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

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

INTRODUCTION

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

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

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

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

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

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

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

Information provided by the Department - Unaudited

DEPARTMENT DIRECTOR AND DEPUTY DIRECTOR/BUREAU MANAGER

During Audit Period: Director: Paul Campbell (7/1/2006 to 3/9/2007)
Deputy Director/Bureau Manager: Tony Daniels (7/1/2006 to 2/22/2007)

Currently: Acting Director: Maureen O'Donnell (3/10/2007 to present)
Acting Deputy Director/Bureau Manager: Doug Kasamis (2/23/2007 to present)

REPORT SUMMARY

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

Midrange Environment

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

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

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

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

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

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

Security Policies

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

Security policies had not been updated to reflect current environment

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

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

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

Information Technology Billings

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

Billing methodology weaknesses were identified

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

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

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

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

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

Disaster Contingency Planning

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

State lacks preparedness

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

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

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

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

AUDITORS' OPINION

With the exception of the three significant deficiencies described above, procedures were generally sufficient to provide reasonable, but not absolute, assurance that relevant general and application control objectives were achieved.



WILLIAM G. HOLLAND, Auditor General

WGH:WJS

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



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

OFFICE OF THE AUDITOR GENERAL
WILLIAM G. HOLLAND

AUDITOR'S REPORT

The Honorable William G. Holland
Auditor General
State of Illinois

We have examined the accompanying description of controls related to the systems and procedures used to control data processing operations at the Bureau of Communication and Computer Services of the Department of Central Management Services (Department). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the Department's controls that may be relevant to a user agency's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user agencies applied the controls contemplated in the design of the Department's controls; and (3) such controls had been placed in operation as of May 31, 2007. Our review, started in July 2006 and primarily performed between January 2, 2007 through May 31, 2007, was limited to controls at the Department. The control objectives were specified by management of the Department. Our examination was performed in accordance with the Illinois State Auditing Act, applicable generally accepted auditing standards, and "Government Auditing Standards" issued by the Comptroller General of the United States. We included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

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

In our opinion, except for the matters referred to in the preceding paragraph, the accompanying description of the aforementioned systems and procedures presents fairly, in all material respects, the relevant aspects of the Department's controls that had been placed in operation as of May 31, 2007.

The Department was in the process of consolidating Information Technology (IT) functions of State government. From May 2006 to April 2007 over 775 servers were transferred to the Department from agencies participating in the consolidation project. During our analysis, it became apparent a standardized process to administer, secure, and monitor the midrange environment had not been implemented. Since a standardized process had not been implemented to manage the midrange environment, we were not able to develop a method to effectively test midrange installation, maintenance, operations, and security controls. Due to the lack of a

standardized process, we were unable to perform tests to provide positive assurance that administration, security, and monitoring controls in the midrange environment were consistently applied to all systems.

Additionally, the description stated the Department developed new security policies relating to the IT environment. Based on inquiries of staff and inspection of activities, we determined those policies had not been implemented and the policies that were in effect did not address the current IT environment.

The description also stated salary and fringe benefits costs for consolidated agency personnel were charged back to the legacy agency through a billing system. The Internet Billing System (IBiS) was developed to provide a mechanism to bill agencies for consolidated services. The billing invoices were the foundation for agencies to make payments to the Department. Additionally, the invoices were to provide documentation for agencies to use for Federal Fund participation purposes. Based on inquiries and review of billing data, we determined a formal methodology clearly documenting the allocation of charges to consolidated agencies did not exist. In addition, the current process and associated documentation did not provide the necessary support to verify the appropriateness of charges to consolidated agencies.

In addition, we do not express an opinion on control objectives not listed in the description of tests and operating effectiveness section (pages 63 to 207). Specifically, we do not express an opinion on:

- Infrastructure Services - Midrange Services - WinTel,
- Infrastructure Services - Midrange Services - Unix,
- Enterprise Capacity Performance and Storage (midrange environment), and
- Change Management (midrange environment).

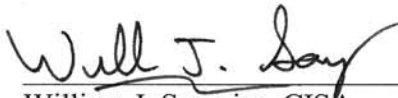
Also, in our opinion, except for the matters referred to in the preceding paragraphs, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user agencies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

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in the body of the report, to obtain evidence about their effectiveness in meeting the control objectives, during the period from January 2, 2007 through May 31, 2007. The specific controls and the nature, timing, extent, and results of the tests are listed in the body of the report. This information has been provided to the Department's user agencies and to their auditors to be taken into consideration, along with information about the internal control at user agencies, when making an assessment of control risk for user agencies. In our opinion, except for the matters referred to in the preceding paragraphs, the controls that were tested, as described in the body of the report, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in the body of the report were achieved during the period from January 2, 2007 through May 31, 2007. However, the scope of our engagement did not include tests to determine whether control objectives at the user agencies were achieved.

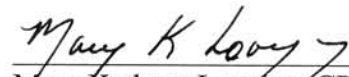
The relative effectiveness and significance of specific controls at the Department, and their effect on assessments of control risk at user agencies, are dependent on their interaction with the controls and other factors present at individual user agencies. We have performed no procedures to evaluate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

The description of controls at the Department is as of May 31, 2007, and information about tests of the operating effectiveness of specified controls covers the period from January 2, 2007 through May 31, 2007. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specified controls at the Department is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

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



William J. Sampias, CISA
Director, Information Systems Audits



Mary Kathryn Loyejoy, CPA, CISA
Information Systems Audit Manager

May 31, 2007

REPORT SUMMARY

INTRODUCTION

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

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

The Department functions as a service organization providing computing and telecommunication resources for State agencies' use. The Department and the agencies that use the Department's computer resources share the responsibility for maintaining the integrity and security of computerized data and functions. Although the Third Party Review addressed controls for which the Department is responsible, we did not review the controls over the 11 consolidated agencies' environments or other user agencies. As a result of our review, we identified numerous control areas that should be reviewed and addressed by user agencies and their internal and external auditors (see Appendix A).

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

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

Accounting Information System;

Central Payroll System;

Central Inventory System; and

Central Time and Attendance System.

We identified several control deficiencies that appear in pages 63 through 207; in addition, we noted three significant deficiencies for which we could not obtain reasonable assurance over the controls.

Midrange Environment

Public Act 93-25 authorized the Department of Central Management Services to consolidate Information Technology (IT) functions of State government. The following agencies were participating in the consolidation project:

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

Per the Department, the physical server consolidation and relocation of equipment began after necessary network infrastructure upgrades were completed in 2006. From May 2006 to April 2007 over 775 servers were transferred to the Department from agencies participating in the consolidation project. Planning for the transfer of approximately 370 additional servers was underway with relocation starting in May 2007.

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

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

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

Department Response

Change Management-Midrange

The Department concurs with the recommendation and will move forward to more effectively standardize our change management environment. We acknowledge that the policy is in need of revision to more accurately reflect our current change management process. The interim change management system is an effective compensating control in meeting the objective of ensuring changes to system software and/or application software are sufficiently controlled. This is demonstrated by the department's successful implementation of over 1,200 change requests during this period with no major outage, data loss, security breach or data corruption resultant from the execution of the interim process.

Midrange-Wintel

We concur with the conclusion/control recommendation. CMS agrees that standardized processes needs to be developed and more effective controls for access rights need to be implemented. CMS has developed and is continuing to develop and implement procedures that will provide consistent methods for managing these various environments. These procedures address such things as inventory, administration, security, and monitoring the servers in the midrange environment. Additionally, work is currently underway to update the Business Reference Model (BRM) which contains a complete listing of agency applications and to identify all critical agency applications that are housed on these systems. This information had never been collected prior to these consolidations.

Many of the issues described are related to legacy environments, and these environments did not have adequate controls in place prior to moving the servers to the CCF. Based on reviews of legacy agency's prior audit reports, it is evident that these systems were not being effectively managed prior to their move and were at serious risk from an environmental and security perspective. In addition, the audit procedures conducted in the SAS 70 review are more comprehensive than the IT reviews previously conducted at the legacy agencies resulting in the discovery of additional issues that need to be corrected. The relocation of these servers enables us to effectively mitigate these risks and address the issues outlined in this recommendation in a more methodical and consistent manner.

The stated control objective is to: *".... ensure an appropriate security structure is established to ensure information assets are adequately protected from unauthorized or accidental disclosure, modification, or destruction."* CMS contends that the physical relocations have helped us in our attempt to reach the control objective. This has been proven over the last year by several incidents that involved systems that had not been physically relocated. Some of these incidents involved the disruption of service after weather related events, which resulted in unplanned downtime for numerous systems in those facilities. These incidents could have been avoided had the servers been relocated to the consolidated site, which was designed specifically to incorporate backup systems, supplemental power, robust security, and more weather-resistant construction.. No such major prolonged outages based on facility failures or major security systems breaches have occurred to servers that were relocated. While we concur that much more can and should be done to improve the security structure, the server relocations/moves as part of IT consolidations have improved our ability to meet this control objective, not hinder them.

Midrange-UNIX

We concur with the conclusion/control recommendation. CMS agrees that standardized processes needs to be developed and additional controls for access rights need to be implemented. CMS has developed and is continuing to develop and implement procedures that will provide consistent methods for managing these various environments. These procedures address such things as inventory, administration, security, and monitoring the servers in the midrange environment.

Many of the issues described are related to the wide variety of legacy environments, some of which did not have adequate controls in place prior to moving the servers to the CCF. By creating a consolidated and consistent environment, the new location of these servers enables us to mitigate risk and address the issues outlined in this recommendation. While we concur that much more can and should be done to improve the security structure, the server relocations/moves as

part of IT consolidations have improved our ability to meet this control objective, not hinder them.

Midrange ECPS (Backup and recovery)

We concur with the conclusion/control recommendation. CMS agrees that standardized processes need to be developed and more effective controls for server backup need to be implemented. CMS has developed and is continuing to develop and implement procedures that will provide consistent methods for managing these various environments.

While we concur that improvements to standardize the backup system need to occur, we do believe that the current systems in place are meeting the control objective as stated. A recent example of this backup recovery capability was demonstrated after a fire at a remote DHS office. Although the building that housed this local office was destroyed by fire, CMS was able to recover all IT services and data in approximately 24 hours. This is just one of many examples that clearly demonstrate our ability to effectively manage these backup systems and meet our control objective in real world recovery situations.

Security Policies

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

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

The Department should thoroughly review and update security policies to address the current technological environment, consolidation issues, and present-day risks. If the IT security policies/procedures approved in December 2006 are suitable, then the policies/procedures should be implemented, formally communicated, and disseminated to all appropriate parties. (See pages 152-154 for additional information)

Department Response

The Department concurs and has reviewed and updated security policies as demonstrated by the new set of policies and procedures published on the BCCS web portal. The Department notified CMS and consolidated Agency staff of the security policies via memos dated May 16th; BCCS will work with CMS Personnel on publications requiring further scrutiny for inclusion in the CMS Employee Handbook. BCCS will then issue a global communication announcing the replacement of policies. The Department has developed an Access database to accommodate policy issuance tracking.

Information Technology Billings

Due to the consolidation of various functions of State government into the Department, the Internet Billing System (IBiS) was developed to provide a mechanism to bill agencies for

consolidated services. The billing invoices were the foundation for agencies to make payments to the Department. Additionally, the invoices were to provide documentation for agencies to use for Federal Fund participation purposes. The Department billed for Information Technology services to consolidated agencies through IBiS. We reviewed the Information Technology portion of IBiS.

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

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

- Develop and implement a formal methodology to clearly document the billing rate structure and allocation of charges.
- Develop a process to review and verify the accuracy of billing statements.
- Provide adequate documentation to agencies to support billing statements and comply with federal fund reimbursement guidelines established by the Office of Management and Budget (OMB) circular A-87.

(See pages 171-178 for additional information)

Department Response

The Department concurs with the finding. Although documentation for the IBiS charging methodology does exist and training was provided to staff, the process was not fully optimized during the period under review. Also, while documentation supporting the charges is provided to each agency based on the agency's own defined parameters, the Department recognizes that in some cases further documentation may be required. The Department provides further detail as requested, and works closely with agencies to provide billing credits where warranted.

The Department notes that it is replacing the majority of IBiS billings in FY08 with more traditional usage-based rates structures. IBiS was a temporary billing system implemented to support the interim consolidated environment.

Other Control Deficiencies

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

Disaster Contingency Planning

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

The Department had not implemented and tested procedures to protect critical information resources, minimize the risk of unplanned interruptions, and ensure the availability of critical information resources within acceptable timeframes. In particular, plans and procedures to recover the midrange environment had not been adequately addressed.

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

The Department should ensure the necessary components (plans, equipment, and facilities) are available to provide for continuation of critical computer operations in the event of a disaster. In addition, the Department should obtain a suitable regional alternate location for recovery services, and conduct comprehensive tests of the plans on an annual basis. (See pages 140-143 for additional information)

Department Response

The Department partially concurs. We agree that we do not have a comprehensive midrange disaster recovery plan as a result of the current state of the consolidation effort. Prior to the consolidation, the degree in which an agency had a midrange disaster recovery plan varied significantly.

BCCS recognizes that this is a significant issue and is in the process of formalizing its Business Reference Model (BRM) to identify and warehouse information concerning Agency business functions relative to their associated computerized applications.

The BRM is being populated with CAT1 information, thereby allowing BCCS to obtain, for the first time, a dashboard view of all critical infrastructure components, enabling us to provide recovery services as defined by Agency business requirements (with an emphasis on distributed recovery capabilities). Agencies have been formally notified that BRM app details must be provided to BCCS in order to receive recovery services.

Lastly, BCCS is upgrading the Harris facility to enhance local outage recovery services, and has recently conducted several mainframe recovery tests at that site.

The Department responses were provided on June 21, 2007, by Doug Kasamis, Acting Deputy Director/Bureau Manager, Bureau of Communication and Computer Services of the Department of Central Management Services.

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

SERVICE ORGANIZATION - DESCRIPTION OF CONTROLS

The following Description of Controls section (pages 11 through 62) consists of text provided by the Department of Central Management Services.

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

Chief of Staff

Procurement

The Procurement Unit coordinates all Bureau purchase requests and contract renewals including Request for Purchase (RFP), Invitation for Bid (IFB), and Request for Information (RFI) for IT/Telecom items regardless of size or method of procurement that have been approved by management.

Tools:

- **Provisioning System:** Residing on the Remedy platform, this system provides an automated process for Bureau procurement approvals by following defined workflow paths. This system routes the electronic procurement form to each designated bureau approver for their review and approval; when the electronic procurement document receives all the required approvals, Bureau Procurement is notified via email. If the procurement request is rejected by any of the required approvers (i.e. more documentation or justification is required), the approval starts over from the beginning. The specific approval groups are managed by the Bureau Procurement Officer and maintained by the system administration staff. All workflow activity is logged in the record's journal. This system was designed to follow and enforce the procurement rules.
- **Procurement Business Case:** Residing on the Remedy platform, this system routes procurement information to each approver depending on the type of procurement. It also serves as a tracking system for procurements.
- **Illinois Procurement Bulletin:** Residing on the NOTES platform, this system allows the State to meet the public posting requirements of the Illinois Procurement Code. The bulletin alerts the Procurement Policy Board of a procurement and allows them the opportunity to review. Questions or concerns are responded to by the Procurement Unit. This system is designed around the regulations regarding the public display of state government procurements.

The Bureau Procurement Unit adheres to the following adopted procedures, polices and laws:

- Contract Administration Procedures
- (Bureau vs. BOSSAP) Roles and Responsibilities - Bureau IT/Telecom Procurements
- Procedures for creating a Procurement Business Case (PBC)
- Procedure for creating a provisioning request (PRV)
- Illinois Procurement Code/Rules
- CPO Notices/Bulletins
- Bureau Procurement Procedures

Environment:

- The structure of both the automated workflow using the tools in place and the accompanying progressively approval documents, procurements adhere to the rules and regulations required by the law. With the exception of emergency purchases, all procurements follow the rules in place. Emergency requests can only be approved by the State Procurement Officer (SPO) of the requesting agency.
- The Bureau Procurement Officer conducts:
 - Bi-weekly conference calls with BOSSAP to discuss the status of procurements and to address any issues that have arisen.
 - bi-weekly conference calls with their customers to discuss the status of their procurements.
 - weekly meetings with the Bureau Procurement staff meeting to discuss the status of procurements, upcoming heavy workloads, and changes to the policies and procedures.
 - bi-weekly meeting with the Chief-of-Staff to discuss unit issues.
- Bureau of Strategic Sourcing and Procurement: acts as a control for the procurement process by reviewing procurement documentation, awarding contracts, and finalizing all contracts except orders against a master contract that are under \$250,000; procurements less than \$250,000 are finalized by Bureau Procurement.

The BCCS Procurement Unit supports the following persons/divisions:

The Division Procurement Liaison, contract owner/end-user, Bureau Procurement Staff, vendor(s), approvers in the provisioning system, Bureau Legal, Bureau of Strategic Sourcing and Procurement, receiving, Business services/fiscal, Comptrollers office, Department State Purchasing Officer, Director of the Department and the Procurement Policy Board.

Workforce and Development and Logistics

The Workforce and Development and Logistics unit coordinates and facilitates internal personnel paperwork, workforce training development and implementation, and workforce logistics for Central Management Services - Bureau of Communication & Computer Services (CMS – BCCS)

Internal Personnel Paperwork:

This unit has many policies/procedures that allow for proper processing of transactions.

Specifically for HR related transactions we follow and refer to the Personnel Rules, the Personnel Code, the CMS Policy Manual, the AFSCME contract, the pay plan, the personnel transactions manual and the alphabetic index.

Workforce training development and implementation:

This area is now being formalized since we have hired a training manager. Initially we are using a new paper training request form and procedure. We work with the BCCS fiscal office for approval on these training requests. Another piece of training involves travel. Travel rules and regulations are followed for approval and reimbursement of travel incurred while training.

Workforce logistics:

This involves the physical location of employees. In order to physically move a union employee we follow past practice of notifying the union 30 days in advance of the move. Moving employees also involves moving of telephones, telephone lines, computers and office equipment which are all coordinated through the specific team (i.e. telephone line move is coordinated through the telecom coordinator).

Since this is a relatively new section, no formal controls are in place.

Executive Program Management Office

The overall mission of the Enterprise Program Management Office (EPMO) is to promote and enable the successful attainment of State of Illinois business and technology objectives through approved initiatives, programs, and projects. The EPMO, and its attendant processes also assist in optimizing the allocation and utilization of the State's limited resources (time, money, and people) to accomplish the State's business and technology objectives. The scope of the EPMO's current responsibility varies by process and is expected to grow over time as the State's consolidation efforts continue. With the exception of IT Governance, the EPMO started with an initial focus on the Department of Central Management Services (DCMS) and is gradually encompassing the Consolidated Agencies and other governmental entities under the Executive Branch of the State of Illinois.

The EPMO works with various DCMS units and processes, as well as various Agencies, Boards and Commissions under the Executive Branch of the State of Illinois. Current collaborative efforts include working with the Illinois Technology Board of Advisors (ITBA) which provides a forum for the State's Information Technology community; the Architecture Rationalization Board (ARB), which serve as gatekeepers for the State's IT Standards; the Resource Allocation Prioritization (RAP) process, currently being piloted within the DCMS Director's Office; the Enterprise Architecture and Strategy (EA&S) group, which assists in implementing the IT Governance process; the Management Review Board (MRB), which reviews and approves proposed projects; the Investment Review Board (IRB), which reviews and approves financial expenditures; and the Chief Information Officer (CIO) and Chief Technology Officer (CTO) who set overall technology strategy and direction.

The methodology utilized by the EPMO includes selective application of best practices embodied within our processes, standardized tools and techniques embodied within our templates; and structured processes including Strategic Portfolio Management (SPM), Information Technology Governance (ITG), and Enterprise Project Management (EPM).

These three processes are further described below:

Strategic Portfolio Management (SPM)

The Strategic Portfolio Management process is responsible for capturing and managing project-related information related to Consolidated Agency business needs and IT strategic plans. This information is organized within an enterprise repository referred to as the Project Portfolio. The scope of this process is currently limited to Consolidated Agencies with a primary focus on DCMS. The information gathered facilitates advance resource and budgetary planning; assists the Department and Bureau in identifying potential Shared Services; and provides input to the enterprise technology strategy.

Controls:

1. Formal notification from the Deputy Director and EPMO Executive to Consolidated Agency Executive Directors, CFOs, and CIOs to provide their IT Strategic Plan; to identify proposed projects (via the EPMO's Project Portfolio); and to respond with a memorandum from the Executive Director confirming that the Agency's IT Strategic Plan and proposed project information has been submitted, and is complete and accurate.
2. Agency IT Strategic Plans and proposed projects are then reviewed by the EPMO to confirm whether submitted information appears to be accurate, complete and sufficiently clear enough to permit evaluation, classification, analysis, and decision-making. Follow-up workshops with Consolidated Agencies are conducted (as needed) to improve the quality of the information provided.
3. Any proposed project that the EPMO determines to be Tier 2 (subject to IT Governance) or Tier 3 (IT Governance and direct EPMO oversight) is referred to the IT Governance process to determine whether a Project Charter has been submitted. Once a charter number has been assigned, it is entered into the Project Portfolio. Project Charters are required for Tier 2 and Tier 3 projects.
4. The EPMO utilizes the information provided for proposed Tier 2 and Tier 3 projects as input for potential Enterprise Shared Services (determined by the CIO) and as input for the Enterprise Technology Strategy (determined by the CTO). The EPMO also assesses proposed projects to ensure adequate sponsorship, and availability of adequate time, resources and funding (aka qualification).
5. The EPMO also produces various reports from the Project Portfolio to support ongoing governance, budgeting, project status, and management reporting.

Information Technology Governance (ITG)

The Information Technology Governance process is responsible for evaluating proposed projects,

initiated via Project Charters, to ensure business and technology alignment and to determine solutions that are consistent with the State's technology standards. This process is designed to optimize technology reuse and to promote enterprise shared services that have the capability to support multiple business applications. The scope of this process includes agencies, boards, and commissions under the Executive Branch of the State of Illinois.

Controls:

1. The IT Governance process provides templates and guidelines for Project Charters, Functional Requirements, Non-Functional Requirements, and Project Financials. Submitters have the option to use substitutes for these templates as long as these documents provide the minimum information necessary for assessment and evaluation under the IT Governance process.
2. IT Governance, in conjunction with Enterprise Architecture & Strategy (EA&S), evaluates proposed projects for business and technology alignment, possible technology re-use, and potential shared service opportunities. This evaluation includes review of new Project Charters as well as specific deliverables required at each of the governance gates to ensure accurate and complete information is provided.
3. IT Governance reviews occur at each of the governance gates to confirm the necessary information has been provided and governance requirements have been satisfied. Missing, inaccurate, or incomplete information is resolved prior to granting approval to proceed to the next gate.

Proposed projects are presented to the Management Review Board (MRB) and Investment Review Board (IRB) to obtain the necessary management and fiscal approvals. The EPMO provides an agenda that identifies the projects to be considered at each MRB/IRB meeting and documents any actions taken and/or decisions made. The state and status of these projects are then tracked in the Project Portfolio.

Enterprise Project Management (EPM)

The Enterprise Project Management process is responsible for increasing the overall project success rate (projects that meet their stated business objectives and are completed on-time, within budget, and within resource allocations). To accomplish this goal, the EPMO has adopted and tailored selected best practices to establish a consistent project management discipline and community of practice within the Department and Bureau. The EPMO also sponsors and facilitates indoctrination, training and mentoring opportunities designed to increase the knowledge and expertise of project management practitioners. The scope of this process includes the Consolidated Agencies, but the initial implementation is limited to projects that require both Governance and EPMO Oversight (Tier 3 Projects) within the Department and Bureau.

Controls:

1. The EPMO qualifies (ensures adequate sponsorship and requisite resources) and activates (mobilizes resources to initiate) projects that have been approved by the MRB & IRB, by

assigning a qualified Program Manager (for Tier 3) and/or Project Manager (for Tier 2) and mobilizing Project Teams.

2. The EP MO publishes selected Project Management (PM) tools and provides mentoring on selected PM practices (typically derived from best practices and existing State of Illinois PM practitioners)
3. Weekly Status Meetings are conducted with the Bureau's Leadership to provide updates on current projects. These meetings are utilized to discuss strategy as well as to identify and resolve issues and other project constraints.
4. Project Status Reports are provided on a weekly basis and include overall status (Red-Yellow-Green); activities planned for the period; activities accomplished during the period; activities planned for next period; as well as identification of significant issues; risks; and requested management actions.
5. Project Team Sites (SharePoint) and Standardized Directory Structure/Project Folders are established for each project team to serve as a repository for project artifacts and other pertinent project documents.

Agency Relations

Liaisons within Agency Relations (AR) establish and maintain productive and efficient customer relationships, and serve as proactive advocates and facilitators focused on anticipating and achieving each customer's legitimate business needs. AR serves as the primary contact and provides guidance to customers in successfully navigating and complying with the Governance process. AR maintains communication with customers to apprise them of their IT and Telecom requests status, and inform them of issues and potential Bureau solutions that may satisfy their business needs. Liaisons are responsible for:

- Assisting customers to help them identify their business needs;
- Communicating with customers and Bureau personnel regarding issues, risks, status, etc.;
- Investigating procurement and project status for customers;
- Providing information regarding ongoing Bureau projects and initiatives that effect or may effect customers, such as planned maintenance activities, enterprise solutions, etc.;
- Coordinating access to other Governance-related groups within Bureau; and
- Providing correct customer contact information with regard to Change Management and other Bureau communications.

Currently, AR has no formal policies. Staff are provided processes and guidelines through verbal instruction, understanding and training.

AR sends out Bureau Deputy Director communications regarding Bureau services via email to all customers, upon approval and signature from the Deputy Director. AR conducts weekly, bi-weekly, monthly or as needed meetings with Consolidated CIOs, Non-Consolidated CIOs and Department LAN and Legacy Customers IT representatives. Meeting intervals are based on agency CIO/IT Manager decision. AR records action items during these meetings, works within

the Bureau and with agency on action items and follows up with CIO verbally or via email on outcome. Each AR Liaison uses an agenda to conduct these meetings. The AR Liaison may bring another Bureau staff person from one of the Shared Services Teams, in order for her/him to have the opportunity to share communication from their control area. Follow up is conducted via email or verbally with CIO/IT manager.

AR executive management and all Liaisons (when available) attend Consolidated Agency CIO, Illinois Technology Board of Advisors meetings and any other event that is pertinent to establishing and maintaining effective customer relationships.

In addition, monthly meetings are held with the Consolidated CIO, Bureau Deputy Director and Executive Agency Relations Manager via bridge conference calls. The CIO has the opportunity to share his/her feedback with overall Bureau services, including, but exclusive to Agency Relations. There are written minutes (issues log) for each of these meetings.

Quarterly the AR Unit is rated via the Bureau's Overall Satisfaction Survey, sent out by the Service Level Management Team.

Agencies that are not included in the aforementioned types of customer service feedback, have been made aware in written or verbal communication that they may contact either the Agency Relations Executive Manager, Customer & Account Management Executive, Bureau Deputy Director, Bureau Leadership or any Bureau Senior Management staff with concerns, issues and/or if they are not satisfied with the representation they are receiving at their agency/board/commission.

Business Services

Business Services

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

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

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

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

Each month the Department receives billing information for communication services from various vendors. Upon receipt of the paper bill from the vendor, the summary page is provided to CRF billing staff who reconcile against the electronic media received from said vendor. Any discrepancies are reconciled and then the billing can proceed with the appropriate changes. The information is compiled to produce the CRF billing for users. Users are charged for usage of voice and data service, cell phones, pagers and communication equipment.

The Bureau also compiles billing information related to Network bandwidth usage and bills appropriately through MAS 90. Regional Technology Centers (RTC's) monitor usage and connectivity in their areas. This usage is reported monthly to Business Services. Once all monthly reports are received a reconciliation takes place for discrepancies, a download from Remedy into MAS 90 takes place. Billings are generated from MAS 90 and sent to the Network customers.

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

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

TECHNICAL STRATEGY

The Technical Strategy unit provides support to the Department's leadership team and serves as liaison for IT strategy to the agencies, boards, and commissions reporting to the governor. The head of this unit is the Chief Technology Officer, and the unit supports two functions. The first is Enterprise Architecture and Strategy. The second is Strategic Planning.

Enterprise Architecture And Strategy

The Enterprise Architecture and Strategy (EA& S) group was developed to ensure that IT investment decisions are aligned with EA&S vision and goals and deliver outcomes that keep in step with the accelerating pace of business changes. Working with the Bureau Leadership team, Enterprise Program Management Office (EPMO) and the Architecture Review Board (ARB), EA&S helps create the IT Strategic Plan, develop standards and reference architectures, create IT transition plans, and provide assistance to all Agencies.

The Architecture Review Board is a cross-Agency authority established to facilitate the IT and Telecom Governance of the State of Illinois. The intent of the ARB is to enable alignment of the IT portfolio and adherence to standards concerning the deployment of IT and Telecom business solutions. It is not intended as a review process to challenge or critique Agency direction. The goal is to align Agency initiatives with the BCCS Unified Plan and that the resultant products conform to established IT standards and architecture defined in approved business models and the Enterprise Architecture and Taxonomy Database. The ARB approves or designates approval authority the EA&S group on all IT Standard products.

The Enterprise Architecture and Taxonomy database contains a list of business applications and products (software) used at a statewide, or enterprise, level. This list was compiled from two data collection efforts, conducted by Bearing Point, reviewed by domain owners and subject matter experts, and approved by the Architecture Rationalization Board. The list of products considered to be a state standard can be identified by accessing the Enterprise Architecture and Taxonomy Database web site, selecting products, then life cycle, then standard, and conducting a search on the database.

EA&S works with various operational units to accomplish the Architectural goals. Those units include: The EPMO, the ARB, Management Review Board (MRB), the Bureau's Policy Review Board (PRB), the State's CIO, and the various customer organizations.

EA& S works with the EPMO through processes embodied by the "Governance" gates 1 through 3 to guide business and technical alignment within enterprise projects. EPMO maintains the gate 1-3 documents of the Governance process as "Charters" and shares responsibility for maintaining the Business Reference Model with EA&S and the Consolidated Agencies.

EA&S utilizes the "Governance" gates 6 and 7 with the approval of the Architecture Review Board to manage the Architectural standards. The major artifacts documenting gates 6 and 7 are: the Technical Reference Model, the Product Standardization Requests and the minutes from the ARB sessions.

EA& S consults with various Boards, Agencies, and Commissions through various sessions for analyzing business needs, determining solutions sets, and assisting with competitive acquisitions (like RFPs and RFIs).

Strategic Planning

The purpose of this Strategic Plan is to identify reprioritized initiatives under a comprehensive framework which integrates with the larger Strategic Plan being developed by CMS. The leadership for the Strategic Plan has joined the State of Il on October 16, 2007. Under the new leadership, the process for the development of the Strategic Plan has been created. The Plan itself is currently under development for a July 1, 2007 issuance.

Infrastructure and Applications

Network Services

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

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

Network Services - Design and Security

The Design & Security team is responsible for establishing architectural standards and methodologies for implementing and supporting wide-area and local-area enterprise systems and services. Established standards currently include: POP Site Power Strategy, Basic MPLS Connectivity Model, Common Connection Methodology for LAN, and Quality of Service. Design and Security staff designs complex network and network service configurations. In addition to this work, staff performs project management and participates in network, network service, and telecommunications related projects.

Design and Security staff conducts, coordinates, and serves as lead(s) on feasibility studies and projects involving wide-area network systems. They have developed test procedures for hardware and software and make recommendations based upon test results. Design and Security staff perform analysis to determine future bandwidth and capacity needs. They also provide network and services related support to other teams with the Department's Network Services such as CMC, Field Operations, Network Operations, and LAN Services.

Network Services - Network Operations

Network Operations is responsible for installing, maintaining and managing the ICN Backbone including backbone circuits, egress circuits, routers, firewalls, switches, fifteen Point of Presence (POP) sites, WAN monitoring tools and WAN services. Additionally, Network Operations provides tier 3 Network Support to other staff within the bureau.

Network Operations staff are responsible for the backbone and POP site management and support. Support includes: delivery, removal and inventory of equipment; installation, maintenance and documentation of all POP site equipment; test and turn-up of all backbone and egress circuits; installation and management of POP sites. Network Operations staff are responsible for installing, customizing, maintaining and supporting WAN management and monitoring. Additionally, Network Operations is responsible for WAN Services including DNS, registrar for

the il.us domain and filtering. WAN services support includes installation, configuration, maintenance and support.

Network Services - LAN Services

LAN Services is responsible for entering rules into the firewalls and monitoring security violations. Additionally, this group is responsible for the consolidated agencies (AGR-Agriculture, CEO-Commerce & Economic Opportunity, DNR-Natural Resources, DHS-Human Services, HFS-Healthcare & Family Services, DOT-Transportation, REV-Revenue, CMS-Central Management Services, DES-Employment Security, DPH-Public Health, FPR-Financial & Professional Regulation, EPA-Environmental Protection) LAN networks, which includes: firewalls, routers, switches, hubs and wireless switches.

Additionally, the LAN Networking Services group is responsible for installation, configuration and support of the Department's LAN networking infrastructure including: switches, routers, hubs, firewalls, IDS, wireless switches and inside cabling.

Network Services – Enterprise Network Support

Enterprise Network Support is responsible for design and support of State Agency network access. Responsibilities include installation and support of access routers, WAN switches, VOIP, video conferencing, fiber, DNS, and Internet. Network Integration also performs tier 3 technical support for the CMC and directly to state agencies.

Enterprise Network Support is responsible for providing a variety of services to state agencies. Functions include customer consultation, access and distribution router configuration, ongoing maintenance, head-end router installations/troubleshooting, making equipment and connectivity recommendations, performing equipment installation/recovery at state agency sites in Springfield and surrounding area, and the provisioning for new circuits, moves and changes.

Enterprise Network Support works closely with LAN Services in support of the Shared Services infrastructure and the consolidated agency server farm.

Enterprise Network Support is responsible for the installation, maintenance, and protection of the CMS MAN fiber Network. Responsibilities include overseeing installation of fiber facilities and outside plant construction projects, fiber plant locating services, and maintenance of accurate fiber records.

***** The following is information concerning the change control, problem tracking, backup and recovery, and configuration standards that are followed by all of the above listed, Network Services teams.**

Change Management

Network Operations, LAN Services, Enterprise Network Support, and Design & Security all utilize the CMS Lotus Notes, Change Management system. In doing so, a Request for Change (RFC) is created within Lotus Notes. RFCs are reviewed at the weekly Change Advisory Council

(CAC) meeting. In parallel to this process, Network Operations and Enterprise Network Support also utilize ICN Remedy to track changes.

Problem Tracking

Network Operations utilizes ICN Remedy for problem tracking. Enterprise Network Support utilizes both ICN Remedy and CMS Remedy for problem tracking. LAN Services utilizes CMS Remedy for problem tracking.

Backup and Recovery

Network Operations and Enterprise Network Support backup firewall, router, and switch configurations via two servers. The servers are backed up to tape weekly and when a major change occurs. Tapes are then rotated off-site. LAN Services backups at consolidated agencies consists of the following for routers, firewalls, switches: AGR – does not backup configurations; CEO – does not backup configurations; DNR – does not backup configurations; EPA – does backup configurations, does not rotate tapes off site; FPR – does not backup configurations; CMS – does backup configurations and does rotate backups off site; DOT – does backup configurations, does not routinely rotate tapes off site; REV – does not backup configurations; DHS – only backs up configurations for devices they consider “critical”, does not rotate tapes off site; DPH – does backup configurations and does rotate tapes off site; HFS – does backup configurations and does rotate tapes off site; DES – does backup configurations and does rotate tapes off site.

Configuration Standards

Design & Security has established standard configuration templates for core, distribution, and WAN access equipment. LAN Services does not currently have a documented standard configuration.

Illinois Wireless Information Network (IWIN)

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

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

Transmissions are sent from the users’ Mobile Data Computer (MDC), equipped with the client software Premier MDC, to the nearest cellular tower equipped with CDMA equipment. CMS has a contract with Verizon Wireless (Verizon) to provide data connectivity throughout the State, as well as with Motorola to provide the software utilized by the IWIN network. Once the cellular

tower has received the transmission from the user's MDC, the transmission is then forwarded to a Verizon -owned and -operated messaging switch. From the messaging switch, the transmission is forwarded to one of the DCMS redundant Premier MDC Servers and then to the CMS's network for access to the appropriate data. Redundant routers, maintained by CMS, connect the CMS's Premier MDC Servers to the Verizon Network.

Business Enterprise Applications

Personal Information Management (PIM)

Establishment of the PIM group within the Bureau meets one component of the legislative mandate to standardize and consolidate IT services for departments, agencies boards and commissions under the jurisdiction of the Governor. PIM provides a centralized and consolidated platform that facilitates a statewide common architecture.

PIM currently manages email in a native format (Mailbox residing on Exchange servers at the CCF for the following agencies: CMS, AGR, CDB, CSC, ICJA, DHHC, CDD, ELRB, OEIG, GOV, HPA, HRC, HRD, JIB, DOL, LRB, LCC, LTGOV, OMB, PRB, PTA, RB, Race Tracks, WCC, ICN, IAHSE, IAMG, PTB, SFM.

The Department currently manages email in an alias format (Mailbox resides on legacy Exchange or Groupwise server. Uses the Department's perimeter solution): All agencies listed above, and the following: DES, EPA, Aging, DNR, HFS, DHS, REV, IGB, DPH, VPA, DNR, DCEO, FPR, DOT, GAC, CCB, IAC, IEMA, DCFS.

These services include: provisioning and email account, supporting user interaction with messaging application, monitoring/reporting service levels, performance tuning, technical support and problem resolution. PIM applications include FAX service, Mobile Messaging, Anti-Virus, Anti-Spam and Content Filtering, and directory support for State of Illinois email. Security is addressed at the perimeter, network and user levels.

Software

The software is a combination of vendor provided solutions to establish a cohesive standardized operating environment:

- Exchange 2003 – Back End environment; used to support standard user logins and email.
- Exchange 2003 – Front End environment; used to support Outlook Web Access (OWA)
- MS ISA – Internet Security & Acceleration; used to support (OWA) interaction with Front End environment
- Public Folders – Used to support documentation sharing and group file interaction
- SMTP Gateway – Used to support Anti Spam, Anti Virus and Content Filtering for email(see PIM Associated Applications below)

PIM Associated Applications

- RightFax connector software has been installed to provide FAX services as a requested adjunct service if a user has that requirement
- Mobile Messaging is supported through Blackberry service and supported devices.
- Anti-Virus, Anti-Spam and Content Filtering software is made up of integrated hardware/software products. This is managed through the Standard Email Gateway (illinois.gov)
- A Unified Directory is provided with directory support for State of Illinois address book/contacts for use within a user's email client

Security Management

The security in the PIM environment is overall one of the most important disciplines in the PIM environment. Security has been addressed at many levels with the following:

- Perimeter Security
 - The perimeter is protected with an Anti Spam, Anti Virus and Content Filtering solutions that detect unsolicited email senders, blocks suspect attachments and scans email for inappropriate content and attachments (*Perimeter security is managed by PIM*)
 - This area is also protected by a multi-layer Firewall architecture that is managed by Network Services
- Network Security
 - Email Security
 - The email servers are protected by an Anti Virus solution which scans all incoming email for potential viruses
 - The server is password protected and administration rights are restricted to the PIM and Midrange support personnel (*Antivirus is managed by Midrange team*)
 - Operating System security
 - The O/S is protected from viruses in the event that security from other 3 levels is compromised. (*Antivirus is managed by Midrange team*)
- User Security
 - The end user email account is secured using an aggressive password scheme. The password policy can be found in the PIM Policies document. (*Managed by Illinois.gov domain owner*)

Mobile Messaging Access

The PIM environment supports Mobile Messaging through wireless handheld units. Currently this service is supported using RIM's Blackberry Enterprise Server for messaging relay and synchronization. The mobile messaging service is available through Microsoft-Exchange and Novell-GroupWise email platforms. All platforms are supported by the PIM team with problem escalation and support through other infrastructure groups and vendors.

PIM Support and Escalations

There are 24/7 support procedures in place.

Major changes or additions are controlled by the Enterprise Change Management unit. (Lotus Notes)

Common Applications – Enterprise Applications

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

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

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

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

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

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

Accounting Information System (AIS)

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

The Department has developed a user manual, the AIS User Manual, which is located on the State's Enterprise Web Server (Intranet). The manual provides guidance to the user when utilizing the various functions.

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

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

Central Inventory System (CIS)

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

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

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

Central Payroll System

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

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

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

Central Time and Attendance System

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

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

Billing Allocation System / Internet Billing System– Department of Central Management Services Accounting

The Department of Central Management Services, Bureau of Computer and Communications Services (Bureau) has developed a web-based application that is used by Accounting to provide billing for various Department service funds such as the facilities Management Revolving Fund.

The Application, known as the "Billing Allocation System/Internet Billing System, " runs on the State's midrange AIX environment and posts thousands of invoices for State agencies per year. The system is generally available 24 hours a day, seven days a week except for downtime scheduled for production moves, which are handled through the Department's Change Management process (Lotus Notes), and during regularly scheduled backup jobs. The system uses databases hosted on the Department's mainframe at the Central Computer facility. In addition, we are responsible for the billing system for the consolidated services.

The Billing Allocation System / Internet Billing System (BAS/IBiS) is a web-based system the Department utilizes to bill agencies for consolidated services: Facilities Management, Internal Audit (IOIA), communication managers (PIO), Legal, and Information Technology. BAS is a paperless system that uses web technology to both present billing to agencies, and to capture allocation of the billing by the agencies for submission to the Department.

BAS/IBiS access is secured with security software and internal system role-based security. Access to the home page of the system is controlled via security software. Once authorized to the system, the user is authenticated for each page or function based on roles assigned by the Department's Accounting division through the system's internal security functions.

BAS was developed to act as a multi-purpose tool to support various aspects of the consolidation process. While various funds and amounts have been identified by agency and consolidation efforts in advance, there remains a need to track the actual funds that benefit from the services provided by the Department each month. BAS fills that need by capturing billing detail from the various service areas and summarizing that detail into allocation billing statements. The billing statements supported by the detail records provide a foundation for agencies to indicate to the Department which funds benefited from the services provided.

Additionally, the statements along with detail records provide documentation for agencies to use for Federal Fund Participation purposes.

To facilitate billing for the various entities whose funding mechanism was changed to a more traditional internal service fund for FY06, an enhancement was made to BAS that created the Internet Billing System (IBiS) path within the system. IBiS billing file inputs follow the same processes as used for BAS. Billing data is compiled by the various entities and provided in a structured layout form to the Bureau. Files loaded to IBiS must successfully pass the load program edits that ensure the file is balanced. Accounting is provided load reports, and Accounting is responsible for the release of the billing to the user agency community along with notification of the release of the billing. Accounting is also responsible for notifying the Bureau that the receivable records associated with billing file are to be loaded to the Accounts Receivable Posting System (ARPS). The ARPS load program ensures the load file passes all pre-edits prior to the load of the receivables.

IBiS has no update capability for the users who are recipients of the billings – only inquiry. There is no allocation function within the IBiS path. The system allows the user to select the type of billing he/she wants to view, and – based on internal system security – is presented with billings associated only with that path in the system (BAS or IBiS). IBiS billing contains no allocation functionality because the agency is responsible for processing an invoice to remit payment to the Department rather than the BAS model of cash transfer via a C-55 Funds Transfer Form.

BAS /IBiS has an on-line user manual available for the Bureau's Financial home page. Instructions on how to use the IBiS functionality were distributed by Accounting. Changes to the

manual are the responsibility of CMS Accounting and must be forwarded to the Bureau for inclusion in the manual.

BAS / IBiS is backed daily, weekly, and monthly. The backups are on disk and maintained at the Department's Central Computer Facility.

Quality Assurance

The EBAS Quality Assurance Section has developed the Application System Development Methodology (Methodology), and the Standards and Documentation Requirements guide for new system development projects and modifications to existing systems. The Methodology provides a structured process for the analysis and design, development, implementation and post implementation review of new system projects, enhancement projects, maintenance and ad hoc requests. The Standards and Documentation Requirements provide standards for consistent terminology, available programming tools, security, and storage.

For standard development, the Methodology requires the above-mentioned four phases to be completed in sequence; however, there are exceptions for Emergency Work Requests and Rapid Application Development (RAD).

Emergency Work Requests are to provide a way to deliver applications to the user as soon as possible. RAD projects utilize iterative and prototyping development technologies that can expeditiously provide completed systems to the user. The criteria for using RAD are: the development platform supports the iterative process or supports prototyping; the scope is limited, such as, but not limited to implementing reports or converting ad hoc reports to production; or the estimated hours for the project are under 200.

The EBAS Quality Assurance established a Standards Committee to review and approve changes to the Methodology and the Standards and Documentation Requirements.

An email or Service Request document is used to initiate a request for systems development projects. The Service Request Registration System registers projects, assigns a unique number to the Service Request (SR) and records the status of the project. In addition to the Service Request Registration System, EBAS utilizes the following tools to assist in tracking projects, assigning resources, and scheduling project time:

- Microsoft Project, and
- Quality Assurance (QA) Project Tracking System.

The EBAS's Methodology documents user involvement in all four project phases. Users of the new development/modification are interviewed and requirements outlined in phases one and two. The user tests and validates the new development/modification in the third phase and a user post implementation questionnaire may be used in the fourth phase.

The Quality Assurance Unit monitors and verifies that projects adhere to the Methodology. The QA Review Procedural Manual (Manual) provides guidance to Quality Assurance staff for each phase of a project. In addition to the Manual, Quality Assurance utilizes a checklist system to identify required tasks for each project.

In addition, the responsibilities of the former Tech Services unit has been transferred to the Quality Assurance Unit. These responsibilities include, security software management, DB2 administration, IMS transaction requests and library control support for EBAS.

The security software management is done through the use of the security software support application. This support is provided for the Department and numerous other agencies, boards and commissions. The Mainframe Security Procedures Technical Manual is the technical reference guide used for this activity. Current personnel act as the administrative coordinator for DB2 security access. This function is done through the use of a "DB2 Coordinator ID".

The submission of all system gen forms for IMS databases to the Data Center is part of the responsibility that has been passed to Quality Assurance Unit. The Unit is also responsible for IMS system backups. These backups are done daily, weekly and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.

Part of the Quality Assurance Unit is a Library Control Unit which is responsible for all mainframe movement of programs into production libraries. The Program Library Procedures provide guidance for ensuring new programs or modified programs are documented and approved before production moves are performed. A Library Control Form must be completed and approved before any move is made.

Workflow

BCCS/EBAS/Workflow Section:

The responsibilities of this section include the development and support of ITSM (Information Technology Service Management) and customized workflow-based applications. These applications are LAN, client server and web-based. The two major application development tool sets used and supported by EBAS/Workflow staff are Lotus Notes and Remedy software products.

The section follows the EBAS standards and methodology maintained by the EBAS Quality Control unit. Requests for new development, enhancements, maintenance, and ad hoc reports are tracked on the Service Request Registration System (SRRS).

Application Security: The access method to the supported systems is inherent to the platform and is controlled by either assigned liaisons or support management. NOTES has its internal security and REMEDY uses both its internal security and a Secure Socket Level (SSL) control that is managed by the server when required.

Task tracking: The Workflow unit uses a system called Production Authorization Release System (PARS) to review and release work completed on a system. The developer opens a PARS ticket for every release. Each ticket contains a *developer's checklist* for task completed listing the Changes/enhancements and the Tested changes/enhancements. When the developer is ready, a section is provided for *Peer Review*. The last section for release is the *move to production* section that provides both the BUM and Section Manager approval for the *Proposed Move Date/Time*.

A *Review History* contains all activity of the PARS activity for each release.

Data backup is performed daily by a common utility maintained by the Infrastructure Storage and Backup unit.

Service Management

Service Description

The Service Management unit conducts project administration for EBAS processes as directed by the EBAS Executive. This unit also acts as the EPMO's liaison for EBAS related projects.

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

Depending on the objective or subject matter, the audience may include state agency senior executives, public and elected officials, and internal Department staff.

The software utilities used in this unit to produce and handle the reports and documents include SharePoint, Microsoft Project, Excel, Word, and Visio.

Other than the normal user security, no additional control is required for the documents and data generated by this unit.

This is a newly formed unit with detailed operational procedures not yet fully documented.

Web Services / LAN Application Development

The Web Services / LAN Application Development Section provides four different types of services: LAN Application Development, Web Services, Enterprise Content Management and Collaboration with SharePoint. A detail description of each is listed below.

LAN Application Development Section

The responsibilities of this section include the development of custom application software on microcomputers, local area networks (LANs), Internet, Intranet and mainframe client server environments. In addition to standard executable application development, many of the projects

are designed and implemented using, but not limited to, Access, Access/SQL, Oracle, SQL, Visual Studio technologies and Fleet Anywhere (a third party application). Additionally, the LAN Application Development Section provides ongoing support to end-users of microcomputer workstations in the utilization of packaged and custom developed software. Clients of the LAN Application Development Section are personnel from the Department, the Governor's Office, and more than twenty other state agencies.

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

Prior to being placed into production, all updates and modifications are reviewed and approved by the owner. Once approval is obtained, the developer requests to their supervisor to move the changes into production.

Web Services Section

The Web Services section supports static and dynamic web sites and the domain name server. The Bureau provides web services that enable more than thirty state agencies to communicate their specific and broadly related information to both public and private sectors. This is accomplished through development and continued support of a variety of internal and external web applications and high profile web sites as well as enterprise-wide standardization and guidance to the agencies.

- The Web Services Section supports (which includes creation, implementation, and on-going update and maintenance) both static and dynamic web sites.
 - Static web sites consist of agency specific documentation, offerings, programs, etc., and applicable linking to other supporting information (including internal, external, and other public arenas).
 - Dynamic web sites consist of interactive, data-driven web-based applications, which allow staff members from state agencies to perform various functions and reporting efficiently and securely (i.e. using public key infrastructure, PKI) via the Internet.
 - Websites and web applications provide anywhere, anytime access. Web Services also takes direct responsibility for website maintenance if an agency requests. Both existing and leading edge development tools are used for web development. Websites maintained by Web Services all utilize the Official State Web Templates developed and administered by Web Services, and comply with the Illinois Web Accessibility Standards IWAS, which are based on the Federal "Section 508" and World Wide Web Consortium accessibility guidelines. Additionally, in an effort to address the needs of all users, prior to

implementation, web applications are thoroughly reviewed for IWAS compliance. Prior to being placed into production, all updates and modifications are reviewed and approved by the owner. Once approval is obtained, the developer requests to their supervisor to move the changes into production.

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

Enterprise Content Management Section

Still in development, the full functionality of Content Management is not in place; the initial controls that are in place are identified later in this description.

Enterprise Content Management provides the capabilities to scan, import, store, secure, index, retrieve and route document-based information. It includes an "out of the box" application for quickly implementing a system with no programming required. It also has a powerful set of Application Programming Interfaces (APIs) to enable custom integration into business applications for exceptional productivity and ease of use. The imaging services also provide an object management system. These business objects are cataloged in the library server, providing a common repository of indexes for easy search and retrieval. The business objects themselves may be located centrally or may be decentralized and close to the users. In all cases, with appropriate user security, any object located anywhere on the network can be retrieved and presented to the user.

Security is managed by the Content Management administrator. The customer's business requirements identify the level and type of security assigned.

The Content Management section is responsible for setting up and maintaining the content management tool and creating an environment for each user as per their needs.

With indepth analysis and prior to being placed into production, all updates and modifications are reviewed and approved by the owner. Once approval is obtained, the developer requests to their supervisor to move the changes into production.

Web Collaboration using SharePoint Section

Microsoft Windows SharePoint Services is a versatile technology that organizations and business units of all sizes can use to increase the efficiency of business processes and improve team productivity. With tools for collaboration that help people stay connected across organizational and geographic boundaries, Windows SharePoint Services gives users access to information they need. SharePoint Services also provides a foundation platform for building Web-based business applications that can flex and scale easily to meet the changing and growing needs of your business. Robust administrative controls for managing storage and Web infrastructure give IT

departments a cost-effective way to implement and manage a high-performance collaboration environment. With a familiar, Web-based interface and close integration with everyday tools including the Microsoft Office system, SharePoint Services is easy to use and maintain. This unit does not currently provide Sharepoint support or maintenance.

Infrastructure Services

End User Computing (EUC)

The EUC division of the Bureau provides personal computer and printer support to all state employees and contractors associated with the agencies consolidated under the Governor, and Legacy Central Management Supported Non-Consolidated Agencies. Responsibilities of EUC include Break/Fix Support, the Enterprise Service Request Process and major IT Rationalization projects. These responsibilities support major projects within the State of Illinois IT Rationalization initiative and daily technical support of the State's daily business.

- **Break/Fix Support:**

This is a daily EUC technical activity that provides Personal Computer (PC) and printer technical support to the above mentioned end users, and is directed primarily through the Bureau's service desk via the Enterprise Remedy helpdesk function. The service desk receives a call from a user regarding a technical problem; a break/fix ticket is created within the Bureau Remedy system, and then assigned to the specific EUC section that supports the identified user. EUC technical staff receives the ticket, acts in the appropriate method to fix the problem, and upon completion of the task resolves the break/fix ticket within the Enterprise Remedy system. Depending on the severity of the problem and its resolution, a single break/fix ticket may consist of multiple entries that include additional equipment or software.

Exceptions to this process do exist and are listed below.

1. Illinois Department of Transportation is one of the agencies still in the process of moving to this break/fix process. There are currently a number of supported agencies that are not presently using the break/fix process; DNR, DCEO and AGR however, are in the mode of transitioning into this model. The EUC teams have been meeting, discussing and instructing supported agencies in the use of CMS Remedy Help Desk process; however, there exceptions still exist (i.e. agencies not using the break/fix process, or using it inconsistently). Monitoring of this process involves identifying agencies not complying, contacting the agencies' respective representatives, and advising them of the break/fix usage process currently in place. The current transitional situation involves socializing the EUC Staff and the Business Side of the consolidated agencies to use the Helpdesk and follow the procedures as an organization, the majority of the work currently is put through the Remedy system but there are still inconsistencies and some work make still be taking place outside the system by staff on both sides of the new process still using the old processes or calling staff directly to get issues fixed quickly. The EUC

team and management is working to change this culture but it will be a while before all the issues are worked out and all parties are using the new processes consistently.

2. The Non-Consolidated, but Legacy CMS supported, agencies (see table 1) use this process inconsistently and may, at times, directly contact technical staff. When this occurs, the agencies' respective representatives are contacted and advised to use the break/fix usage process currently in place. The current transitional situation involves socializing the EUC Staff and the Business Side of the consolidated agencies to use the Helpdesk and follow the procedures as an organization, the majority of the work currently is put through the Remedy system but there are still inconsistencies and some work may still be taking place outside the system by staff on both sides of the new process, EUC and Business Side, may still be using the old processes or calling staff directly to get issues fixed quickly. The EUC team and management are working to change this culture but it will be a while before all the issues are worked out and all parties are using the new processes consistently.
 3. Emergency Situations: Emergency situations are major outages or specific PC failures for a critical individual. These occur during non- business hours, when the Service Desk is unavailable, and normal processes will delay reaction to the situation. These types of situations are documented and entered into the Enterprise Remedy Help Desk system during normal business hours.
- **Enterprise Service Request Process (ESR):**

This is a daily function of the EUC technical staff. Authorized staff of the supported agencies fills out and file service request template forms for scheduled projects. All authorizations for these types of requests may involve the following activities:

 4. Moving PCs and printers from one location to another: This type of request may include the reconfiguration of PC software and hardware to meet new location's requirements.
 5. Installation/de-installation of software to PCs. This may be done manually or in conjunction with the Midrange team who, only after receiving EUC confirmed authorizations, remotely install/de-install software.
 6. Installation/de-installation of specific PCs or peripherals.

Monitoring of the ESR process for the End User Computing section of the Bureau is done as follows. The ESR request from the supported agency is sent to the Bureau Service desk, which then enters the request into the Enterprise Remedy System. The Change ticket which is generated by Remedy is then assigned to the EUC supervisor or their assigned representative who in turn creates multiple tasks for multi part projects and assigns them to the appropriate EUC technician. In the cast of a one step project the Change ticket is assigned to the appropriate technician who then creates one task, accomplished the task / ESR request and then resolves the task. At this

point the Change Ticket resolves and after three days will close. The monitoring primarily is done by the CSC.

Exceptions to using the ESR system do exist and are listed below:

1. Department of Natural Resources and Illinois Department of Transportation agencies are still transitioning to this process and have not fully implemented the ESR system on an agency wide basis.
2. A number of Non-Consolidated, but CMS Supported agencies, are still in the process of adopting the ESR system; (see table 1.) however, not consistently. These are agencies are Legacy CMS supported but non– consolidated agencies, therefore not under the IT Rationalization guild lines of CMS. EUC Staff are working with the CMS supported Agencies on utilizing the ESR process.
3. The current transitional situation involves socializing the EUC Staff and the Business Side of the consolidated agencies to use the ESR Process and follow the procedures as an organization, the majority of the work currently is put through the Remedy system but there are still inconsistencies and some work may still be taking place outside the system by staff on both sides of the new process, EUC and Business Side, may still be using the old processes or calling staff directly to get issues fixed quickly. The EUC team and management are working to change this culture but it will be a while before all the issues are worked out and all parties are using the new processes consistently.

▪ **PC Refresh Deployments:**

This is a major IT Rationalization program currently underway where the EUC team is deploying newly purchased PC's at the 12 consolidated agencies. These deployments are either in process or pending due to funding and procurement schedules. PC Refresh Deployment s activity involve imaging, installing, and follow up on any technical issues after the initial installation.

Standard operating processes are in place; however, no formalized policies exist. The EUC Supervisor assigned to the deployment by the EUC Manager monitors of PC Deployments. The EUC Supervisor plans, executes and follows up on any technical issues after a deployment is completed. There are processes in place to receive sign offs from the receiving users for the equipment once the deployment is complete.

Table 1.

Executive Ethics Committee
Governor's Office – First Lady's Office
Governor's Office
Lt. Governor's Office
Governor's Office of Management and Budget
Guardianship & Advocacy Commission

Prisoner Review Board
State police Merit Board
Deaf & Hard of Hearing Comm., IL
Educational Labor relations Board
Office of the Executive Inspectors General
Department of Human Rights
Illinois Assoc. of Minorities in Government
Illinois Assoc. of Hispanic State Employees
Department of Labor
Illinois Student Assistance Commission
Human Rights Commission
Procurement Policy Board
Planning Council on Developmental Disabilities
Civil Service Commission

Vendor Management

The Vendor Management Team is responsible for ensuring effective and efficient management of and compliance with vendor agreements with regard to infrastructure products and services.

Specific functions in support of these responsibilities include:

- Contract Management
 - Participate in Contract Negotiations
 - Monitor/Report on Contract Expiration/Renewals
 - Invoice Approval Processing
 - Direct administration of enterprise critical agreements
- Procurement Management
 - Creation/Review of Purchase Requests
 - Procurement Status Tracking/Reporting
 - Vendor Communication
 - Software/License Receipt/Tracking
 - Software Library Administration
- Budget Management
 - Liaison to Business Services
 - Expenditure Tracking/Reporting

In meeting said responsibilities, Vendor Management acts as a service provider for the Infrastructure Services Division and the Consolidated Agencies. Vendor Management interfaces with Bureau Procurement, BOSSAP, Business Services, EA&S, Legal, and Vendors to fulfill these responsibilities.

Operational direction and guidance for meeting said responsibilities are provided through Vendor Management processes and procedures. Documented procedures are stored on a drive accessible to the Vendor Management Staff.

Enterprise Production Operations Services Processes and Controls:

The Enterprise Production Operations Services (EPOS) area is made up of four functional areas. They are Library Services, Command Center Operations, Input / Output (I/O) Control and Production Control. The processes and controls listed below are for the I/O and Production Control sections of EPOS.

The general duties of the I/O section are two fold. The Input side monitors all production jobs processing on the mainframe to ensure that the jobs come to successful completion. The ones that do not complete successfully are examined for the cause of their abnormal termination (Abend) and are repaired if possible by the technicians on duty. If they are unable to affect the proper repairs there is a call list available for each job that processes. The appropriate applications person is notified and the problem turned over to them. After the problem has been resolved I/O will reinitiate the process and monitor the job until such time as the job comes to a successful completion. Written procedures are in place which are available to authorized personnel.

The Output side of the section is responsible for printing and distribution of all documents and reports generated as a result of the successful processing of the jobs mentioned in the Input section write up.

The Production Control Section of EPOS is responsible for the following activities:

Proc Acceptance – Any new or changed job or system that is presented for acceptance into the production environment must first pass through the Production Control area. The documentation is checked for adherence to standards, naming conventions and run procedures. All must be in order before the job is accepted.

Job setup and processing – All jobs that are processed in the production environment, whether they run through CA-Scheduler or are manually submitted, must be setup and processed by Production Control. Applications people in the DHS production arena do not have access to any production data sets or production files. They cannot execute any production processing. It must be done by the production control section.

Abend Resolution – Any time a job abnormally terminates and it is due to a cart problem or a problem with how the job was setup for processing, the people responsible for the job in the production control correct the problem and restart the job. If it is a problem with the job itself, it takes someone from applications to fix the problem. In that case the applications people fix the problem, then notify production control and they resubmit the job. Written procedures are in place which are available to authorized personnel.

Automated Distribution and on-line viewing of reports – The majority of the output from jobs processed for the Department of Human Services pass through the Mobius Automated distribution and on-line viewing system. All jobs that produce output, whether it is to be printed or to be

viewed on-line are setup by staff in the Reporting unit of the Production Control Section. Written procedures are in place which are available for authorized personnel.

The following are the physical controls that are in place at the Harris Computer Facility:

- Security Guards are in the front entry way.
- Security Cameras are strategically located around the building, inside and out.
- All areas within the Harris Computer Facility (HCF) have proximity readers and you must have a badge with the proper accesses in order to enter.
- Special brightly colored badges with very limited accesses are available for use by individuals entering the building to pick up printed output from the I/O Control area. These badges will only open the first set of double doors leading into the first floor of Harris I.

The individuals picking up output are instructed to go to the pick up window. If the reports are too large to fit through the window they are taken out the door and handed to the person picking up the report.

Individuals must identify themselves and say what reports they are there to pick up. The individual is then looked up on the “Focal” system which contains a list of individuals that are authorized to pick up reports from I/O Control.

They then must sign the report manifest indicating they received the correct reports.

They are then reminded to return their badge as they exit the building.

For Payrolls processed by the CMS Production Control area for other agencies and entities the following procedures are in place.

Payrolls are processed and printed out for Department of Human Services (DHS) Department of Natural Resources (DNR) Department of Corrections (DCOR) Department of Children and Family Services (DCFS) Department of Juvenile Justice (DJJ), Home Services and Contractual Services.

The DHS payroll is given to the DHS messenger. The messenger takes the payroll to a designated person in the Harris Facility for Signatures. It is then taken to the office of Central Payroll. No signatures are required as it is all handled by DHS personnel and only goes to DHS locations.

For DNR, DCOR, DCFS, and DJJ these payrolls are processed, packaged and taken to the office of the Security officer for DHS. Each agency has authorized individuals who come to the HCF and get special badges that allow them access to the Security officers office where they pick up their reports. They must identify themselves to the security officer and sign the manifest showing that they have taken possession of their reports.

For Home Services Payroll, it is processed and given to Linda Mckinney from the payroll department. There are no signatures required as these reports are hand delivered to the appropriate person.

For Contractual Services Payroll, it is processed and given to Jonel May from the payroll department. There are no signatures required as these reports are hand delivered to the appropriate person.

Mainframe - Systems Programming

z/OS

The primary operating system at the Department's Central Computer Facility is Zero Downtime Operating System (z/OS). z/OS is a complex operating system used on mainframes and functions as the system software that controls the initiation and processing of work within the computer. The System Management Facility (SMF) records the activity within the operating system. The some subsystems that run on z/OS are IMS, DB2, CICS, MQ series, NEON, SMS, HSM, TSM, JES, CA-scheduler, Mobius, HSC, TMS, etc.

The agency RACF administrator must submit a request to the CMS RACF staff if a user ID needs to have TSO access on the mainframe.

z/VM

The Department's secondary operating system utilized at the Central Computer Facility is Virtual Machine (VM). VM is time-sharing, interactive, multi-programming operating system for IBM mainframes. The major subsystem that is supported in VM is NOMAD.

The agency RACF administrator must request and obtain a VM User ID from the z/VM staff. Agencies are assigned user IDs with the most restrictive security rights. The VM directory is restricted, which contains information regarding user IDs, mini-disk size and location, and operating functions.

SECURITY

The Department utilizes security software to control access and protect resources. The security software is the primary tool for controlling and monitoring access to the Department's computer resources. A user ID is used to identify the client along with a password to verify the client's identity. The Department maintains a log of all access attempts, which is used to monitor unauthorized access attempts and identify areas of weakness. Clients are responsible for protecting their program and data files.

The Department has appointed staff with primary responsibility for the implementation and administration of the security software. The Department has a procedure in place for the monitoring of security violations. The CMS Data Security Administrator reviews violations with CCF violation reports being distributed to staff for which they must be signed and returned with

an explanation. The agency RACF administrators have the capability of producing the reports for their agency.

CHANGE/PROBLEM MANAGEMENT

System changes follow the Department's Information Management Change and Problem procedures (INFOMAN). There are three types of changes that may occur to the environments: reported problems that can be isolated to a specific module, Program Update Tapes, and new versions or releases. Initial Program Load requests are handled in the same format.

Mainframe - Database Management

DB2

DataBase 2 (DB2) is a relational database management system for z/OS environments, which the Department makes available to customers. The Department has established ten+ subsystems at the Central Computer Facility

The Department has assigned staff to monitor the performance and problems of DB2. The DB2 staff is also responsible for software installation, maintenance and security.

All customers who access DB2 are required to have a security software ID and password. The customer must authenticate to the security software first. If the customer authenticates, DB2 allows access. DB2 internal security verifies access rights to specific data. The Department authorizes one user ID at each agency to coordinate the use of DB2 within the agency. This user ID allows each agency to create its own authority.

The DB2 Software Support Group will monitor specific application problems when customers call. System performance is monitored on a continuous basis. The Department's Information Management System is utilized to report and document problems.

CICS

The Customer Information Control System (CICS) is a software product that enables online transaction processing. CICS allows numerous transaction types, entered from multiple terminals, to be processed concurrently by customer written application programs. CICS acts as an interface between the operating system and application programs.

The Department offers three different levels of CICS support for customers, described as follows:

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

- **Level Three** – The Department supports the CICS software, maintains CSD/table definitions, and supports both CICS and the application software for the agency. The Department is also responsible for security for these regions.

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

IMS

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

Infrastructure Services-Midrange Services-WinTel

WinTel Services is responsible for the configuration and monitoring of the Department’s Intel based servers running the Microsoft or Novell Operating System. Additionally, this group is responsible for all consolidated agencies’ Intel based Servers running the Microsoft or Novell Operating System. Until the physical consolidation of the merged agencies, the Intel based Servers running the Microsoft or Novell Operating System are being maintained under the respective agencies policies.

Configuration changes are managed through the Department’s change management process. (Lotus Notes)

Policies are available on the Unit’s secured Sharepoint site. Administrative access to the servers is controlled by WinTel Management. No administrative rights are granted without prior written management approval.

Infrastructure Services-Midrange Services-Unix

The UNIX Services Group is responsible for the installation, configuration, maintenance, and general health and well-being of the Bureau’s distributed UNIX environment. The current exceptions are the Department of Healthcare and Family Services (DHFS) and Department of Public Health (DPH) IBM System P servers. Additionally, this group is responsible for the consolidated agencies’ UNIX servers. Until the physical consolidation as well as a formalized transition plan that is executed, the infrastructures are being maintained under the respective agencies processes and currently established processes.

The UNIX Services Group is responsible for the backup and recovery of the DHS IBM System P servers and the DHFS SUN servers.

Configuration changes are managed through the Bureau's Lotus Notes Change Management System.

Policies, procedures and standards are currently being analyzed for the UNIX Service Group. Informal processes are currently in place that allow authorized personnel to perform duties.

Enterprise Capacity Performance and Storage (ECPS)

Enterprise Capacity Performance and Storage (ECPS) is responsible for the allocation, backup and removal of storage for the Bureau's mainframe systems, Bureau open systems and the defined agencies consolidated into the data center. The team is also responsible for the backup functions associated with these systems.

Backups are run on 2 different environments

OPEN SYSTEMS: The storage team currently performs backups for the following agencies at the data center CMS, AGR, DNR and DCEO. The policy by which data is being backed up is the previously defined agency policy.

New servers are backed up after a server backup request has been completed and reviewed by storage staff. This form is located on the sharepoint site for the backup team. Most existing servers are on a defined backup schedule, although there are some servers which are not being backed up (test, development and some application servers may not be backed up). This is by agency request, and usually includes test servers which are not considered important enough to warrant backup.

In the event of data needing to be recovered from backups a Bureau REMEDY problem ticket is opened and assigned to the storage team. After a completed restore, the ticket is closed and user notification sent.

Offsite vaulting is in place for backups. Documentation for this process is located on the team sharepoint site.

ZOS BACKUPS: backups are performed on the mainframes systems data. System data is backed up daily and weekly with the weekly copies sent to the regional vault on a 4 week cycle. Backups are also performed by HSM. These backups are controlled by the SMS routines and are set by the user at allocation time. When the user allocates a new file a management class is assigned which determines how long the data is kept.

(TSM) Tivoli Storage Manger backs up UNIX files on the ZOS. The retention policy is in accordance with the Department's policy.

Restores are processed after an INFO management ticket is opened. Procedures are documented on the shared network drive for resource management.

Storage:

Storage requests are generated in either INFOMAN (ZOS) or Bureau Remedy (SAN). The requestor must fill out a disk space request form located on the team sharepoint site. After management has evaluated if the requested space is available either a change management ticket (Lotus Notes) is generated to add the needed disk or a procurement is created to purchase the needed disk. Once the disk is online a backup request form is generated to insure that the disk is being backed up. Procedures are located on the sharepoint site along with the resource management shared drive on the network.

Infrastructure Services - CCF Tape Library

The Tape Library is located at the Central Computer Facility. Access to the Central Computer Facility and the Tape Library requires an access card with appropriate access rights. The user agency is responsible for providing Department Security with current authorization lists of staff that may request assigned media movement.

Security officers and Tape Librarians are responsible for confirming that individuals are authorized to deliver or remove media. A Security officer and a Tape Librarian must verify that the triplicate media transmittal forms are correct, signed, and retain a copy. All media is identified with unique tracking alphanumeric identification numbers (volume serial number). The Tape Management System (TMS) is utilized to track and record the location of media. Carts not listed in TMS are transient carts recorded in database called the Transient Tape System (ITTS). The media in and out transmittals and procedures are used in the same manner for these types of tapes.

The "Library Services Vault Transmittal Procedures" outline the procedures to be conducted during the movement of media. This includes transportation of media to and from the secured off site vault.

The tape library is responsible for the backup tapes of the DHS **WINTEL** servers. These are handled with the same control measures as other tapes using the authorization list for verification and the media transmittals being checked and signed. Additionally, the tape library has taken over the Concurrent server backups, but are still working out procedures.

Twice a year, the Data Security Administrator sends user agencies a Security Authorization List, an Information Management System Authorization List, and a Tape Diskette Authorization List, which are to be updated and returned within two weeks.

Infrastructure Quality Assurance and Methods

Service Description

The Infrastructure Quality Assurance and Methods (IQAM) organizes, plans and controls work activities for the Infrastructure Services Division as directed by the Infrastructure Manager.

Infrastructure Administration includes reviewing Pending Gate 3 charters, functional and non-functional requirements, gathering and organizing detail design activities, tracking and documenting issues and action items, status reporting, documenting work processes, and coordinating activities between client agencies and the Department.

IQAM organizes and coordinates technical resource and service support to ensure availability of Category 1 agency business applications.

IQAM works with EPMO staff to understand direction and priorities of the Bureau. We also work with EPMO to validate correct process is being followed according to Governance.

Depending on the objective or subject matter, the audience may include State agency executives, technicians, and internal Department staff.

The tool we currently use to gather detailed design documentation is the Project Assessment Requirements (PAR) form. This is a Microsoft Word template.

Infrastructure Services - Data Center Operations

The Command Center is the Systems Operation Center component of the Bureau's Enterprise Production Operations Services organization. The mission of the Command Center is to provide continuous monitoring and operation of the Bureau's computing resources to ensure availability, performance, and support response necessary to sustain customer business demands.

The Command Center operates twenty-four hours a day, seven days a week, 365 days a year. The Command Center is responsible for the monitoring of systems, responding to system messages, and logging problem calls concerning the availability or performance of the systems and the applications running on the systems. The monitoring of systems is divided among the personnel in the Command Center.

The Command Center is responsible for documenting daily actions and events which affect the status of the computing environment and customer business functions. Additionally, the Command Center maintains availability and functionality of computing resources as scheduled in support of customer business needs and coordinates and oversees implementation of changes to the computing environment.

The Bureau maintains several reports that record the Command Center activities. The following reports provide a complete record of all operator actions: SYSLOG, Shift Change Checklist and

the Daily Shift Report. In addition, the Bureau utilizes INFOMAN, a management tool, to record and monitor the progress of problem resolutions.

Additionally, the Bureau collects, reviews, and analyzes operating statistics to identify trends, detect problems, and project future resources through the following reports:

- Availability Report - reflects the system and application availability on a daily and weekly basis.
- Resource Management Facility Report - reflects CPU utilization by system and machine, as well as the average and maximum number of users at any one time.
- D-Collect Report - reflects space, allocated space versus space used.

Risk Management

Recovery Services

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

The following contingency plans address restoration of various client environments:

- Continuity Methodology,
- Recovery Activation Plan,
- Network Services, Recovery Activation Plan.

Each state entity is responsible for coordinating recovery services with the Bureau.

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

The Bureau maintains a Statewide Critical Application Listing based on information received from State agencies. State agencies are required to prioritize their applications in one of five categories:

- Human Safety: (Category One) Resources that directly impact the lives and safety of Illinois citizens, including state employees.
- Welfare Human Service: (Category Two) Resources that directly impact the well being of Illinois citizens.
- Non-Welfare Human Service: (Category Three) A human service resource that indirectly impacts the welfare of Illinois citizens.
- Administrative State Functions & Processes: (Category Four) Resources that support the administration of state processes.

- Support of Specific Agency Functions & Processes: (Category Five) Resources related to the maintenance of a specific agency function or process.

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

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

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

Physical Security BCCS

The Department utilizes an access card system to provide control over access to many of its facilities. The system utilized is Hirsch/Velocity (H/V), procured from a master contract with A1-Lock, Inc. The system controls and logs the use of access cards (badges and/or PINs) at the Central Computer Facility, Communications Building, the Benefits Building, and the Business Services Building.

For the above facilities, all employees, visitors, vendors/contractors, and State agency representatives are required to be assigned a badge with appropriate access privileges. Requests for badges are submitted to the Risk Management (RM) Division for activation. Individual access privileges are based on job duties. Visitors and employees who forget their access card are required to sign-in and register at the guard's desk. The RM division also produces card and PIN credentials for over 40 State Agencies, although these credentials do not adhere to CMS/BCCS policy, and some badges are for use as authentication credentials only, in lieu of providing any electronic door access.

The RM division houses an issuance procedure document outlining how to control the adding and modifying of credentials in this system. The H/V system is pre-populated with certain data fields to serve as a control when entering new data. Other critical controls are employee pass-back and the establishment of absentee limits, which are in use at (and between) the CCF and the CCC and the benefits building. The system also produces routine access listings to display who has access to which doors and door groups, so management can determine if the list is accurate.

The badges are FIPS 201-1 compliant and contain the proper text to outline cardholder responsibilities as well as instructions on what to do if a lost badge is found by someone other than the owner. It is also CMS policy to recover employee badges upon employee termination/separation. Non-personal badge credentials are inventoried 3 times per day to ensure no CMS credentials are in the wild.

The Bureau has updated the H/V systems to the latest technology (HID encryption) for the following campuses. They are all now consolidated utilizing a single server housed at the Central Computer Facility.

- The afore-mentioned buildings
- 4 CMS regional buildings:
 - East St. Louis
 - Springfield
 - Des Plaines
 - Rockford / Giorgi Center

Tape-based backups for the H/V system are done on a periodic basis, but they are currently not stored in an offsite location; Recovery testing has not been performed in a timely manner.

In anticipation of pertinent consolidation of Enterprise-wide Access Control Systems, the following Agencies have also been upgraded to the HID technology and are utilizing the centralized server:

- The Department of Commerce and Economic Opportunity (DCEO)
- The Department of Human Rights (DHR)

Video surveillance cameras are located on the exterior of the above CMS facilities, as well as strategic locations within the interior. Video feeds are monitored on appropriate consoles. Monitors are capable of split-screen imaging or single-screen imaging. Since images from some of the analog cameras are of poor quality and a minimum amount of retention (a one-week supply of video tapes) is maintained, BCCS has initiated a video upgrade program for its 3 facilities:

- 201 W. Adams
- 120 W. Jefferson
- 726 S. College

These upgrades are in concert with the new H/V Access Control System upgrades and are intended to accommodate future expansion in the form of consolidating State Agency Access Control and surveillance requirements, migrating from decentralized disparate systems to a single Network Video Recording (NVR) system, allowing for significant cost reduction as well as provision of consistent operational and security deployments.

To date, BCCS has upgraded its video surveillance systems roughly 70%, with multiple IP cameras installed and the majority of the Infrastructure work completed to allow for discontinued use of analog surveillance and the ability to accommodate future expansion and integration of State wide video systems.

While the commencement of this project has seen limited success to-date, there are no controls or procedures in place to set its deployment or usage metrics.

Technical Safeguards Unit

Subsequent to consolidated agencies server relocations to the Department/Bureau Data Center, the Technical Safeguards Unit (TSU) conducts vulnerability scans to evaluate network components for vulnerabilities using plans, procedures, and specific scanning tools. Note: The server scanning schedule is being performed in the same order as the server relocation schedule. Appropriate Bureau personnel are apprised of any findings along with recommendations to remediate the known vulnerabilities.

During the vulnerability scans, the team conducts security assessments to determine if baseline standards for servers (and desktops as appropriate) are being implemented. The assessments include confirming that patches have been applied in a timely manner and validating that password best practices are in use.

The team also performs external penetration testing of the relocated servers to identify vulnerabilities, focusing on the servers, infrastructure, and underlying software to complete a comprehensive analysis of the environment. Vulnerabilities within the environment are then identified, enumerated, and the implications assessed. Mitigation strategies are created and forwarded to the appropriate Bureau team for remedial action.

Under direction of the Risk Management Executive, the team participates in the development and assemblage of computerized material for use in any investigations, litigations, or other informational requests initiated by State Agency Management, Illinois Inspector General, Illinois State Police, Illinois Attorney General or other law enforcement entities. Where applicable chain of custody procedures are followed.

The Technical Safeguards Unit actively participates in appropriate procedures when an event occurs that has the potential of breaching security or disrupting service. The staff implements specific safeguards and takes pre-determined actions as well as providing information to law enforcement or inspector general personnel.

The unit collaborates with other Bureau teams to develop and deploy technical policies and/or procedures, including firewall/port, wireless, software patching, vulnerability assessment, and VPN.

Change Management

The Change Management team has participated in the deployment of the first phase of the Enterprise Service Request (ESR) project which supports the Department in providing shared services to the consolidated agencies. ESR is a Remedy based tool that provides a standard method for processing routine requests for hardware or software changes for the end-user community.

Key Performance Indicator (KPI) reports display how many requests are processed and their status. ESR training classes and materials (offered to the consolidated agencies), and process documentation provide steps on how to use the system.

The Illinois Office of Internal Audit (IOIA) reviewed this system prior to production deployment and drafted a memo to Director Campbell stating the system was acceptable for use and presented only residual risk to the Enterprise.

The Department's change management services are facilitated through two systems based on processing platform. "INFOMAN" is limited to mainframe changes, incidents, and notifications. The other Change Management System is a Lotus Notes based tool, and is used for midrange and distributed platform based changes. No mainframe changes are reflected in the Lotus system. Access into each system is shared by mainframe and midrange support staff. There is open participation in each platform's weekly change meeting enhancing communication and ensuring that the impact of a change does not adversely affect another resource.

The Enterprise Change Management System (ECMS) policy and the Lotus Notes 'Change Management Database User Guide' help to ensure the procedures are in place to support the Lotus Notes Application. Introductory (overview and awareness training) documentation is provided to new users as well as an offering for hands-on training. KPI reporting is done on upon request, reflecting changes by category and RFC status.

A change affecting a midrange or distributed platform resource is facilitated through the submission of a Request for Change (RFC). The RFC is reviewed by the Change Management team and assessed for impact to the environment. Once the impact has been assessed, the Change Management team may request that follow up items be completed by the RFC owner before final approval is granted. Weekly meetings are conducted to review submitted changes.

A Change Advisory Committee (CAC) is in place that includes delegated representatives across the Bureau and provides additional input during the weekly meetings. The CAC meets each Wednesday. To be included in a Wednesday RFC review, RFCs must be received no later than the day before, Tuesday. The Change Team records meeting minutes, RFCs reviewed, and assesses impact of proposed changes.

All Production CMS Servers or other hardware assets must follow legacy change management procedures related to any configuration add, move or change within the CMS / BCCS organization.

Any rationalization effort managed by CMS / BCCS related to the temporary or permanent relocation of Production Servers or Hardware Assets across the consolidated agencies (consisting of the following state agencies: AGR, DCEO, IDES, DNR, DHS, DOT, DPH, EPA, FPR, HFS, or REVENUE) must follow legacy change management procedures related to any configuration Add, Move or Change.

Any regional sites, remote office facilities, or locations otherwise that contain any Production Server or Hardware Asset that has a CMS inventory tag and is attached to the CMS Production Network and is supported or maintained by the CMS / BCCS organization must follow legacy change management procedures related to any configuration Add, Move or Change.

Any Production Application changes or new deployments that are related to a request ticket logged in the Service Request Registration System (SRRS) must follow legacy change management procedures.

Any incident / request ticket logged within the ICN Remedy tracking system that are related to any Production Server or Hardware Asset configuration Add, Move, or Change must follow legacy change procedures.

Administrative Safeguards Unit

The Risk Management Executive serves as the chairman of the Bureau Policy Review Board (PRB). The PRB was formally established in October 2006 with the signing of the Charter by CMS executive management, and accompanying bylaws and policy submittal instructions clarify the processes.

The Administrative Safeguards Unit (ASU) manager functions as administrator for the PRB performing several management duties, including developing, reviewing, and publishing policies and procedures that relate to Bureau-managed resources. The PRB Sharepoint site serves to track and monitor PRB activity, and an Access database has been developed to accommodate policy issuance tracking.

The following IT security policies/procedures have been approved:

- Shared Services Standard Glossary
- IT Security Policy
- Use Policy
- IT Users Procedures
- Standard of Relevant Laws and Regulations
- Data Classification Standard
- Availability Policy

Until the PRB publishes new policies, the following IT security policies remain in effect:

- Department Policy Manual (each section is dated);
 - Information Technology Security Policy (dated April 26, 2002) included as Chapter 4, Section 3 of the Department Policy Manual
- Statewide Internet Security Policy (dated December 11, 2001)
- Information Security Policy - Local Area Network (LAN)/Office Automation (OA) (dated May 26, 1995)

- Statewide Information Security Policy BCCS/CCF Internal (dated February 4, 2003)
- Office Automation Coordinators Manual (dated February 2003)

This unit recommends system development guidelines to help ensure the security of information which is processed, stored, maintained, or transmitted on computing systems managed by the Bureau Enterprise Business Applications Systems (EBAS) team. The Illinois Office of Internal Audit (IOIA) and the EBAS team have been furnished with the Risk Management Minimum Security Controls for Applications Development Systems document.

The unit also serves as Bureau liaison to the Department Chief Operating Officer (COO) in the ongoing development of the Department Continuity of Operations Plan (COOP). The work is mapped against a checklist provided by the CMS Chief Operations Officer (COO) staff in charge of the COOP.

Customer and Account Management

The Customer and Account Management unit is comprised of Field Operations, the Communications Management Center, and the Communications Solution Center.

Field Operations

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

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

Field Operations began serving State agencies within the last couple of years as part of the State's consolidation effort. As a result, some of our processes may be specific to the legacy ICN constituents of the education community, libraries, museums, municipalities and other not-for-profit groups, while others are specific to State agencies. Field Operations utilize two versions of Remedy for constituent connectivity provisioning. Agency provisioning is via a Bureau version of Remedy, where all other constituent and non-agency records, provisioning and trouble ticketing is via ICN Remedy.

Field Operations is responsible for the following Services, Provisioning, and Support:

- **Services** (see <http://www.illinois.net/services/default.htm#tech> for a listing of services)

- Consultation – help constituents design efficient and cost effective network connectivity, identify circuit options, and identify appropriate equipment.
- Filtering – perform sales and ongoing support for content filtering software designed to allow constituents to restrict access to inappropriate content on the Internet. Support includes router configurations, setting up user accounts, adding IP addresses, providing end user training, and troubleshooting problems. Primary constituents using this product include municipalities and K12 education sites.
- IP Video – consultation, installation and troubleshooting IP based video conferencing systems.
- Monitoring/Analysis – monitor constituent connections for up/down status and provide constituent access to utilization data for their circuits.
- Configuration services – multicast and quality of service (QoS) configurations for specific applications including video streaming, IP voice and video, and preference cueing.
- Technical Support – support and dispatch for circuits, equipment, and services.
- IP Addressing – maintain and assign Internet Protocol (IP) addresses.
- DNS – configure and maintain Domain Name Service (DNS) for domain name resolution services.
- **Provisioning**
 - Circuit orders – place orders for circuits with telecommunication companies (telcos) and maintain a database (ICN Remedy) of all circuits connected to the ICN for both legacy ICN constituent connections and State Agency connections. Track installation dates and keep constituents notified of status via email and phone. Process Moves/Adds and Changes (MAC) to existing services. CMS Remedy is used by Field Operations staff for processing work orders initiated by the Customer Service Center (CSC).
 - Installations – visit constituent sites, install and configure equipment, connect and test circuits. Track and record inventory.
- **Support**
 - Technical Support – Provide Tier 2 and 3 level support for constituent connections, equipment and services. Perform or arrange for repairs, replacements, upgrades, configuration changes and provide information. Work is documented and tracked using the trouble ticketing and circuit ordering modules of ICN Remedy and via Email.
 - Maintenance – Provide on site emergency repair and regular maintenance and equipment installation at network backbone points of presence (POP sites).
 - Cost Recovery – Provides quotes, bandwidth allocations and adjustments, vendor pricing verifications and invoicing support.
 - Out reach – meet with potential constituents, perform sales services and present at meetings/conferences.

Tools used to complete tasks include the following.

- *Solar Winds* and *What's Up* monitor constituent connections and local services.
- *Solar Winds* and *MRTG* monitor bandwidth utilization for internal and constituent access.

- Remedy is used for provisioning orders, trouble ticketing, and constituent sites, circuits, and contacts served by Field Operations.
- Lists Serves are used for electronic constituent communications which can be targeted to specific groups such as technology staff, administrative staff, geographic area, etc.

Policies, Procedures and Documentation

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

Constituent Groups

Field Operations staff is the customer facing portion of the network and are in touch with constituents on a daily basis by phone, email and in person. Staff regularly meets with constituents to discuss connecting to the ICN, when performing installation and service calls, and by participating in meeting, conferences, and workshops sponsored by constituent groups and organizations.

Communication regarding network issues, maintenance, outages, and network slowdown is sent to constituents via our customer database list serves. Notices and announcements of network updates, costs and bandwidth allocations, conferences, vendor services and workshops are communicated to constituents via our customer database list serves and are posted at www.illinois.net.

Staff contact information is available to the public at <http://www.illinois.net/support/default>.

Customer Management Center (CMC)

The CMC is the 24/7 network support center for the State of Illinois. The CMC supports the backbone and customer access circuits for all legacy ICN customers such as the educational community, which includes K-12 schools as well as libraries, museums, hospitals and other non for profit organizations. The CMC also supports consolidated agencies, the multiple boards and commissions, and non-consolidated agencies. After 5:00 PM and during non-business hours, weekends and holidays, the CMC provides emergency help desk support for voice, wireless, and data services. The CMC is also responsible for processing Change Management issues that pertain only to the ICN backbone. The Bureau uses the Bureaus' Lotus Notes Change Management system to track events, and deliver outage notifications to affected parties, when controlled

outages are initiated via Change Management. For ICN customers (educational and State agencies), the CMC acts as the first point of contact between the trouble initiator or end-user and any internal/external vendor/resource that has a required step in isolating and repairing network incidents. Incidents are managed in accordance with established procedures.

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

CMC supports the entire legacy ICN network. CMC regularly deals with agency help desks, problem sites and associated user contacts. The magnitude of issues varies from a single point site problem to one that may have a statewide affect.

Communications Solution Center (CSC)

The CSC is responsible for providing Tier 1 support for Telecommunications (excluding Illinois Century Network and Radio) and IT services. The CSC is a single point of contact (SPOC) where client solutions are handled for different technologies and simplifying end user support. The CSC is responsible for validating and verifying the performance, timelines and value of the products and services offered through the CSC Service Desk and the vendors supporting those products and services.

Telecommunications Service Desk

The Telecommunications Service Desk is comprised of 4 units (Help Desk, Provisioning, Consulting and Procurement, and Quality Assurance). There are two Consulting and Procurement staff members in the JRTC Building in Chicago. The Telecommunications Service Desk is responsible for maintenance and provisioning of voice, video, data and wireless systems and services for State agencies, departments, constitutional officers, commissions, boards, universities and institutions. The Telecommunications Service Desk handles all calls for telecommunications services during regular business hours Monday thru Friday 8am through 5pm, excluding ICN and Internet calls which are routed directly to the CMC. All telecommunications service calls outside regular business hours and on holidays are handled by the CMC.

The Help Desk currently uses multiple systems to record incidents (VOTS, MONIES and Bureau Remedy). VOTS is an Access 97 database and is used to record all voice incidents; MONIES is used to record non-ICN data incidents; and all wireless incidents are recorded in the Bureau Remedy Help Desk module. Issues are reported to the Help Desk by phone. The Help Desk is responsible for all reported incidents from the time the incident was reported until resolution and confirmation from the customer is achieved. Procedures exist for the Help Desk task.

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

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

The agency coordinators have access to MONIES and can check status of their agency orders only. The MONIES system tracks ordered and installed facilities and telecommunications equipment. The inventory module does not track an asset's cost, but does provide location information along with user name, tag number, serial number, 'AU' code, maintenance vendor description, catalog description and model description. The inventoried asset's installation and monthly recurring costs can be found for all rated catalog codes in the MONIES Inventory Catalog Maintenance menu module. Anytime an inventoried piece of equipment is installed, removed or moves from one location to another, an order is entered into the MONIES system to update the system inventory.

Tagged data equipment is received and tagged by Business Services' warehouse staff while tagged voice equipment is sent directly to the site. Newly tagged items for data entries into MONIES are uploaded into the Central Inventory System (CIS) Suspense File nightly by a batch job. A Property Control Form (PCF) is completed for newly tagged voice entries into MONIES and attached to the original invoice before it is sent to Business Services for processing and entry into CIS. The voice system is tagged by the Consulting and Procurement staff at the time of acceptance. Tagged data and voice equipment listed in MONIES is reconciled to the listed equipment in CIS annually by Business Services. Discrepancies are reported to CSC management and investigated. Appropriate reconciliation is then taken.

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

This unit is also responsible for managing master contracts and site/service specific contracts for telecommunications equipment and services. Network Services assists this unit with the review of TDRs that are related to the ICN backbone and LAN requests for the Consolidated Agencies.

Network Services assists with the review of TSRs for complex procurements and installations such as new Automatic Call Distributors (ACD), Integrated Voice Response (IVR) systems, and large Private Branch Exchange (PBX) systems.

The Quality Assurance (QA) unit analyzes the information gathered from MONIES to generate monthly reports based on a fiscal year to track and monitor CSC performance levels for voice orders. Task related reports are available.

- The Quality Assurance (QA) unit analyzes the information gathered from MONIES to generate monthly reports based on a fiscal year to track and monitor vendor performance levels for completion of voice orders in the Springfield and Chicago dedicated areas, the non-dedicated areas, non-routine orders and the overall vendor performance level. These figures are reconciled with the appropriate vendor(s). The CSC managers and QA staff attend a quarterly meeting with the vendor(s) to review task related reports.
- The QA unit generates a monthly voice incident report based on a fiscal year from the VOTS system to monitor the vendor(s) performance levels for voice related services. These figures are reconciled with the appropriate vendor(s). The CSC managers and QA staff attend a quarterly meeting with the vendor(s) to review task related reports.
- The QA unit generates monthly reports based on a fiscal year from the Avaya phone system to track the monthly CSC Telecommunications Service Desk and CMC performance levels. Task related reports are available.
- An Avaya phone report for the IT Service Desk that tracks the weekly cumulative performance levels by agency. (IT Service Desk managers review these statistics on a weekly basis.)
- An Avaya Split/Skill phone report that provides a weekly view of individual phone agent statistics by agency. (Information is used to make decisions on phone coverage and workload allocation.)
- A weekly report from Remedy on the ESR process (identified below). (The reports provide a detailed view of all open ESRs by agency.) As a separate tab of this weekly report, a cumulative view of all ESR's is provided as the "ESR Agency Digest".

CSC Telecom M&Ps are stored on the Shared Drive for staff to access (hard copies are available for Chicago staff).

CSC IT SERVICE DESK

The CSC IT Service Desk is responsible for providing Tier 1 IT technical and end user support to the consolidated agencies as well as the multiple boards, commissions and non-consolidated agencies. The IT Service Desk is the single point of contact for reporting IT incidents and requesting new services. The IT Service Desk utilizes the Bureau's Remedy to record and track incidents and service requests. The physical consolidation of service desk staff for 7 of the 11 agencies in Springfield was completed in October 2006. The CSC IT Service Desk In Springfield is comprised of 3 separate teams which provide support to designated 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 HFS and DHS. Evening coverage for

HFS and DHS is provided by production operations staff working at the legacy agency locations. Appropriate security is inherent to the tool used.

Chicago-based IT Service Desk staff (DES and DFPR) remain at their legacy location utilizing the Bureau's Remedy for ticketing and legacy phone systems/numbers for inbound calls.

Customers contact the IT Service Desk via phone or email to report an incident. The Service Desk staff opens a ticket in BCCS Remedy and records the category, type, and item (CTI), as well as the customer name, agency, contact and demographic information and a detailed incident description. If the IT Service Desk is unable to resolve the incident, the ticket is assigned to Tier 2 or Tier 3 support teams based on the CTI and/or description field. The IT Service Desk has processes and guidelines in place for enterprise-wide incident management, escalation and notifications, and other operational needs. These are included in the "IT Service Desk Guide to Daily Operations". Service requests are submitted via email using the Bureau's Enterprise Service Request (ESR) Form (the enterprise service request process has not been implemented at DNR and DOT). Procedures are in place for processing Enterprise Service Requests.

Service Engineering

Service Level Management

Service Level Management currently provides the following two primary activities:

- Management of Service Level Agreements
- Assembly and production of Service Level Reports

Service Level Agreements

The objective of the Service Level Agreements (SLAs) is to provide a basis and framework for the delivery and measurement of Information Technology services that meet the needs and priorities of the Client (Client being the consolidated agencies).

The services reflect technological activities "as is" within each of the agencies, but also reflect a level of negotiation by the Client to close gaps that existed within their legacy IT operations but for which capability and/or staff was not transferred to the Bureau. The first SLA effort was to simply put a "stake in the ground" and establish a baseline to work forward from.

SLAs are subject to periodic review and change. Any SLA changes proposed undergo the Department's internal approvals across appropriate service factories and are documented and tracked by Service Level Management. Upon internal approval, the changes are then presented to the Client agency for their own internal approval process.

Signed SLAs and any service related inter-agency agreements are maintained and recorded by Service Level Management.

SLAs are subject to discussion and change on a quarterly basis, but can be opened for consideration of changes at any time by the Client agency or the Department/Bureau. SLAs will continue to change as new SLM policies, procedures, processes, work-instruction, Service Catalog, Operational Level Agreements (OLAs), measurement capabilities (tools) and new customer demand is introduced.

Service Level Reporting

Current service measures reflect a cross-agency “best fit” view of legacy agency measurement capabilities. The service elements to be measured are reflected within the Service Level Agreements. Currently there is no governing policy over Service Level Management.

Data gathering, to allow generation of service metrics, varies across Client agencies ranging from some automated methods available to a purely manual tracking and reporting process. In some instances the measures were not possible or represented unusual effort within the legacy infrastructure as individual agencies, of different sizes and budgets, each had their own methods of managing their technological environment. Inconsistent operational and baseline metric capabilities coupled with the lack of consistent historical tracking across the Client agencies has added complexity to achieving a uniform standardized approach to service level reporting.

Service metric reviews between the Department/Bureau and Client agencies are scheduled and conducted. The Client meeting and reporting criteria are outlined under Schedule G of the SLA. Metrics are reported and published on a monthly basis via an online tool (PBViews). The monthly “online” report is also available for viewing by the Client agency. Historical monthly metric data is maintained by the SLM unit.

Service level reporting capability will continue to change as new Service Management policies, procedures, processes, work-instruction, measurement capabilities (tools) and new metrics are introduced across the shared service organization.

Control Description: Business Process Engineering

Business Process Engineering (BPE) is assigned the following responsibilities:

- Develop BPE process framework which includes the team’s processes, policies, procedures, standards, tools, work instructions, metrics and required competencies/skill sets.
- At the direction of Bureau leadership, BPE supports project teams and/or process owners in the design, development and potential reworking of new or existing IT service delivery and service support processes.

In meeting said responsibilities Business Process Engineering acts as a service provider to internal Bureau Shared Services teams.

BPE team collaborates with internal Bureau staff and customer agencies, when needed, to design and deliver processes which adhere to the following:

- Review existing processes to determine whether several jobs can be combined
- Determine logical order for processes to use
- Review and eliminate non-value-added activities or multiple overlapping processes
- Apply the most efficient and effective controls and to ensure they are included within the governance/compliance
- Reengineer processes to reduce costs and time and improve efficiency
- Standardize processes, procedures, methods/work instruction, IT services and tools
- Provide Bureau leadership with visibility and opportunities for further process improvements

Currently operational direction and guidance for meeting said responsibilities is provided through a documented process overview and corresponding form templates.

Illinois Office of Internal Audit

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

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

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

DCMS Accounting

By the 20th of each month, BCCS Business Services prepares a summary salary file by agency service center code that is uploaded to the mainframe. The file contains salary and fringe benefits costs for all Black Pearl agency personnel whose time is charged back to their legacy agency. The data is based upon the service center code that was entered into the Service Center Allocation System (SCAS) and applied to the employee's payroll costs for each pay period that month. Detail spreadsheets that list each agency employee's Personal Services, Retirement, Social Security, and Group Insurance amounts for each pay period that month are also prepared by Business Services to send to the agencies as backup once the billing has been created. The file can also contain manual debits that must be processed for a legacy agency.

After the file has been uploaded, Business Services sends an email to CMS Accounting that the payroll file is ready. Accounting sends an email to Enterprise Business Application Solutions Group (EBAS) requesting that an AIS extract be pulled and a generated report be sent to an Accounting printer for review. Accounting verifies that the totals of the extract and EXP5T report agree. If a discrepancy exists, the bureau is notified for resolution. Once reports are in agreement, Accounting emails the EBAS Group and requests a load extract to IBiS. Upon verification from the Accounting Division that billings in IBiS are correct, an ARPS load request form is completed and sent to Operations to load billings into ARPS. If the load report ties to total in IBiS, then Accounting releases the IT billing from IBiS and emails user agencies that billing is available for processing of payments.

When Business Services receives the monthly email notification that the IBiS billings have been produced, Business Services downloads the AIS billing file. The file is sorted by agency, and a spreadsheet file is created for each agency. This detail file lists each invoice that was paid on behalf of the agency that month and includes the agency service center, the cost center, DOC, voucher control number, voucher date and number, vendor name, vendor invoice number, beginning and ending dates of the service, a description of the services, and the amount. The agency salary costs and AIS billing detail spreadsheets are then emailed to agency designated staff. This usually occurs the same day or the day after Business Services receives the notification that the IBiS billing statements are available.

Agencies process billing invoices and remit payments to CMS Accounting. Payments are posted to Billing and Accounts Receivable Cash Management System (BARCS) and to Accounts Receivable Posting System (ARPS). Segregation of duties ensures that cashier functions and billing/accounts receivable duties are performed by different Accounting employees. Credits are initiated by the Bureau and are entered into ARPS by Accounting. Accounting reconciles receipts to Comptroller SB04 Report and reconciles accounts receivables to ARPS. Internal controls exist within Accounting systems edits to prevent fraud. Administrative controls provide reasonable assurance that revenues are properly recorded and accounted for.

Facility Services Management

Physical Security BOPM

The Department has installed a fire suppression and detection system at the Central Computer Facility (CCF). The System utilizes an environmentally friendly gaseous agent. The Department has installed smoke detectors which are connected to the alarm system and local fire/police departments. The Department's Communications Building and the Business Services Building also have fire detection and suppression systems, smoke detectors and fire extinguishers. These controls are tested periodically to ensure operational efficiency.

The Department has contracted with janitorial services to perform duties on a daily, weekly, and monthly basis. The contracts outline the duties and timing of the duties to be performed. The Department conducts background checks and training for each janitorial employee.

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

Real Property Keys

The CCF, Telecommunication Building, and the Business Services Building are designed to have BCSS individuals assigned the responsibility of handling real property keys and to collaborate with Property Management to ensure the keys are properly allocated and tracked, but the identity of these individuals is either unknown or the individuals are not aware of any forms or procedures necessary to accomplish this task.

Security Guards

The Department maintains a master contract with E.L.A. Security, Inc.

This contract states the agencies, which utilize E.L.A. Security, Inc. guards, are required to provide a Post Order Manual for the guards at each location. This is to ensure communication between the guards and their expected duties at each facility.

**SERVICE AUDITOR
DESCRIPTION OF TESTS AND OPERATING EFFECTIVENESS**

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

The results of our review are included in the General Controls (pages 65 through 181) and Application Controls (pages 183 through 207) sections of this report.

This Page Intentionally Left Blank

CHIEF OF STAFF - PROCUREMENT

CONTROL OBJECTIVE

Management should develop and follow a set of procedures and standards that is consistent with the overall procurement process.

EXISTING ENVIRONMENT

Department Description of Control: The Procurement Unit coordinates all Bureau purchase requests and contract renewals including Request for Purchase (RFP), Invitation for Bid (IFB), and Request for Information (RFI) for IT/Telecom items regardless of size or method of procurement that have been approved by management.

Tests Performed: Interviewed staff.

Test Results: The Procurement Unit coordinated contract renewals and RFPs. The Bureau of Strategic Sourcing and Procurement (BOSSAP) coordinated IFBs and RFIs.

No significant exception noted.

Department Description of Control: This system (Provisioning System) routes the electronic procurement form to each designated bureau approver for their review and approval. When the electronic procurement document receives all the required approvals, Bureau Procurement is notified via email. The specific approval groups are managed by the Bureau Procurement Officer and maintained by the system administration staff. All workflow activity is logged in the record's journal. This system was designed to follow and enforce the procurement rules.

Tests Performed: Reviewed Provisioning System and interviewed staff.

Test Results: We reviewed 15 records in the Provisioning System and noted they were approved by appropriate staff members, and workflow activity was included in the record's journal.

No significant exception noted.

Department Description of Control: This system (Procurement Business Case) routes procurement information to each approver depending on the type of procurement. It also serves as a tracking system for procurements.

Tests Performed: Interviewed staff.

Test Results: The Procurement Business Case System routed information to approvers and tracks procurements.

No significant exception noted.

Department Description of Control: The Illinois Procurement Bulletin alerts the Procurement Policy Board of a procurement and allows them the opportunity to review.

Tests Performed: Reviewed Procurement Bulletin and interviewed staff.

Test Results: The Illinois Procurement Bulletin provided information for the Procurement Policy Board.

No significant exception noted.

Department Description of Control: The Bureau Procurement Unit adheres to the following adopted procedures, polices and laws:

- Contract Administration Procedures,
- (Bureau vs. BOSSAP) Roles and Responsibilities - Bureau IT/Telecom Procurements,
- Procedures for creating a Procurement Business Case (PBC),
- Procedure for creating a provisioning request (PRV),
- Illinois Procurement Code/Rules,
- CPO Notices/Bulletins, and
- Bureau Procurement Procedures.

The structure of both the automated workflow using the tools in place and the accompanying progressively approval documents, procurements adhere to the rules and regulations required by the law

Tests Performed: Interviewed staff.

Test Results: The Procurement Unit utilized these procedures, policies and laws to assist in its responsibilities.

No significant exception noted.

Department Description of Control: With the exception of emergency purchases, all procurements follow the rules in place. Emergency requests can only be approved by the State Procurement Officer (SPO) of the requesting agency.

Tests Performed: Reviewed emergency requests.

Test Results: Emergency requests were required to be approved by a State Procurement Officer.

No significant exception noted.

Department Description of Control: The Bureau Procurement Officer conducts:

- Bi-weekly conference calls with BOSSAP to discuss the status of procurements and to address any issues that have arisen.

- Bi-weekly conference calls with their customers to discuss the status of their procurements.
- Weekly meetings with the Bureau Procurement staff meeting to discuss the status of procurements, upcoming heavy workloads, and changes to the policies and procedures.
- Bi-weekly meeting with the Chief-of-Staff to discuss unit issues.

Tests Performed: Reviewed records and interviewed staff.

Test Results: Procurement Unit Management stated conference calls and meetings were routinely conducted.

No significant exception noted.

Department Description of Control: Procurements less than \$250,000 were finalized by Bureau Procurement.

Tests Performed: Interviewed staff.

Test Results: The Procurement Unit was responsible for procurements against master contracts and those under \$250,000.

No significant exception noted.

OVERALL CONCLUSION

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

WORKFORCE AND DEVELOPMENT AND LOGISTICS

CONTROL OBJECTIVE

Management should ensure practices that support recruiting, training, evaluating performance, promoting and terminating staff are well defined.

EXISTING ENVIRONMENT

Background Information Provided by the Department: The Workforce and Development and Logistics unit coordinates and facilitates internal personnel paperwork, workforce training development and implementation, and workforce logistics for Central Management Services - Bureau of Communication & Computer Services.

Department Description of Control: This unit (Internal Personnel Paperwork) has many policies/procedures that allow for proper processing of transactions. Specifically for HR related transactions we follow and refer to the Personnel Rules, the Personnel Code, the CMS Policy Manual, the AFSCME contract, the pay plan, the personnel transactions manual and the alphabetic index.

Tests Performed: Reviewed policies/procedures and interviewed staff.

Test Results: The Workforce Development Unit utilized various policies/procedures for the completion of human resource transactions. In addition, all transactions were sent to the Department's Bureau of Personnel for review and final approval.

No significant exception noted.

Department Description of Control: Initially we are using a new paper training request form and procedure.

Tests Performed: Reviewed training request forms and training database.

Test Results: In February 2007, Workforce Development implemented a new training request form.

The training form was to be completed with relevant training information, supervisory approval, and then submitted to the training coordinator for final approval. Upon approval of the training request, the information was to be entered into a database.

No significant exception noted.

Department Description of Control: We work with the BCCS fiscal office for approval on these training requests.

Tests Performed: Reviewed training forms and interviewed staff.

Test Results: Upon approval from Workforce Development, the training request was sent to Business Services in order to obtain fiscal approval. Business Services was responsible for ensuring the proper funds were available.

No significant exception noted.

Department Description of Control: Travel rules and regulations are followed for approval and reimbursement of travel incurred while training.

Tests Performed: Reviewed travel processes and procedures.

Test Results: In the event training requires travel expenditures, a travel form was required. Travel forms were to be completed in accordance with the Travel Regulations.

No significant exception noted.

Department Description of Control: In order to physically move a union employee we follow past practice of notifying the union 30 days in advance of the move.

Tests Performed: Reviewed notifications and interviewed staff.

Test Results: Upon determination by management that an employee was to be physically moved, the Union was supposed to be notified 30 days prior to the move. We reviewed 20 moves noting, the Union was not properly notified in five instances.

No significant exception noted; however, the Department did not comply with its 30 day notification requirement.

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

Tests Performed: Reviewed position descriptions and interviewed staff.

Test Results: The Workforce Development Unit was responsible for ensuring the Bureau's position descriptions accurately reflect the employee's actual duties.

We noted numerous position descriptions did not accurately represent the duties of the employees. Management stated they were aware of this issue and had initiated a project to update the position descriptions.

No significant exception noted; however, the position descriptions did not always accurately reflect actual job duties.

Tests Performed: Reviewed staffing.

Test Results: Management stated as of April 12, 2007, the Bureau had 133 vacancies for staff.

Our review of the Department identified staffing shortages or undefined responsibilities in areas such as recovery services, help desk, computer operations, and enterprise application development. In addition, we identified over-reliance on key staff members without properly trained backup personnel.

No significant exception noted in the current environment; however, staff vacancies and over-reliance on key employees had not been adequately addressed.

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:

- Assess current staffing and technical experience levels, and develop a staffing plan to address any deficiencies.
- Update position descriptions to reflect actual duties.
- Ensure the Union is notified 30 days prior to a physical move.

EXECUTIVE PROGRAM MANAGEMENT OFFICE (EPMO)

CONTROL OBJECTIVE

Management should establish an effective governance framework including defining organizational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives.

EXISTING ENVIRONMENT

Background Provided by the Department: The overall mission of the Enterprise Program Management Office (EPMO) is to promote and enable the successful attainment of State of Illinois business and technology objectives through approved initiatives, programs, and projects. The EPMO, and its attendant processes also assist in optimizing the allocation and utilization of the State's limited resources (time, money, and people) to accomplish the State's business and technology objectives.

EPMO is divided up into three sections: Strategic Portfolio Management (SPM), Information Technology Governance (ITG), and Enterprise Project Management (EPM). The Strategic Portfolio Management process is responsible for capturing and managing project-related information related to Consolidated Agency business needs and IT strategic plans. The Information Technology Governance process is responsible for evaluating proposed projects, initiated via Project Charters, to ensure business and technology alignment and to determine solutions that are consistent with the State's technology standards. The Enterprise Project Management process is responsible for increasing the overall project success rate (projects that meet their stated business objectives and are completed on-time, within budget, and within resource allocations).

Department Description of Controls: Formal notification from the Deputy Director and EPMO Executive to Consolidated Agency Executive Directors, CFOs, and CIOs to provide their IT Strategic Plan; to identify proposed projects (via the EPMO's Project Portfolio); and to respond with a memorandum from the Executive Director confirming that the Agency's IT Strategic Plan and proposed project information has been submitted, and is complete and accurate. Agency IT Strategic Plans and proposed projects are then reviewed by the EPMO to confirm whether submitted information appears to be accurate, complete and sufficiently clear enough to permit evaluation, classification, analysis, and decision-making. Follow-up workshops with Consolidated Agencies are conducted (as needed) to improve the quality of the information provided.

Tests Performed: Reviewed communications, workshop documentation, and interviewed staff.

Test Results: On September 25, 2006, the Deputy Director sent a communication to the consolidated agencies that requested each agency to identify and submit all of their Business Initiatives (projects), ranked in accordance to priority. Additionally, the agencies were asked to provide their IT Strategic Plans.

All of the consolidated agencies provided information on their projects.

During our review, we noted the Department had received only two of the 11 consolidated agencies IT Strategic Plans and associated Executive Director confirmations. During November and December 2006, the Department held meetings with each of the consolidated agencies to review their project records.

Although a process existed to request information from consolidated agencies, the information received was incomplete, and a mechanism to ensure compliance with the directive did not exist.

Department Description of Controls: Any proposed project that the EPMO determines to be Tier 2 or Tier 3 is referred to the IT Governance process to determine whether a Project Charter has been submitted. Once a charter number has been assigned, it is entered into the Project Portfolio. Project Charters are required for Tier 2 and Tier 3 projects.

Tests Performed: Reviewed projects and interviewed staff.

Test Results: A project charter was required when a project meets the definition of an initiative. “An initiative is an effort with a sponsor and budget that has a defined scope with an estimated start date and an end date. Initiatives can be related to improvement efforts or implementation of a new system, technology, process or service.”

We reviewed a listing of projects requiring a project charter from the Project Portfolio database and found two did not have a project charter.

Project charters were not completed for all applicable projects.

Department Description of Controls: The EPMO also produces various reports from the Project Portfolio to support ongoing governance, budgeting, project status, and management reporting.

Tests Performed: Reviewed reports and interviewed staff.

Test Results: On a weekly basis, six standard reports were produced and made available to staff.

No significant exception noted.

Department Description of Controls: The IT Governance process provides templates and guidelines for Project Charters, Functional Requirements, Non-Functional Requirements, and Project Financials. Submitters have the option to use substitutes for these templates as long as these documents provide the minimum information necessary for assessment and evaluation under the IT Governance process.

Tests Performed: Reviewed templates, guidelines and interviewed staff.

Test Results: The Department developed templates for Project Charters, Functional Requirements, Non-Functional Requirements, Financial Requirements and Post-Implementation Review documentation.

No significant exception noted.

Department Description of Controls: IT Governance, in conjunction with Enterprise Architecture & Strategy (EA&S), evaluates proposed projects for business and technology alignment, possible technology re-use, and potential shared service opportunities. This evaluation includes review of new Project Charters as well as specific deliverables required at each of the governance gates to ensure accurate and complete information is provided.

Tests Performed: Reviewed evaluation procedures for proposed projects and interviewed staff.

Test Results: The Department had not developed formal evaluation procedures or timelines. Department Management stated each project was unique; therefore, the evaluation of each project must be addressed project by project.

We selected and reviewed five projects and found that documentation supporting the evaluation process was lacking and the approval timeline appeared excessive.

The Department had not established formal evaluation procedures or timelines.

Department Description of Controls: IT Governance reviews occur at each of the governance gates to confirm the necessary information has been provided and governance requirements have been satisfied. Missing, inaccurate, or incomplete information is resolved prior to granting approval to proceed to the next gate.

Tests Performed: Reviewed approval process and interviewed staff.

Test Results: The Department had not developed formal evaluation procedures or timelines. Department Management stated each project was unique; therefore, the evaluation of each project must be addressed project by project.

Although projects required approval prior to initiation, we identified five projects which started prior to receiving the required approval.

The Department had not established formal evaluation procedures or timelines. In addition, the Department did not have a mechanism in place to ensure projects adhere to approval requirements.

Department Description of Controls: Proposed projects are presented to the Management Review Board (MRB) and Investment Review Board (IRB) to obtain the necessary management and fiscal approvals. The EPMO provides an agenda that identifies the projects to be considered

at each MRB/IRB meeting and documents any actions taken and/or decisions made. The state and status of these projects are then tracked in the Project Portfolio.

Tests Performed: Reviewed agendas, action items and interviewed staff.

Test Results: We reviewed nine projects noting only two had obtained MRB and IRB approvals. The Department did not have a mechanism in place to ensure projects adhered to MRB and IRB approval requirements.

Department Description of Controls: The EPMO qualifies (ensures adequate sponsorship and requisite resources) and activates (mobilizes resources to initiate) projects that have been approved by the MRB & IRB, by assigning a qualified Program Manager (for Tier 3) and/or Project Manager (for Tier 2) and mobilizing Project Teams.

Tests Performed: Reviewed projects.

Test Results: We reviewed four projects noting a Program Manager had been assigned to each. Additionally, three of the projects had a project team identified.

No significant exception noted.

Department Description of Controls: The EPMO publishes selected Project Management (PM) tools and provides mentoring on selected PM practices (typically derived from best practices and existing State of Illinois PM practitioners)

Tests Performed: Reviewed practices and interviewed staff.

Test Results: The EPMO established a 'framework' to guide project activities.

The Department, in conjunction with Lincoln Land Community College, developed a PM course for state employees.

No significant exception noted.

Department Description of Controls: Weekly Status Meetings are conducted with the Bureau's Leadership to provide updates on current projects. These meetings are utilized to discuss strategy as well as to identify and resolve issues and other project constraints.

Tests Performed: Reviewed meeting minutes.

Test Results: The EPMO provided updates to the Bureau's leadership via Project Coordination meetings. We reviewed the meeting minutes for FY07, noting they provided the status of various projects.

No significant exception noted.

Department Description of Controls: Project Status Reports are provided on a weekly basis and include overall status (Red-Yellow-Green); activities planned for the period; activities accomplished during the period; activities planned for next period; as well as identification of significant issues; risks; and requested management actions.

Tests Performed: Reviewed project status reports.

Test Results: We reviewed three server consolidation projects, noting none had project status reports. In addition, documentation supporting the projects was lacking.

The Department did not have a mechanism in place to ensure project status reports were developed and disseminated, or adequate documentation was maintained.

Department Description of Controls: Project Team Sites (SharePoint) and Standardized Directory Structure/Project Folders are established for each project team to serve as a repository for project artifacts and other pertinent project documents.

Tests Performed: Reviewed project team sites and interviewed staff.

Test Results: We reviewed three server consolidation projects, noting two maintained project team sites. According to Department Management the third project was initiated without EP MO involvement.

No significant exception noted.

OVERALL CONCLUSION

EP MO had not implemented a formal process to ensure all staff were efficiently and effectively meeting its goals and objectives. To enhance the current process, the Department should develop formal policies, procedures, and guidelines to provide clear and consistent guidance to staff. The guidance should promote a formal evaluation process, compliance with requirements, maintenance of documentation and records, project approval, and standard timelines.

AGENCY RELATIONS (AR)

CONTROL OBJECTIVE

Management should ensure the awareness and understanding of business, IT objectives, and direction; including current and future services that are to be provided, and communicate this information throughout the enterprise.

EXISTING ENVIRONMENT

Per the mission statement of Agency Relations, they are responsible for:

- Knowing how and why their assigned Customers do business,
- Serve as the primary contact and provide guidance to Customers,
- Provide coordination as necessary with the appropriate BCCS Staff,
- Identify, clarify and seek timely resolution of emergency business issues, and
- Provide reasonable visibility to each Customer.

The mission statement also states Agency Relations must establish and maintain productive and efficient Customer relationships, and serve as proactive advocates and facilitators focused on anticipating and achieving each Customer's legitimate business needs.

Department Description of Control: Staff are provided processes and guidelines through verbal instruction, understanding and training.

Tests Performed: Interviewed staff and reviewed training records.

Test Results: Agency Relations staff attended training courses and had been provided verbal guidance. Policies and procedures had not been developed to provide guidance to staff.

Although Agency Relations staff received training and verbal guidance, policies, procedures, and guidelines to provide clear and consistent guidance to staff had not been developed.

Department Description of Control: Agency Relations sends out Bureau Deputy Director communications via email to all users, upon approval and signature from the Deputy Director.

Tests Performed: Reviewed Deputy Director communications.

Test Results: A complete history of communications was not retained by Agency Relations. In addition, documentation to support Deputy Director Approval was not always available.

No significant exception noted; however, the process to maintain historical records or ensure Deputy Director Approval of communications had not been fully implemented.

Department Description of Control: AR conducts weekly, bi-weekly, monthly or as needed meetings with Consolidated CIOs, Non-Consolidated CIOs and Department LAN and Legacy

Customers IT representatives. AR records action items during these meetings, works within the Bureau and with agency on action items and follows up with CIO verbally or via email on outcomes. Each AR Liaison uses an agenda to conduct these meetings. Follow up is conducted via email or verbally with CIO/IT manager.

Tests Performed: Reviewed meeting minutes, dates, attendees and interviewed staff.

Test Results: Documentation to support meetings was not available for two of the eight staff members. In addition, the documentation provided to support meetings for the remaining staff members was inconsistent and incomplete.

Although it appeared Agency Relations staff did meet with the various agencies, documentation to support meetings was unavailable, inconsistent or incomplete. As a result, we were unable to determine the extent of user agency coverage and content of meetings.

Department Description of Control: Monthly meetings are held with the Consolidated CIO, Bureau Deputy Director and Executive Agency Relations Manager via bridge conference calls. The CIO has the opportunity to share his/her feedback with overall Bureau services, including, but exclusive to Agency Relations. There are written minutes (issues log) for each of these meetings.

Tests Performed: Reviewed issue logs.

Test Results: Agency Relations Management maintained an issue log for each consolidated agency, identifying issues noted by the agency, correspondence on the issue, date of open and resolution. Per review of the log, the issues appeared to remain open for a number of months before resolved, if resolved.

Although an issue log was maintained for consolidated agencies, it did not appear that all issues were resolved in a timely manner.

Department Description of Control: Quarterly the AR Unit is rated via the Bureau's Overall Satisfaction Survey, sent out by the Service Level Management Team.

Tests Performed: Interviewed staff.

Test Results: Per Department Management, the Bureau's Overall Satisfaction Survey was not distributed to user agencies during fiscal year 2007.

The process to rate the AR unit on a quarterly basis had not been implemented. As a result, agencies were not provided with a formal mechanism to rate services.

Department Description of Control: Agencies that are not included in the aforementioned types of customer service feedback, have been made aware of in written or verbal communication that they may contact either the Agency Relations Executive Manager, Customer & Account Manager Executive, Bureau Deputy Director, Bureau Leadership or any Bureau Senior Management staff

with concerns, issues and/or if they are not satisfied with the representation they are receiving at their agency/board/commission.

Tests Performed: Interviewed staff and review communications to agencies.

Test Results: Agency Relations Management stated, “All customers have been informed via email from various individuals. Additionally, the customers should understand they may contact BCCS senior management, if they are not pleased with the customer service they are receiving from Agency Relations.”

Although it appears Agency relations staff did communicate with the various agencies, documentation to support the communications was not retained.

OVERALL CONCLUSION

Agency Relations had not implemented a formal process to ensure all staff are efficiently and effectively meeting its goals and objectives. To enhance the current process, the Department should develop formal policies, procedures, and guidelines to provide clear and consistent guidance to staff. The guidance should promote routine communications, maintenance of documentation and records, and timely problem resolution.

BUSINESS SERVICES

CONTROL OBJECTIVE

Management should ensure a billing system exists, which accurately charges users for computer services, provides for sufficient audit trails, and supplies users with sufficient information to determine the accuracy of the individual billings.

EXISTING ENVIRONMENT

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

Department Description of Control: The Department has developed procedures for each phase of the SSRF billing process.

Tests Performed: Reviewed procedures.

Test Results: The Department developed the “SSRF ISD/IMS Monthly Bill” procedures. The procedures outlined the step-by-step process for the completion and reconciliation of the SSRF monthly billing.

No significant exception noted.

Department Description of Control: At the end of each phase, verification is performed to ensure all totals are correct. Reports from each source are verified against each other to ensure accuracy of the information. Throughout the process, an “Edit Check” is conducted to ensure completeness and accuracy of each phase.

Tests Performed: Reviewed verification process, “Edit Check”, and interviewed staff.

Test Results: A verification was performed to ensure completeness and accuracy of the data. We reviewed the “Edit Check” and the corresponding source reports for the month of January 2007, noting no exceptions.

No significant exception noted.

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

Tests Performed: Interviewed staff.

Test Results: The Department completed the analysis of costs and revenues.

No significant exception noted.

Department Description of Control: Upon receipt of the paper bill from the vendor, the summary page is provided to CRF billing staff who reconcile against the electronic media received from said vendor. Any discrepancies are reconciled and then the billing can proceed with the appropriate charges. The information is compiled to produce the CRF billings for users.

Tests Performed: Reviewed CRF reconciliation.

Test Results: The Department received billing data and reports from several vendors. Once the data was uploaded to MONIES, several reports were generated and reconciled to the vendor reports to ensure the accuracy of the data.

We reviewed the reconciliation for the month of January 2007, noting no exception.

No significant exception noted.

Department Description of Control: The Bureau also compiles billing information related to Network bandwidth usage and bills appropriately through MAS90. Regional Technology Centers monitor usage and connectivity in their areas. This usage is reported monthly to Business Services. Once all monthly reports are received, a reconciliation takes place for discrepancies, a download from Remedy into MAS90 takes place. Billings are generated from MAS90 and sent to Network customers.

Tests Performed: Reviewed reconciliation and interviewed staff.

Test Results: Business Services received and uploaded Network data into MAS90 to generate billings. Several reports were generated and reconciled to ensure the upload into MAS90 was complete and accurate.

We reviewed the various reports and the reconciliation for the month of January 2007, noting no exception.

No significant exception noted.

Department Description of Control: The Department's Accounting Division is responsible for pursuing outstanding SSRF and CRF accounts. If an agency persists in not paying delinquent amounts, the Department's Director will send a letter to the Director of the delinquent agency requesting payment.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: The Department processed outstanding accounts in accordance to the Department's Accounts Receivable Policy, Number 06.04.00, dated March 1, 2004.

If an agency was delinquent in its payments, an initial contact was made. If the agency continued to be delinquent after 91 days, a formal letter was to be sent to the agency's Director. In addition, beginning in November, the Department would issue "catch-up" billing to any agency with an outstanding balance from the prior fiscal year.

No significant exception noted.

Department Description of Control: Business Services pursue outstanding Network accounts. Non payment for Network Services results in submission to the IOC offset program through the Department's Accounting Division.

Tests Performed: Interviewed staff.

Test Results: Business Services' Management stated non-payment of Network accounts was usually not a problem. If an agency was delinquent in its payments, the following steps were to be taken:

- 60 days - the agency was called,
- 90 days - a letter was sent to the agency,
- 120 days - a second letter was sent stating service would be disconnected.

If the agency did not make payments, the service would be disconnected, and the account was turned over to the Department's Accounting division.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance the controls, the Department should ensure the annual analysis to comply with the Federal Department of Human Services' requirement is completed on a timely basis.

TECHNICAL STRATEGY - ENTERPRISE ARCHITECTURE AND STRATEGY

CONTROL OBJECTIVE

Management should establish an IT Governance Framework and ensure that IT functions are in alignment with enterprise wide goals.

EXISTING ENVIRONMENT

Background Provided by the Department: The Enterprise Architecture and Strategy (EA&S) group was developed to ensure that IT investment decisions are aligned with EA&S vision and goals and deliver outcomes that keep in step with the accelerating pace of business changes.

Department Description of Control: The Enterprise Architecture and Taxonomy database (Technical Reference Model (TRM)) contains a list of business applications and products (software) used at a statewide, or enterprise, level.

Tests Performed: Reviewed the database.

Test Results: The Department developed the Enterprise Architecture Taxonomy database, which contained a listing of business applications and products which were supported.

No significant exception noted.

Department Description of Control: EA&S utilizes the “Governance” gates 6 and 7 with the approval of the Architecture Review Board to manage the Architectural standards. The major artifacts documenting gates 6 and 7 are: the Technical Reference Model, the Product Standardization Requests and the minutes from the ARB sessions.

Tests Performed: Reviewed process and interviewed staff.

Test Results: The Department established a process to review and approve projects. We reviewed two projects and found general compliance with the process.

No significant exception noted.

OVERALL CONCLUSION

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

TECHNICAL STRATEGY - STRATEGIC PLANNING

CONTROL OBJECTIVE

Management should continually monitor and assess trends, risks, and conditions to ensure the technological infrastructure supports, and will continue to support, the missions and objectives of the department.

EXISTING ENVIRONMENT

Background Information Provided by the Department: The purpose of the Strategic Plan is to identify reprioritized initiatives under a comprehensive framework which integrates with the larger Strategic Plan being developed by the Department.

Department Description of Control: The leadership for the Strategic Plan has joined the State of IL on October 16, 2006. Under the new leadership, the process for the development of the Strategic Plan has been created.

Tests Performed: Interviewed staff.

Test Results: The Acting Deputy Director for the Bureau was originally hired as the Head of Technical Strategy and assigned the responsibility for the creation of the Strategic Plan. The Acting Deputy Director was working with several staff members, and planned to complete the FY08 Strategic Plan by July 1, 2007.

No significant exception noted.

Department Description of Control: The Plan itself is currently under development for a July 1, 2007 issuance.

Tests Performed: Reviewed draft Plan.

Test Results: A draft of the *FY08 Information Technology and Network Strategic Plan* had been developed. The plan was scheduled to be finalized by July 1, 2007.

No significant exception noted.

OVERALL CONCLUSION

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

NETWORK SERVICES

CONTROL OBJECTIVE

Management should ensure an appropriate security structure is established to ensure information assets are adequately protected from unauthorized or accidental disclosure, modification, or destruction.

EXISTING ENVIRONMENT

Background Provided by the Department: The Division of Network Services is currently responsible for management and oversight of the Illinois Century Network (ICN), Local Area Networking (LAN) for selected agencies, the Illinois Wireless Information Network and all engineering responsibilities related to State of Illinois telecommunication services. The Division consists of four teams which includes: Design & Security, Network Operations, LAN Services, and Network Integration (Enterprise Network Support).

Department Description of Control: The Design & Security team is responsible for establishing architectural standards and methodologies for implementing and supporting wide-area and local-area enterprise systems and services. Established standards currently include: POP Site Power Strategy, Basic MPLS Connectivity Model, Common Connection Methodology for LAN, and Quality of Service.

Tests Performed: Reviewed the standards and methodologies.

Test Results: The Department developed several standards and methodologies to assist with the implementation and support of the LAN and WAN infrastructures. The standards and methodologies provided guidance regarding security, redundancy and availability.

No significant exception noted.

Department Description of Control: Design and Security staff design complex network and network service configurations. In addition to this work, staff performs project management and participates in network, network service, and telecommunications related projects.

Tests Performed: Interviewed staff.

Test Results: The Design and Security staff assisted various entities with the implementation of architectural standards and methodologies. During the fiscal year the Design and Security staff were involved in 22 projects.

No significant exception noted.

Department Description of Control: Design and Security staff conducts, coordinates, and serves as lead(s) on feasibility studies and projects involving wide-area network systems.

Tests Performed: Interviewed staff.

Test Results: The Design and Security staff completed or was working on ten feasibility studies.

No significant exception noted.

Department Description of Control: They have developed test procedures for hardware and software and make recommendations based upon test results.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: The Design and Security staff developed and implemented six testing procedures for hardware and software.

No significant exception noted.

Department Description of Control: Design and Security staff perform analysis to determine future bandwidth and capacity needs.

Tests Performed: Interviewed staff.

Test Results: The Design and Security staff used tools to monitor and review bandwidth and capacity needs.

No significant exception noted.

Department Description of Control: Network Operations is responsible for installing, maintaining and managing the ICN Backbone including backbone circuits, egress circuits, routers, firewalls, switches, fifteen Point of Presence (POP) sites, WAN monitoring tools and WAN services.

Tests Performed: Reviewed configurations and interviewed staff.

Test Results: The Backbone network was divided logically into two layers: Core Network and Distribution Network.

We reviewed the electronic configurations of the devices, which contained software revision levels and fully documented high-level rule base descriptions. We reviewed the full configurations of 21 Core Routers, 21 Agency Distribution Routers, and 14 Educational Institution Distribution Routers.

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

Department Description of Control: Network Operations provides tier 3 Network Support to other staff within the bureau.

Tests Performed: Interviewed staff.

Test Results: Network Operations assisted the Customer Management Center and the Field Operations staff with network support.

No significant exception noted.

Department Description of Control: Network Operations staff are responsible for the backbone and POP site management and support. Support includes: delivery, removal and inventory of equipment; installation, maintenance and documentation of all POP site equipment; test and turn-up of all backbone and egress circuits; installation and management of POP sites.

Tests Performed: Reviewed website and interviewed staff.

Test Results: The State was divided into nine Regional Technology Centers (RTCs). The staff at the RTCs were responsible for the maintenance of the POP sites and circuits.

The Network Operations staff developed a checklist to assist in the performance of duties.

No significant exception noted.

Department Description of Control: Network Operations staff are responsible for installing, customizing, maintaining and supporting WAN management and monitoring.

Tests Performed: Reviewed policies, tools and interviewed staff.

Test Results: Network Operations staff developed several policies and tools to assist with the management of the WAN.

No significant exception noted.

Department Description of Control: Network Operations is responsible for WAN Services including DNS, registrar for the il.us domain and filtering.

Tests Performed: Reviewed policies and interviewed staff.

Test Results: Network Operations provided support for the hardware and software comprising WAN Services.

No significant exception noted.

Department Description of Control: WAN services support includes installation, configuration, maintenance and support.

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

Test Results: Network Operations staff developed several policies, procedures, and tools to assist in supporting the WAN.

No significant exception noted.

Department Description of Control: LAN Services is responsible for entering rules into the firewalls and monitoring security violations. The group is responsible for the consolidated agencies (AGR-Agriculture, CEO-Commerce & Economic Opportunity, DNR-Natural Resources, DHS-Human Services, HFS-Healthcare & Family Services, DOT-Transportation, REV-Revenue, CMS-Central Management Services, DES-Employment Security, DPH-Public Health, FPR-Financial & Professional Regulation, EPA-Environmental Protection) LAN networks, which includes: firewalls, routers, switches, hubs and wireless switches.

The LAN Services group is responsible for installation, configuration and support of the Department's LAN networking infrastructure including: switches, routers, hubs, firewalls, IDS, wireless switches and inside cabling.

Tests Performed: Reviewed policies, configuration and interviewed staff.

Test Results: LAN Services provided the LAN network architecture (including firewalls, routers, and switches between the "Access" routers and the servers) for the Department and the consolidated agencies.

We reviewed the electronic configurations of the devices, which contained software revision levels and fully documented high-level rule base descriptions. We reviewed the full configurations for 23 firewalls, 42 routers and 24 switches.

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

Department Description of Control: Enterprise Network Support is responsible for design and support of State Agency network access. Responsibilities include installation and support of access routers, WAN switches, VOIP, video conferencing, fiber, DNS, and Internet.

Tests Performed: Reviewed policies and interviewed staff.

Test Results: Enterprise Network Support developed several policies to assist in the support the State agency networks.

No significant exception noted.

Department Description of Control: Network Integration also performs tier 3 technical support for the CMC and directly to state agencies.

Tests Performed: Interviewed staff.

Test Results: Enterprise Network Support provided technical support to CMC and RTC staff to assist in resolving complex problems.

No significant exception noted.

Department Description of Control: Enterprise Network Support is responsible for providing a variety of services to state agencies. Functions include customer consultation, access and distribution router configuration, ongoing maintenance, head-end router installations/troubleshooting, making equipment and connectivity recommendations, performing equipment installation/recovery at state agency sites in Springfield and surrounding area, and the provisioning for new circuits, moves and changes.

Tests Performed: Reviewed policies and interviewed staff.

Test Results: Enterprise Network Support developed several policies/procedures and tools to assist in providing services to agencies.

No significant exception noted.

Department Description of Control: Enterprise Network Support is responsible for the installation, maintenance, and protection of the CMS MAN fiber Network. Responsibilities include overseeing installation of fiber facilities and outside plant construction projects, fiber plant locating services, and maintenance of accurate fiber records.

Tests Performed: Reviewed policies, configurations and interviewed staff.

Test Results: Routers connected agencies to the Department's Backbone network.

We reviewed the electronic configurations of the devices, which contained software revision levels and fully documented high-level rule base descriptions. We reviewed the full configurations of 77 routers.

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

Change Management

Department Description of Control: Network Operations, LAN Services, Enterprise Network Support, and Design & Security all utilize the CMS Lotus Notes, Change Management system. In doing so, a Request for Change (RFC) is created within Lotus Notes. RFCs are reviewed at the weekly Change Advisory Council (CAC) meeting.

Tests Performed: Reviewed Lotus Notes change requests and interviewed staff.

Test Results: If a change had the potential to have an impact on an agency's connectivity, an RFC was created in Lotus Notes.

No significant exception noted.

Configuration Standards

Department Description of Control: Design & Security has established standard configuration templates for core, distribution, and WAN access equipment.

LAN Services does not currently have a documented standard configuration.

Tests Performed: Reviewed templates and interviewed staff.

Test Results: The Design & Security staff developed several standard configuration templates. However, during our review of the various configurations, the templates were not consistently deployed.

No significant exception noted; however, the standard configuration templates had not been consistently deployed.

Illinois Wireless Information Network (IWIN)

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

Tests Performed: Reviewed policies.

Test Results: The IWIN Policy Manual (Manual), dated December 19, 2005, outlined the responsibilities for: DCMS – IWIN Support Center, Illinois State Police, Local Agency IWIN Coordinators, and IWIN users.

The Manual posted on the Internet had not been updated since December 2005 and did not depict the current environment.

No significant exception noted; however, the Manual had not been updated to depict the current environment.

Department Description of Control: Redundant routers, maintained by CMS, connect the CMS's Premier MDC Servers to the Verizon Network.

Tests Performed: Reviewed configurations and interviewed staff.

Test Results: We reviewed the electronic configurations of the devices, which contained software revision levels and fully documented high-level rule base descriptions. We reviewed the full configurations for two firewalls, which provided network connectivity.

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

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

Tests Performed: Reviewed access rights and interviewed staff.

Test Results: We reviewed Accounts with powerful access rights to determine if the accounts were appropriately assigned and controlled.

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

OVERALL CONCLUSION

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

- Develop and implement formal standards (and associated templates) for configurations.
- Continually review security parameters to ensure security issues are adequately addressed.
- Update the IWIN Policy Manual to reflect the current environment.

BUSINESS ENTERPRISE APPLICATIONS - PERSONAL INFORMATION MANAGEMENT (PIM)

CONTROL OBJECTIVE

Management should ensure an appropriate security structure is established to ensure information assets are adequately protected from unauthorized or accidental disclosure, modification, or destruction.

EXISTING ENVIRONMENT

Department Description of Control: The perimeter is protected with an Anti Spam, Anti Virus and Content Filtering solutions that detect unsolicited email senders, blocks suspect attachments and scans email for inappropriate content and attachment.

Tests Performed: Reviewed Anti Spam, Anti Virus and Content Filtering solutions.

Test Results: The Department utilized a combination of software solutions for perimeter security.

No significant exception noted.

Department Description of Control: The end user email account is secured using an aggressive password scheme. The password policy can be found in the PIM Policies document.

Tests Performed: Reviewed password scheme and policies.

Test Results: An acceptable password scheme had been established. The Department developed a draft version of PIM Policies (Shared Services PIM Standards); however, the Policies had not been approved and finalized.

Although an acceptable password scheme had been established; the corresponding policies had not been finalized.

No significant exception noted.

Department's Description of Control: There are 24/7 support procedures in place.

Tests Performed: Reviewed contact list.

Test Results: The Department developed a contact list to provide assistance to users 24 hours a day.

No significant exception noted.

OVERALL CONCLUSION

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

ENTERPRISE APPLICATIONS - QUALITY ASSURANCE

CONTROL OBJECTIVE

Management should ensure that a suitable structured systems development methodology exists and is utilized to ensure that applications are developed and/or modified in a manner that promotes consistency, integrity, and security to ensure that applications satisfy management's intentions.

EXISTING ENVIRONMENT

The Department's Enterprise Business Application Services (EBAS) was responsible for the development of computer systems (enterprise applications) available for use by the user agencies as well as those systems used by the Department.

Department Description of Control: The EBAS Quality Assurance Section has developed the Application System Development Methodology (Methodology). The Methodology provides a structured process for the analysis and design, development, implementation and post implementation review of new system projects, enhancement projects, maintenance and ad hoc requests.

Tests Performed: Reviewed the Methodology and interviewed staff.

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

The Methodology outlined four system development phases:

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

Management stated the Methodology contained some outdated sections, but was followed as closely as possible.

No significant exception noted.

Department Description of Control: The EBAS Quality Assurance Section has developed the Standards and Documentation Requirements. The Standards and Documentation Requirements provide standards for consistent terminology, available programming tools, security, and storage.

Tests Performed: Reviewed the Standards and Documentation Requirements (Manual) and interviewed staff.

Test Results: The Manual aided in the development and maintenance of applications by providing standards for: consistent terminology, available programming tools, security, and storage.

A Manual existed; however it contained some outdated sections.

No significant exception noted.

Department Description of Control: Emergency Work Requests are to provide a way to deliver applications to the user as soon as possible.

Tests Performed: Reviewed emergency work requests for compliance with Methodology.

Test Results: Emergency Work Requests were exceptions to the sequential processes of the Methodology. The purpose of this exception was to provide a way to deliver applications to the user as soon as possible when Rapid Application Development (RAD) technology could not be used, provide the minimum amount of Methodology paperwork prior to deployment, and complete the remaining Methodology deliverables after deployment.

According to Department Management, the SRRS did not indicate which service requests were classified as an emergency.

No significant exception noted; however, the SRRS did not have a field to indicate if a change was classified as an emergency.

Department Description of Control: RAD projects utilize iterative and prototyping development technologies that can expeditiously provide completed systems to the user.

Tests Performed: Reviewed RAD projects for compliance with Methodology.

Test Results: During the audit period there were no RAD projects.

No significant exception noted.

Department Description of Control: The EBAS Quality Assurance established a Standards Committee to review and approve changes to the Methodology and the Standards and Documentation Requirements.

Tests Performed: Reviewed Standards Committee meeting minutes.

Test Results: From July to December 2006, the Standards Committee met twice.

Although a Standards Committee existed to review and approve changes, we noted several documents contained some outdated information.

No significant exception noted.

Department Description of Control: An email or Service Request document is used to initiate a request for systems development projects.

Tests Performed: Reviewed emails or service requests.

Test Results: We reviewed 30 requests noting each had an email or service request.

No significant exception noted.

Department Description of Control: The Service Request Registration System registers projects, assigns a unique number to the Service Request (SR) and records the status of the project.

Tests Performed: Reviewed Service Requests.

Test Results: The Service Request Registration System (SRRS) registered projects, assigned an SR number and recorded the status of the project.

We reviewed 30 SRs, noting substantial compliance with requirements.

No significant exception noted.

Department Description of Control: In addition to the Service Request Registration System, EBAS utilizes the following tools to assist in tracking projects, assigning resources, and scheduling project time: Microsoft Project, and Quality Assurance (QA) Project Tracking System.

Tests Performed: Reviewed Microsoft Project and the Quality Assurance Project Tracking System.

Test Results: During our review, we noted QA utilized Microsoft Project for the management of three projects.

In addition, EBAS utilized the QA Project Tracking System to monitor the status of projects. The QA Project Tracking System was able to provide various management reports:

- Status of projects that have not completed Phase I, II, and III,
- Overdue Post Implementation,
- Projects Open,
- Projects without corresponding checklists, and
- Checklists without Service Requests.

No significant exception noted.

Department Description of Control: The EBAS's Methodology documents user involvement in all four project phases.

Tests Performed: Reviewed user involvement.

Test Results: The Department required the project teams to work closely with user groups when developing a new application. The Methodology states: “User involvement is vital for system development to be successful. They will participate in each phase of system development. Users will assist with defining the business rules and designing the system. Users are responsible for developing and executing system tests according to the business rules.”

Users were required to be involved in each phase of the development. Additionally, users must sign off at the close of each phase.

No significant exception noted.

Department Description of Control: The Quality Assurance Unit monitors and verifies that projects adhere to the Methodology. The QA Review Procedural Manual provides guidance to Quality Assurance staff for each phase of the project. In addition to the Manual, Quality Assurance utilizes a checklist system to identify required tasks for each project.

Tests Performed: Reviewed QA Review Procedural Manual (Manual) and reviewed projects for compliance with Methodology.

Test Results: QA was responsible for monitoring projects that were either enhancements or new developments for compliance with the Methodology. The Manual outlined each phase of the Methodology and the required deliverables. Additionally, QA developed a checklist, which listed all required deliverables by phase.

During our review, the Department completed two enhancement projects, which were required to be completed in accordance with the Methodology. We reviewed the ASD Methodology Development Checklist, noting QA had signed-off as reviewing the required deliverables.

No significant exception noted.

Department Description of Control: The security software management is done through the use of the security software support application.

Tests Performed: Reviewed security software management.

Test Results: Security software management was done through the use of the security software support application.

No significant exception noted.

Department Description of Control: The Mainframe Security Procedures Technical Manual is the technical reference guide used for security software management.

Tests Performed: Reviewed the Mainframe Security Procedures Technical Manual.

Test Results: The Department developed the Mainframe Security Procedures Technical Manual, dated August 2006. The Manual addressed the following:

- Setting up IDs, groups, datasets, tapes, and transaction profiles,
- Process on how to complete a request form,
- Resetting passwords,
- Processing transaction dump requests,
- Inactive Accounts,
- Processing Separation Reports,
- Processing Separation Notifications,
- Security Processing,
- IDs managed by a local coordinator,
- Processing Violations, and
- Reports.

No significant exception noted.

Department Description of Control: Current personnel act as the administrative coordinator for DB2 security access. This function is done through the use of a “DB2 Coordinator ID”.

Tests Performed: Interviewed staff.

Test Results: According to Department management, the individual assigned to DB2 administration retired December 2006 and the responsibilities had not been reassigned.

Although the DB2 Coordinator ID existed; responsibilities to administer security had not been formally reassigned.

No significant exception noted.

Department Description of Control: The submission of all system gen forms for IMS databases to the Data Center is part of the responsibility that has been passed to Quality Assurance Unit.

Tests Performed: Reviewed system gen forms.

Test Results: There were no system gen forms, which were required to be completed, during the audit period.

No significant exception noted.

Department Description of Control: The Unit is also responsible for IMS system backups. These backups are done daily, weekly and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.

Tests Performed: Interviewed staff.

Test Results: Management stated the Enterprise Application Group was responsible for the backup of IMS. IMS system backups were conducted the same time as the Enterprise Application back ups are conducted.

No significant exception noted.

Department Description of Control: The Program Library Procedures provide guidance for ensuring new programs or modified programs are documented and approved before production moves are performed.

Tests Performed: Reviewed Program Library Procedures.

Test Results: The Department developed the Program Library Procedures, dated May 2005. The Procedures outlined the process for submitting a request and the approval process for moving jobs into production.

In addition, we reviewed staff with access to production libraries, noting they appeared appropriate.

No significant exception noted.

Department Description of Control: A Library Control Form must be completed and approved before any move is made.

Tests Performed: Reviewed Library Control Forms.

Test Results: We reviewed 11 program moves, noting each had a completed and approved Library Control Form.

No significant exception noted.

OVERALL CONCLUSION

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

- Ensure the Standards Committee routinely and continually meets to review standards, policies, procedures, and guidelines to ensure they adequately address control requirements and reflect current practices.
- Update the SRRS to document service requests that were classified as an emergency.
- Formally reassign DB2 security and administration responsibilities.

BCCS – EBAS – WORKFLOW

CONTROL OBJECTIVE

Management should ensure a suitable structured systems development methodology exists and is utilized to ensure applications are developed and/or modified in a manner which promotes consistency, integrity, and security and to ensure applications satisfy management's intentions.

EXISTING ENVIRONMENT

Background Information Provided by the Department: The responsibilities of Workflow include the development and support of ITSM (Information Technology Service Management) and customized workflow-based applications. These applications are LAN, client server and web-based.

Department Description of Control: The Workflow section follows the EBAS standards and methodology maintained by the EBAS Quality Control unit. Requests for new development, enhancements, maintenance, and ad hoc reports are tracked on the Service Request Registration System (SRRS).

Tests Performed: Reviewed new developments, enhancements, maintenance and ad hoc requests for compliance with the EBAS standards and methodology and reviewed SRRS.

Test Results: The Workflow section was responsible for the following applications:

- Enterprise Service Desk,
- Enterprise Change Management/Service Request,
- PC Lease Management,
- Illinois Procurement Bulletin,
- Enhanced AMBER Alert System,
- Procurement Business Case, and
- BCCS Provisioning.

The Workflow section was also responsible for Lotus Notes and the Remedy platforms.

We reviewed six service requests relating to the various applications, for compliance with the EBAS methodology, noting no exceptions. In addition, the six service requests were documented in the SRRS.

During our testing of the six service requests, we noted the programmer who completed the service request also moved the change into production for three of the requests. However, we did note, the service requests were independently approved before the move to production.

The EBAS standards and methodology were followed for changes to applications; however, the duties of the programmer were not segregated from production control.

Department Description of Control: NOTES has its internal security and REMEDY uses both its internal security and a Secure Socket Level (SSL) control that is managed by the server when required.

Tests Performed: Reviewed appropriateness of individuals with administrative access.

Test Results: Five individuals had administrative access to Remedy and Notes. The individuals were responsible for technical support of the applications and the access rights appeared to be appropriate.

No significant exception noted.

Department Description of Control: The Workflow unit uses a system called Production Authorization Release System (PARS) to review and release work completed on a system. Each (PARS) ticket contains a developer's checklist for task completed listing the changes/enhancements and the tested changes/enhancements. When the developer is ready, a section is provided for Peer Review. The last section for release is the move to production section that provides both the BUM and Section Manager approval for the Proposed Move Date/Time.

Tests Performed: Reviewed PARS tickets.

Test Results: The Department had a documented process for the utilization of PARS tickets.

During the audit period, there were nine PARS tickets completed. We reviewed each PARS ticket for the developer's checklist, Peer Review, BUM, and Section Manager approvals, noting no exceptions.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance the controls, the Department should ensure an adequate segregation of duties exists between programming and moves to production.

SERVICE MANAGEMENT

CONTROL OBJECTIVE

Management should establish a project administration framework for all projects to reduce the risk of unexpected costs, project cancellations, and to ensure the value and quality of project deliverables.

EXISTING ENVIRONMENT

Background Information Provided by the Department: The Service Management unit “conducts project administration for the Enterprise Business Application Services’ (EBAS) processes as directed by the EBAS Executive.”

Department Description of Control: The software utilities used in this unit to produce and handle the reports and documents include SharePoint, Microsoft Project, Excel, Word, and Visio.

Tests Performed: Interviewed staff.

Test Results: Management stated Service Management was a newly formed unit with detailed operational procedures not yet fully documented. Management also stated the software utilities identified in the Department’s Description of Control are not currently used; they are the utilities planned for future use by Service Management.

Project administration policies and procedures had not been developed to provide guidance to staff. In addition, reports or documents had not been developed to support Service Management’s project administration activities.

OVERALL CONCLUSION

Service Management had not implemented a formal process to ensure staff consistently and effectively administer projects. To enhance the current process, the Department should develop formal policies, procedures, and guidelines to provide clear and consistent guidance to staff.

WEB SERVICES AND LAN APPLICATION DEVELOPMENT

CONTROL OBJECTIVE

Management should ensure that a suitable structured systems development methodology exists and is utilized to ensure that web services and LAN applications are developed and/or modified in a manner that promotes consistency, integrity, and security and to ensure that applications satisfy management's intentions.

EXISTING ENVIRONMENT

Background Information Provided by the Department: The Web Services / LAN Application Development Section provide different types of services: LAN Application Development, Web Services, and Enterprise Content Management.

Background Information Provided by the Department: The responsibilities of this section include the development of custom application software on microcomputers, local area networks (LANs), Internet, Intranet and mainframe client server environments.

Department Description of Control: In addition to standard executable application development, many of the projects are designed and implemented using, but not limited to, Access, Access/SQL, Oracle, SQL, Visual Studio technologies and Fleet Anywhere (a third party application).

Tests Performed: Reviewed documentation and interviewed staff.

Test Results: The Department utilized various tools in the design and implementation of projects.

No significant exception noted.

Department Description of Control: The LAN Application Development Section provides ongoing support to end-users of microcomputer workstations in the utilization of packaged and custom developed software.

Tests Performed: Reviewed documentation and interviewed staff.

Test Results: If a problem would arise, the user would contact the Bureau's Help Desk for assistance. The Help Desk would complete a problem ticket and assign it to LAN Application Development staff. If an issue would requires a change in code, the EBAS Methodology would be utilized and the change would be documented in the SRRS database.

There were no completed problem tickets during the audit period.

No significant exception noted.

Department Description of Control: The section follows the set standards and methodology for rapid application development maintained by the EBAS Quality Assurance Section. For projects that are classified as enhancements or new development, QA requires a checklist of deliverables to be created and delivered. Prior to being placed into production, all updates and modifications are reviewed and approved by the owner. Once approval is obtained, the developer requests to their supervisor to move the changes into production.

Tests Performed: Reviewed developments and enhancements for compliance with the EBAS Methodology and checklists, and interviewed staff.

Test Results: LAN Application Development completed one new development during the audit period. Management stated the application owner required an expedited implementation prior to the completion of all requirements outlined in the EBAS Methodology. The application was moved into production on December 15, 2006 and the Department was in the process of completing all required documentation.

Although the EBAS Methodology was used to guide development projects, all required steps were not completed prior to implementation.

No significant exception noted.

Department Description of Control: Tracking the status of requests is performed using a local Access database and/or the Service Request Registration System (SRRS).

Tests Performed: Reviewed Access Database, SRRS, and interviewed staff.

Test Results: LAN Application Development utilized the SRRS, while Web Content Management utilized the Access Database to track requests.

We reviewed the SRRS and the Access Database, noting requests were being tracked.

No significant exception noted.

Background Information Provided by the Department: The Web Services section supports static and dynamic web sites and the domain name server. The Bureau provides web services that enable more than thirty state agencies to communicate their specific and broadly related information to both public and private sectors.

Department Description of Control: The Web Services Section supports (which includes creation, implementation, and on-going update and maintenance) both static and dynamic web sites.

Tests Performed: Reviewed procedures.

Test Results: The Department developed the Web Content Change Policy, not dated. The Policy outlined the process a request was to follow.

No significant exception noted.

Department Description of Control: Both existing and leading edge development tools are used for web development.

Tests Performed: Reviewed tools and interviewed staff.

Test Results: The Department utilized various tools for web development.

The Department did not complete any major web development projects during the audit period.

No significant exception noted.

Department Description of Control: Websites maintained by Web Services all utilize the Official State Web Templates developed and administered by Web Services, and comply with the Illinois Web Accessibility Standards (IWAS), which are based on the Federal “Section 508” and World Wide Web Consortium accessibility guidelines

Tests Performed: Reviewed compliance with IWAS standards and interviewed staff.

Test Results: Web developers were instructed to code in compliance with the IWAS standards and use software to test pages for accessibility. In addition, prior to the implementation of a website, the Illinois Office of Communication and Information – Web Content Services would perform a usability and accessibility review.

The Department did not complete any major web development projects during the audit period.

No significant exception noted.

Department Description of Control: Prior to being placed into production, all updates and modifications are reviewed and approved by the owner. Once approval is obtained, the developer requests their supervisor to move the changes into production.

Tests Performed: Reviewed web content changes for approvals.

Test Results: The Web Content Change Policy required owners to review, test, and approve changes before the developer requested a supervisor move the changes into production.

There were no major web developments during the audit period; however, we reviewed ten web content changes, noting one did not have owner approval documented.

No significant exception noted.

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

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: The Department did not have a formal policy in place for the administration of DNS' and URL's. However, the following process was followed: Users completed the applicable form, signed it, and sent it to the Department. The request was reviewed and if it fit the Illinois.gov framework, it was approved.

No significant exception noted.

Department Description of Control: Enterprise Content Management provides the capabilities to scan, import, store, secure, index, retrieve and route document-based information. Security is managed by the Content Management administrator. The customer's business requirements identify the level and type of security assigned.

The Content Management section is responsible for setting up and maintaining the content management tool and creating an environment for each user as per their needs.

With indepth analysis and prior to being placed into production, all updates and modifications are reviewed and approved by the owner. Once approval is obtained, the developer requests to their supervisor to move the changes into production.

Still in development, the full functionality of Content Management is not in place.

Tests Performed: Interviewed staff.

Test Results: As outlined in the Department's Description of Control, Content Management controls had not been fully implemented.

OVERALL CONCLUSION

Based on the test results described above, the LAN Application and Web Services controls were operating with sufficient effectiveness to achieve the control objective.

The Enterprise Content Management Section had not implemented a formal process to ensure all staff were efficiently and effectively meeting its goals and objectives. To enhance the current process, the Department should develop formal policies, procedures, and guidelines to provide clear and consistent guidance for the Enterprise Content Management Section.

Additionally, in order to enhance the controls, the Department should:

- Complete LAN Application developments in accordance with the EBAS Methodology.
- Complete Web content changes in accordance with the Web Content Change Policy.

END USER COMPUTING

CONTROL OBJECTIVE

Management should ensure procedures exist to register, track, and address all user queries.

EXISTING ENVIRONMENT

Background Information Provided by the Department: The EUC division of the Bureau provides personal computer and printer support to all state employees and contractors associated with the agencies consolidated under the Governor, and Legacy Central Management Supported Non-Consolidated Agencies. Responsibilities of EUC include Break/Fix Support, the Enterprise Service Request Process and major IT Rationalization projects. These responsibilities support major projects within the State of Illinois IT Rationalization initiative and daily technical support of the State's daily business.

Department Description of Control: The service desk receives a call from a user regarding a technical problem; a break/fix ticket is created within the Bureau Remedy system, and then assigned to the EUC section that supports the identified user. EUC technical staff receives the ticket, acts in the appropriate method to fix the problem, and upon completion of the task resolves the break/fix ticket within the Enterprise Remedy system.

Tests Performed: Reviewed service desk tickets.

Test Results: The EUC was assigned 3,355 service tickets for the period of July 16, 2006 through May 18, 2007, of which 523 had not been resolved. The average resolution time for a service ticket was 24.17 hours.

No significant exception noted.

Department Description of Control: The change ticket which is generated by Remedy is then assigned to the EUC supervisor or their assigned representative who in turn creates multiple tasks for multi part projects and assigns them to the appropriate EUC technician. In the case of a one step project the change ticket is assigned to the appropriate technician who then creates one task, accomplished the task/ESR request and then resolves the task.

Tests Performed: Reviewed ESR tickets.

Test Results: The EUC was assigned 960 ESR tickets for the period of July 1, 2006 through May 18, 2007, of which 56 had not been resolved. The average resolution time for an ESR ticket was 4 days, 2 hours and 44 minutes.

No significant exception noted.

Department Description of Control: Standard operating processes are in place; however, no formalized policies exist.

Tests Performed: Reviewed operating procedures and interviewed staff.

Test Results: The EUC maintained a Sharepoint site with procedures, checklists, customer approval documentation, and a customer satisfaction survey. However, upon review of the documents, we noted several were still in draft form or incomplete.

Standard operating procedures had been established; however, formalized policies and procedures did not exist.

No significant exception noted.

Department Description of Control: There are processes in place to receive sign offs from the receiving users for the equipment once the deployment is complete.

Tests Performed: Reviewed sign-offs and interviewed staff.

Test Results: Documentation to support the requirement for a sign-off from users receiving equipment did not exist.

No significant exception noted; however, the Department did not maintain documentation to support user approvals for all deployments.

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 develop formal policies and procedures and receive and maintain documentation to support user approvals for all deployments.

VENDOR MANAGEMENT

CONTROL OBJECTIVE

Management should ensure effective and efficient management of and compliance with vendor agreements with regard to infrastructure products and services.

EXISTING ENVIRONMENT

Background Information Provided by the Department: The Vendor Management Team is responsible for ensuring effective and efficient management of and compliance with vendor agreements with regard to infrastructure products and services. Specific functions in support of these responsibilities include: Contract Management, Procurement Management, and Budget Management.

Department Description of Control: Monitor/Report on Contract Expiration/Renewals.

Tests Performed: Reviewed the monitoring/reporting system.

Test Results: A Vendor Management database had been created to record maintenance renewals, beginning with fiscal year 2007. The database documents the beginning and ending date for maintenance renewals and, where necessary, products within contracts. However, the database had not been completely populated and will not be verified until the end of fiscal year 2007.

Formal policies, procedures, and guidelines had not been developed to guide monitoring and reporting activities.

Although a database to help monitor and report on contracts existed, the database had not been fully populated and policies, procedures, and guidelines to provide clear and consistent guidance to staff had not been developed.

Department Description of Control: Invoice Approval Processing.

Tests Performed: Reviewed the Invoice Approval Processing procedure and tested for compliance.

Test Results: The Department developed the Invoice Processing procedure, dated February 8, 2007. The procedure provided a standard process for receipt, tracking, approval, and payment of invoices.

We reviewed 28 invoices for proper approval, noting all had been properly approved.

No significant exception noted.

Department Description of Control: Direct administration of enterprise critical agreements.

Tests Performed: Reviewed administration of enterprise critical agreements.

Test Results: The Department had not developed policies and procedures for administering enterprise critical agreements.

Policies, procedures, and guidelines to provide clear and consistent guidance to staff had not been developed.

Department Description of Control: Creation/Review of Purchase Requests and Procurement Status Tracking/Reporting.

Tests Performed: Reviewed purchase requests and tracking/reporting of purchase requests.

Test Results: The Department developed policies and procedures for reviewing and tracking/reporting of purchase requests.

The Department developed the following policies and procedures for procurement status tracking/reporting:

- Procurement Process-IFB Procurements,
- Procurement Process-RFP Procurements,
- Procurement Process-Small Procurements,
- Procurement Process-Sole Source Procurements, and
- Procurement Process-Purchase Request.

No significant exception noted.

Department Description of Control: Software/License Receipt/Tracking and Software Library Administration.

Tests Performed: Reviewed the Software Library Administration process and reviewed the Software License Tracking database.

Test Results: The Department had not developed policies and procedures over the Software Licensing Administration.

The Department used a database to track contract information and software licenses. The database indicated the product and number of licenses purchased; the database did not indicate the number of licenses actually utilized.

In addition, the Department did not have policies or procedures in place to review software licenses to ensure compliance with contracts.

Although a database to help track software licenses existed, it did not contain information on software utilization. In addition, policies, procedures, and guidelines to provide clear and consistent guidance to staff had not been developed.

Department Description of Control: Expenditure Tracking/Reporting.

Tests Performed: Reviewed the expenditure tracking/reporting process.

Test Results: The Department developed the Budget Procedure, dated January 31, 2007, which provided guidance for the budget process.

No significant exception noted.

OVERALL CONCLUSION

Vendor Management had not implemented a formal process to ensure all staff were efficiently and effectively meeting its goals and objectives. To enhance the current process, the Department should develop formal policies, procedures, and guidelines to provide clear and consistent guidance to staff.

Specifically, we recommend the Department:

- Ensure the Vendor Management Database is updated to reflect the complete population of agreements.
- Track the utilization of software licenses under its jurisdiction to ensure utilization is within the terms of the licensing agreements.

ENTERPRISE PRODUCTION OPERATIONS SERVICES

CONTROL OBJECTIVE

Management should develop and organize the scheduling of jobs, processes and tasks into the most efficient sequence, maximizing throughput and utilization to meet business requirements, and establish appropriate physical safeguards over special-purpose printers.

EXISTING ENVIRONMENT

Background Information Provided by the Department: The general duties of the Input/Output (I/O) section are two fold: the Input side monitors all production jobs processing on the mainframe to ensure the jobs come to successful completion. The Output side of the section is responsible for printing and distribution of all documents and reports generated as a result of the successful processing of the jobs.

During our review, we found the Department's I/O Control and the Department of Human Service's (DHS) I/O Control were merged as a result of the IT consolidation. Additionally, in December 2006, the Department's I/O Control was physically consolidated with DHS at the Harris facility. During this transition period, DHS processes are following DHS legacy policies and procedures. Additionally, all remaining processes follow the Department's policies and procedures.

Department Description of Control: The Input side monitors all production jobs processing on the mainframe to ensure that the jobs come to successful completion. The Output side of the section is responsible for printing and distribution of all documents and reports generated as a result of the successful processing of the job. Written procedures are in place which are available to authorized personnel.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: The Department developed the CCF I/O Operations Guide, dated by section. The Guide provided procedures for the Command Center, Tape Library and I/O Control.

During our review of the Guide, we noted it made references to employees who are no longer employed, and had not been updated to reflect the merger and consolidation with DHS.

No significant exception noted; however, the Guide did not reflect the current environment and controls.

Department Description of Control: If staff are unable to affect the proper repairs there is a call list available for each job that processes.

Tests Performed: Reviewed call list and interviewed staff.

Test Results: According to I/O Management, in the event of a problem staff would place a call to the individual indicated on the call list.

No significant exception noted.

Department Description of Control: Any new or changed job or system that is presented for acceptance into the production environment must first pass through the Production Control area. The documentation is checked for adherence to standards, naming conventions and run procedures. All jobs that are processed in the production environment, whether they run through CA-Scheduler or are manually submitted, must be setup and processed by Production Control.

Tests Performed: Reviewed documentation and interviewed staff.

Test Results: There were two different processes in place over Production Control.

Department jobs were managed and controlled by the responsible divisions. Management stated they were in the process of reassigning the responsibility for Department jobs to DHS Production Control.

DHS jobs were managed and controlled by DHS Production Control.

No significant exception noted; however, the Department had not merged its production control responsibilities to DHS Production Control.

Department Description of Control: Any time a job abnormally terminates and it is due to a cart problem or a problem with how the job was setup for processing, the people responsible for the job in the production control correct the problem and restart the job. Written procedures are in place, which are available to authorized personnel.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: The Department developed the CCF I/O Operations Guide. The Guide outlined various procedures to assist staff with corrections of problems. Our review of the Guide indicated it did not reflect the current process, due to the merger and physical consolidation with DHS Production Control.

No significant exception noted; however, the Guide did not reflect the current environment and controls.

Department Description of Control: The majority of the output from jobs processed for the Department of Human Services pass through the Mobius Automated distribution and on-line viewing system. Written procedures are in place which are available for authorized personnel.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: The Department had not developed procedures for automated distribution.

The Mobius application allowed agencies on-line viewing capabilities and printing capabilities. Access to the on-line view feature and printing of reports was controlled with RACF security software. In order to obtain access, an individual would send Production Control an email stating what access was needed.

No significant exception noted.

Department Description of Control: All areas within the Harris Computer Facility (HCF) have proximity readers and you must have a badge with the proper accesses in order to enter. Special brightly colored badges with very limited accesses are available for use by individuals entering the building to pick up printed output from the I/O Control area. These badges will only open the first set of double doors leading into the first floor.

Tests Performed: Reviewed physical security and interviewed staff.

Test Results: The Department of Human Services was responsible for the security of the Harris facility.

The Department of Human Services Administrative had a Directive - 01.01.02.210 Physical Safeguards – Building Access Controls. The Directive stated:

- All guests must sign in and be escorted by DHS staff or DHS contractor to their destination;
- Security guards, where assigned, shall be on duty 24 hours a day to guarantee that only authorized personnel enter the DHS building; and
- All guests and DHS employees must display a temporary/visitor or DHS employee identification (ID) badge.

In our review of physical security at the Harris Facility, we noted that several security features were implemented, including the use of security guards and card-key security to restrict access.

Although security controls existed at the Harris Facility, some weaknesses with the implementation of these controls were identified in the June 30, 2005 Compliance Examination of the Department of Human Services (finding 05-3).

Department Description of Control: Individuals must identify themselves and say what reports they are there to pick up. The individual is then looked up on the “Focal” system, which contains a list of individuals that are authorized to pick up reports from I/O Control. They then must sign the report manifest indicating they received the correct reports.

Tests Performed: Reviewed pick-up logs and observed controls.

Test Results: Staff members of the I/O Control area utilized Focal, a database, to check and verify if individuals picking up reports were authorized.

No significant exception noted.

OVERALL CONCLUSION

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

- Develop standardized I/O policies and procedures that accurately reflect the current environment and controls.
- Review physical security at the Harris Facility and ensure security controls meet Department standards.

ENTERPRISE CAPACITY PERFORMANCE AND STORAGE (ECPS) - MAINFRAME ENVIRONMENT

CONTROL OBJECTIVE

Management should monitor and review performance and capacity of IT resources to ensure backup and restoration of systems is adequate.

EXISTING ENVIRONMENT

Department Description of Control: Offsite vaulting is in place for backups.

Tests Performed: Reviewed backups maintained at the CCF and at the off-site storage location.

Test Results: We reviewed the list of backup tapes and identified daily, weekly, and monthly backup tapes. We selected 90 backup tapes from the list and located all the tapes at the CCF or Regional Vault.

No significant exception noted.

Department Description of Control: z/OS BACKUPS: backups are performed on the mainframes systems data. System data is backed up daily and weekly with the weekly copies sent to the regional vault on a 4 week cycle. Backups are also performed by HSM. These backups are controlled by the SMS routines and are set by the user at allocation time.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: Daily and weekly backups were maintained; daily backups remained on site, while the weekly backups were rotated to the Regional Vault.

No significant exception noted.

Department Description of Control: Restores are processed after an INFO management ticket is opened. Procedures are documented on the shared network drive for resource management.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: The Department's Data Processing (DP) Guide provided guidance for the restoration of mainframe backups. The DP Guide stated an INFOMAN ticket is to be completed for each restore conducted.

During the audit period, one restore was completed. We reviewed the related INFOMAN ticket, noting no exceptions.

No significant exception noted.

OVERALL CONCLUSION

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

MAINFRAME – SYSTEMS PROGRAMMING – z/OS

CONTROL OBJECTIVE

Management should ensure an appropriate security structure is established to ensure information assets and resources are adequately protected from unauthorized or accidental disclosure, modification, or destruction.

EXISTING ENVIRONMENT

Background Provided by the Department: The primary operating system at the Department's Central Computer Facility is Zero Downtime Operating System (z/OS). z/OS is a complex operating system used on mainframes and functions as the system software that controls the initiation and processing of work within the computer.

Department Description of Control: The System Management Facility (SMF) records the activity within the operating system.

Tests Performed: Interviewed staff and reviewed system and security reports.

Test Results: The System Management Facility recorded activities within the operating system.

No significant exception noted.

Department Description of Control: The agency RACF administrator must submit a request to the CMS RACF staff if a user ID needs to have TSO access on the mainframe.

Tests Performed: Reviewed email notifications and confirmation by Department staff.

Test Results: Authorized user-agency representatives would send an electronic mail message to RACF staff to request TSO access.

No significant exception noted.

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

Tests Performed: Interviewed staff, reviewed security profiles, reviewed system configurations using specialized software, and reviewed system options.

Test Results: Security software and system options were implemented to secure libraries, and protect resources and data.

No significant exception noted.

OVERALL CONCLUSION

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

MAINFRAME – SYSTEMS PROGRAMMING – z/VM

CONTROL OBJECTIVE

Management should ensure that operating systems are configured and controlled to promote security and integrity.

EXISTING ENVIRONMENT

Background Information Provided by the Department: The Department's secondary operating system utilized at the Central Computer Facility is Virtual Machine (VM). VM is time-sharing, interactive, multi-programming operating system for IBM mainframes. The major subsystem that is supported in VM is NOMAD.

Department Description of Control: The agency RACF administrator must request and obtain a VM User ID from the z/VM staff.

Tests Performed: Confirmation by Department staff.

Test Results: Authorized user agency representatives would send an electronic mail message to VM staff to request a VM User ID.

No significant exception noted.

Department Description of Control: Agencies are assigned user IDs with the most restrictive security rights.

Tests Performed: Reviewed security reports and confirmation by Department staff.

Test Results: z/VM user IDs were assigned the most restrictive access rights. Only VM staff and service machines had less restrictive access rights.

No significant exception noted.

Department Description of Control: The VM directory is restricted, which contains information regarding user IDs, mini-disk size and location, and operating functions.

Tests Performed: Reviewed security reports and confirmation by Department staff.

Test Results: Access to the VM directory was limited to VM staff. System options and parameters were implemented to protect data and resources.

No significant exception noted.

OVERALL CONCLUSION

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

MAINFRAME – SYSTEMS PROGRAMMING – SECURITY

CONTROL OBJECTIVE

Management should ensure that an appropriate security software structure is established to ensure that information assets and resources are adequately protected from unauthorized or accidental disclosure, modification, or destruction.

EXISTING ENVIRONMENT

Department Description of Control: The Department utilizes security software to control access and protect resources. The security software is the primary tool for controlling and monitoring access to the Department's computer resources.

Tests Performed: Reviewed literature, reviewed security software reports, and confirmation by Department staff.

Test Results: A security software package, Resource Access Control Facility (RACF), was used to control and monitor access to Department resources.

No significant exception noted.

Department Description of Control: A user ID is used to identify the client along with a password to verify the client's identity.

Tests Performed: Reviewed literature, reviewed security software reports, and confirmation by Department staff.

Test Results: User IDs were used to identify a user's identity as a key control mechanism within RACF. The security software protected access and enforced user accountability over data and system resources by positively verifying the user's authority to utilize that data or system resource, and by logging the user's actions.

No significant exception noted.

Department Description of Control: The Department maintains a log of all access attempts, which is used to monitor unauthorized access attempts and identify areas of weakness. The Department has a procedure in place for the monitoring of security violations. The agency RACF administrators have the capability of producing the reports for their agency.

Tests Performed: Reviewed literature, reviewed security software reports, and confirmation by Department staff.

Test Results: Each user agency had access to the RACF violation report so they could view any access violations for their agency. Department staff periodically generated violation reports to

review and follow-up on issues. System options were set to log commands and IDs with powerful attributes.

No significant exception noted.

Department Description of Control: Clients are responsible for protecting their program and data files.

Tests Performed: Reviewed security software reports and confirmation by Department staff.

Test Results: User agencies were responsible for specifying the datasets to be protected and for properly using the available security resources.

No significant exception noted.

Department Description of Control: The Department has appointed staff with primary responsibility for the implementation and administration of the security software.

Tests Performed: Reviewed security software reports and confirmation by Department staff.

Test Results: The Department assigned staff members with the primary responsibility to implement and administer security software. The access rights were appropriately assigned to these staff members.

No significant exception noted. However, we did note an excessive number of revoked IDs on the system.

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

Tests Performed: Reviewed mainframe security procedures and reviewed security software reports and associated options and parameters.

Test Results: The Department had a formal Mainframe Security Procedures Manual which was updated as of August 2006. System options and parameters were implemented to protect data and resources.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance the controls, the Department should work with user agencies decrease the number of unused (revoked) IDs.

MAINFRAME – DATABASE MANAGEMENT – DB2

CONTROL OBJECTIVE

Management should ensure that DB2 security features and other controls are utilized to protect information assets and resources from unauthorized or accidental disclosure, modification, or destruction.

EXISTING ENVIRONMENT

Background Information Provided by the Department: Database 2 (DB2) is a relational database management system for z/OS environments, which the Department makes available to user agencies. The Department has established ten+ subsystems at the Central Computer Facility.

Department Description of Control: The Department has assigned staff to monitor the performance and problems of DB2.

Tests Performed: Interviewed staff.

Test Results: The Database Administration Group consisted of two lead staff responsible for DB2 performance monitoring and database design. One lead acted as the Department's liaison for user agencies, and maintained a list of agency assigned DB2 Coordinators. The other lead had overall responsibility over DB2 Distributed Environments.

No significant exception noted.

Department Description of Control: The DB2 staff is also responsible for software installation, maintenance and security.

Tests Performed: Interviewed staff.

Test Results: The DB2 Software Support Group was responsible for providing software installation, maintenance and security.

No significant exception noted.

Department Description of Control: All users who access DB2 are required to have a security software ID and password. The user must authenticate to the security software first. If the user authenticates, DB2 allows access.

Tests Performed: Reviewed security reports and interviewed staff.

Test Results: DB2 was integrated with RACF security software. Users must have a valid RACF ID and password before they can gain access to DB2 resources.

No significant exception noted.

Department Description of Control: DB2 internal security verifies access rights to specific data.

Tests Performed: Reviewed security reports and interviewed staff.

Test Results: DB2 authorization catalog tables were used to grant certain access privileges and were created during the DB2 installation. These tables describe such things as table spaces, tables, columns, indexes, privileges, plan authorizations, application plans, and packages. There was a unique set of tables for each DB2 subsystem. We reviewed the DB2 authorization tables and found the DB2 high level administrative privileges appeared to be properly restricted.

No significant exception noted.

Department Description of Control: The Department authorizes one user ID at each agency to coordinate the use of DB2 within the agency. This user ID allows each agency to create its own authority.

Tests Performed: Reviewed Agency DB2 Coordinator Listing and interviewed staff.

Test Results: Each user agency was required to assign a DB2 Coordinator for their agency, who in turn was responsible for assuring access privileges were adequately controlled within the user agency.

No significant exception noted.

Department Description of Control: The DB2 Software Support Group will monitor specific application problems when users call.

Tests Performed: Interviewed staff.

Test Results: When a user requested assistance, the DB2 Software Support Group monitored the application and reviewed the database design.

No significant exception noted.

Department Description of Control: System performance is monitored on a continuous basis.

Tests Performed: Interviewed staff.

Test Results: Department staff used tools to monitor system performance.

No significant exception noted.

Department Description of Control: The Department's Information Management System is utilized to report and document problems.

Tests Performed: Interviewed staff.

Test Results: The Department used INFOMAN, in addition to weekly status reports and email to report and document problems to DB2 staff.

No significant exception noted.

OVERALL CONCLUSION

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

MAINFRAME – DATABASE MANAGEMENT – CICS

CONTROL OBJECTIVE

Management should establish policies and procedures, and ensure that security features of CICS are utilized to protect information assets and other resources from unauthorized or accidental disclosure, modification, or destruction.

EXISTING ENVIRONMENT

Background Information Provided by the Department: The Customer Information Control System (CICS) is a software product that enables online transaction processing. CICS allows numerous transaction types, entered from multiple terminals, to be processed concurrently by user written application programs. CICS acts as an interface between the operating system and application programs.

Department Description of Control: The Department offers three different levels of CICS support for users, described as follows:

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

Tests Performed: Interviewed staff.

Test Results: Department staff stated there had been no changes in level of support provided to the CICS user agencies in the past year. The Department offered three different levels of CICS support for user agencies, Level One, Level Two, and Level Three.

No significant exception noted.

Department Description of Control: Production regions are segregated from test and development regions to restrict access, based upon the various needs for each type of region. Test regions have fewer access restrictions and allow programmers to test and debug against non-production files.

Tests Performed: Reviewed region listings and interviewed staff.

Test Results: The production CICS regions were separated from the test and development/training CICS regions. Non-production regions (test, development, training CICS

regions) had fewer access restrictions to allow programmers to develop and test CICS applications.

No significant exception noted.

Department Description of Control: Restricted access to sensitive CICS transactions is established over production regions.

Tests Performed: Reviewed security reports, general resource classification listings, and interviewed staff.

Test Results: Restricted access to sensitive CICS transactions was established over production regions.

No significant exception noted.

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

Tests Performed: Reviewed security software reports and interviewed staff.

Test Results: System options and parameters were implemented to protect data and resources.

No significant exception noted.

OVERALL CONCLUSION

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

MAINFRAME – DATABASE MANAGEMENT – IMS

CONTROL OBJECTIVE

Management should ensure that IMS security features and other controls are utilized to protect information assets and resources from unauthorized or accidental disclosure, modification, or destruction.

EXISTING ENVIRONMENT

Background Information Provided by the Department: Information Management System (IMS), which is an online database software subsystem, used as the control architecture under which online database system applications process. An IMS system is capable of running many different applications within a single definition of one or more “Message Processing Region” and one “Control Region”. The IMS applications can access IMS, DB2 and CICS data files.

Department Description of Control: RACF security is used for access to datasets and IMS transactions.

Tests Performed: Interviewed staff and reviewed access screens.

Test Results: IMS was integrated with RACF security software. Most users were required to have a valid RACF ID and password before they could gain access to IMS resources. In some specific cases, terminal security (transactions were limited to a specific terminal) was utilized instead of RACF.

No significant exception noted.

Department Description of Control: Users control their own TIMS and GIMS RACF definitions.

Tests Performed: Interviewed staff.

Test Results: User agency RACF Coordinators were responsible for permitting RACF access to agency specific IMS resources.

No significant exception noted.

Department Description of Control: Currently, there are three production IMS regions with 10+ testing regions.

Tests Performed: Interviewed staff and reviewed region listing.

Test Results: There were three primary production regions and over 10 testing regions.

No significant exception noted.

OVERALL CONCLUSION

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

INFRASTRUCTURE SERVICES – CCF TAPE LIBRARY

CONTROL OBJECTIVE

Management should maintain an inventory of onsite and offsite media and ensure their usability and integrity.

EXISTING ENVIRONMENT

Department Description of Control: Tape Librarians are responsible for confirming that individuals are authorized to deliver or remove media.

Tests Performed: Reviewed individuals authorized to request media.

Test Results: A Media Authorization list was maintained to control the delivery or removal of media.

We selected 15 check-in and 15 check-out Media Transmittal Forms from January 16, 2007 to ensure individuals that requested media were authorized. All 30 forms in the sample referenced authorized individuals from the Media Authorization list.

No significant exception noted.

Department Description of Control: A security officer and a Tape Librarian must verify that the triplicate media transmittal forms are correct, signed, and retain a copy.

Tests Performed: Reviewed the process and tested transmittal forms for compliance.

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

We selected 30 transmittal forms for January 16, 2007, noting all forms were properly authorized. However, one form did not contain the date and another form did not include the name of the requestor.

No significant exception noted; however, two transmittal forms were not properly completed.

Department Description of Control: All media is identified with unique tracking alphanumeric identification numbers.

Tests Performed: Reviewed media for identification numbers.

Test Results: Tape media had a unique tracking identification number for identification.

We reviewed 62 media tapes, noting all were identified with unique tracking identification numbers.

No significant exception noted.

Department Description of Control: The Tape Management System (TMS) is utilized to track and record the location of media.

Tests Performed: Reviewed the process and tested for compliance.

Test Results: Tape media was tracked utilizing the Tape Management System.

We selected a sample of 30 tapes and found all 30 tapes were identified in the Tape Management System and in the proper location.

No significant exception noted.

Department Description of Control: Carts not listed in TMS are transient carts recorded in database called the Transient Tape System (TTS).

Tests Performed: Reviewed the TTS database.

Test Results: Transient tapes (carts or cartridges) were tracked utilizing the Transient Tape System.

We selected a sample of 32 transient tapes and found that 30 of 32 were documented in the TTS. Management immediately took corrective action to document the other 2 transient tapes.

No significant exception noted; however, transient tapes were not always properly documented in the TTS database.

Department Description of Control: The "Library Services Vault Transmittal Procedures" outline the procedures to be conducted during the movement of media.

Tests Performed: Reviewed the Library Services Vault Transmittal Procedures.

Test Results: The Department had procedures in place to control the movement of tape media.

No significant exception noted.

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

Tests Performed: Reviewed security over media.

Test Results: According to management, policies or procedures to require the encryption of confidential or personal information on tape media had not been developed. However, some tape media included a security code to protect against unauthorized access.

Policies or procedures to require the encryption of confidential or personal information on tape media had not been developed.

OVERALL CONCLUSION

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

- Ensure all transmittal forms are properly completed.
- Ensure transient tapes are properly documented in the TTS.

In addition, the Department should conduct an assessment to determine if confidential information (for example, personal information, as defined by the Personal Information Act (815 ILCS 530)), is potentially subject to unauthorized disclosure on backup media. To prevent the disclosure of confidential or personal information maintained on transportable media, the Department should utilize encryption.

INFRASTRUCTURE QUALITY ASSURANCE AND METHODS

CONTROL OBJECTIVE

Management should establish a project administration framework for all Infrastructure projects to reduce the risk of unexpected costs, project cancellations, and to ensure the value and quality of project deliverables.

EXISTING ENVIRONMENT

Background Information Provided by the Department: The Infrastructure Quality Assurance and Methods (IQAM) organizes, plans and controls work activities for the Infrastructure Services Division as directed by the Infrastructure Manager.

As outlined below, IQAM began its responsibilities in January 2007; thus, our review was limited to a review of policies, procedures, and guidelines.

Department Description of Control: Infrastructure Administration includes reviewing Pending Gate 3 charters, functional and non-functional requirements, gathering and organizing detail design activities, tracking and documenting issues and action items, status reporting, documenting work processes and coordinating activities between client agencies and the Department.

Tests Performed: Reviewed IQAM policies and interviewed staff.

Test Results: According to IQAM management, IQAM began their responsibilities on January 17, 2007.

The following policies were developed to guide IQAM staff activities:

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

No significant exception noted; however, since IQAM had only been in effect since January 17, 2007, compliance with the policies was not tested.

Department Description of Control: IQAM organizes and coordinates technical resource and service support to ensure availability of Category 1 agency business applications.

Tests Performed: Interviewed staff and reviewed documentation.

Test Results: We reviewed various agendas and meeting minutes that documented IQAM activities to coordinate availability of business applications.

No significant exception noted.

Department Description of Control: IQAM works with EPMO staff to understand direction and priorities of the Bureau. We also work with EPMO to validate correct process is being followed according to Governance.

Tests Performed: Interviewed staff and reviewed documentation.

Test Results: IQAM staff attended weekly EPMO charter review meetings to gain an understanding of the directions and priorities of the Bureau.

No significant exception noted.

Department Description of Control: The tool we currently use to gather detailed design documentation is the Project Assessment Requirements (PAR) form.

Tests Performed: Reviewed PAR forms.

Test Results: A PAR form had been developed to gather detailed design documentation.

No significant exception noted; however, since IQAM had only been in effect since January 17, 2007, no PAR forms had been completed.

OVERALL CONCLUSION

Based on the test results described above, the framework to support the IQAM objectives appeared to be established.

INFRASTRUCTURE SERVICES – DATA CENTER OPERATIONS

CONTROL OBJECTIVE

Management should ensure that the operations environment encourages the realization of the agency's missions and goals and that appropriate policies and procedures have been developed to protect information assets as well as ensuring that problems and incidents are resolved and the cause investigated to prevent reoccurrence.

EXISTING ENVIRONMENT

Background Information Provided by the Department: The Command Center is the Systems Operation Center component of the Bureau's Enterprise Production Operations Services organization. The mission of the Command Center is to provide continuous monitoring and operation of the Bureau's computing resources to ensure availability, performance, and support response necessary to sustain customer business demands.

Department Description of Control: The Command Center operates twenty-four hours a day, seven days a week, 365 days a year.

Tests Performed: Reviewed time sheets.

Test Results: The Command Center operated twenty-four hours a day, seven days a week.

No significant exception noted.

Department Description of Control: The Command Center maintains availability and functionality of computing resources as scheduled in support of customer business needs and coordinates and oversees implementation of changes to the computing environment.

Tests Performed: Reviewed process for coordination of changes.

Test Results: The Command Center Supervisor chaired the weekly INFOMAN change management meetings. At the meeting the upcoming weekend changes were discussed.

When the Command Center was responsible for the implementation of a change, it was scheduled and monitored. If a problem occurred, the Command Center contacted the appropriate individual for assistance.

No significant exception noted.

Department Description of Control: The Bureau maintains several reports that record the Command Center activities. The following reports provide a complete record of all operator actions: SYSLOG, Shift Change Checklist and the Daily Shift Report.

Tests Performed: Reviewed the SYSLOG (system generated log), Shift Change Checklist, and the Daily Shift Report.

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

The Shift Change Checklists were utilized to aid in reviewing the status of the various operating systems and applications. Checklists also aid in determining if there are problems with systems or applications.

We reviewed the Shift Change Checklist for the first week of October 2006, noting 55 checklists had been completed. Of the 55 checklists, we found 12 that were either not properly completed or did not have evidence of supervisory review.

The purpose of the Daily Shift Report was to record all activities which had occurred (downtimes, person contacted, action take, etc.).

We reviewed the Daily Shift Reports for the month of October 2006, noting each date had a report.

Additionally, we reviewed 25 problems noted on the Daily Shift Reports for corresponding INFOMAN problem ticket, noting each had a problem ticket.

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

Department Description of Control: In addition, the Bureau utilizes INFOMAN, a management tool, to record and monitor the progress of problem resolutions.

Tests Performed: Reviewed INFOMAN problem tickets for resolution time.

Test Results: INFOMAN provided notification and escalation of unresolved problems or scheduled changes, which had not been designated as resolved or completed.

We reviewed 25 problems in INFOMAN, noting one was resolved in 12 days, one was resolved in 7 days, and the remaining 23 problems were resolved in 3 days or less. In addition, of the 25 problems reviewed, none were considered significant.

No significant exception noted.

Department Description of Control: The Bureau collects, reviews, and analyzes operating statistics to identify trends, detect problems, and project future resources through the Availability Report, which reflects the system and application availability on a daily and weekly basis.

Tests Performed: Reviewed the Availability Report.

Test Results: During our review, we noted the Command Center was not responsible for the Availability Report, the Quality Assurance (QA) and Methods division was responsible.

The Department developed the Availability Reporting (Mainframe) Data Collection and Validation Process document, not dated, which outlined the process for the collection of data and the creation of the Availability Report.

We reviewed the Availability Reports from July 9, 2006 to December 31, 2006, noting all downtime noted was scheduled downtime.

During our review, we noted the Availability Report did not reflect application availability, only system availability.

In addition, the Availability Report had not been used to identify trends, detect problems, and project future resources.

No significant exception noted; however, the Availability Report did not include application availability and had not been used to identify trends, detect problems, and project future resources.

Department Description of Control: The Bureau collects, reviews, and analyzes operating statistics to identify trends, detect problems, and project future resources through the Resource Management Facility Report, which reflects CPU utilization by system and machine, as well as the average and maximum number of users at any one time.

Tests Performed: Reviewed the Resource Management Facility (RMF) report and procedures.

Test Results: During our review, we noted the Command Center was not responsible for this report; the Enterprise Capacity and Performance Storage division was responsible.

The Department developed the Daily RMF Procedures, dated February 15, 2006, which outlined the process for the collection of data and the creation of the Resource Management Facility Report.

No significant exception noted.

Department Description of Control: The Bureau collects, reviews, and analyzes operating statistics to identify trends, detect problems, and project future resources through the D-Collect Report, which reflects space, allocated space versus space used.

Tests Performed: Reviewed the D-Collect Report and procedures.

Test Results: During our review, we noted the Command Center was not responsible for this report; the Enterprise Capacity and Performance Storage division was responsible.

The Department developed the Monthly DASD Billing Procedures, not dated, which outlined the process for the collection of data and the creation of the D-Collect Report.

In addition, we noted the D-Collect report was not utilized to identify trends, detect problems or project future resources.

No significant exception noted; however, the D-Collect report had not been used to identify trends, detect problems, and project future resources.

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

Tests Performed: Reviewed the Data Processing (DP) Guide.

Test Results: The DP Guide, which was dated by section, provided guidelines for the various command center activities.

No significant exception noted.

Tests Performed: Reviewed system performance tools.

Test Results: The Command Center utilized two system performance tools: Tivoli and Focal Point, to monitor the Department's environment.

No significant exception noted.

OVERALL CONCLUSION

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

- Ensure all Shift Change Checklists are properly completed and contain evidence of supervisor approval.
- Review and assess the various reports and logs in order to analyze resources, identify trends, detect problems, and project future resources.

RISK MANAGEMENT - RECOVERY SERVICES

CONTROL OBJECTIVE

Management should ensure that procedures have been developed and tested to protect critical information resources, minimize the risk of unplanned interruptions, and ensure the availability of critical information resources within acceptable timeframes.

EXISTING ENVIRONMENT

Public Act 93-25 (20 ILCS 405/405-410) authorized the Department of Central Management Services (Department) to consolidate Information Technology (IT) functions of State government. The IT Rationalization project was initiated to centralize IT functions for select agencies under the umbrella of the Department.

The following agencies are participating in the consolidation project:

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

After the consolidation, there were 44 Category One applications included in the Statewide Critical Application Listing that run on the Department's computer systems. Category One applications are those considered critical that impact the lives and safety of Illinois citizens.

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

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

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

There were no satellite locations that meet the Department's recovery needs. The Department had a contract to provide recovery services at an out-of-state location for mainframe services and limited midrange services.

A satellite location to provide local recovery services or a location for complete recovery of midrange services did not exist.

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

- Continuity Methodology,
- Recovery Activation Plan,
- Network Services, Recovery Activation Plan.

Tests Performed: Reviewed plans and interviewed staff.

Test Results: The Department developed the Continuity Methodology (Methodology) and the Recovery Activation Plan (Plan), both dated March 29, 2007.

The Methodology and the Plan provided high-level guidance in the event the Department's Central Computing Facility is deemed inoperable. The Methodology and the Plan both referenced documents for the detail recovery of the Department's mainframe operating system.

However, the responsibility for the development and implementation of application recovery plans rests with the owner (user agency).

Department Management stated the Network Services, Recovery Activation Plan had not been developed. Thus, a recovery plan to address the midrange environment did not exist.

After the IT consolidation, the Department became responsible for the midrange infrastructure of 28 Category One applications.

The Continuity Methodology and Recovery Activation Plan existed; however, Network Services, Recovery Activation Plan for the midrange environment did not exist.

Department Description of Control: The Bureau purchases exercise time annually to conduct a comprehensive recovery exercise at the vendor provided recovery location.

Tests Performed: Reviewed testing documentation and interviewed staff

Test Results: In July 2006, the Department conducted its annual Statewide Comprehensive Recovery Exercise at the disaster recovery service provider's site. During this exercise, 16 of the 44 Category One applications were tested.

Sixteen of the 44 Category One applications that run on the Department's computer systems were included in the July 2006 test.

Department Description of Control: The Bureau maintains a Statewide Critical Application Listing based on information received from State agencies.

Tests Performed: Reviewed critical application listing.

Test Results: The Department maintained a Statewide Critical Application Listing based on information received from agencies. In the event a disaster would occur, only those applications listed in the Statewide Recovery File which have been tested would be considered for recovery.

In order for an agency to be placed on the Statewide Critical Application Listing, the agency must evaluate their applications and annually provide the Department with a summary of the application's importance to the State and society.

The Statewide Critical Application Listing indicated 53 Category One application, which requires them be given recovery priority. Forty-four of the Category One applications run on the Department's computer systems.

No significant exception noted.

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

Tests Performed: Reviewed testing documentation and interviewed staff.

Test Results: We reviewed testing documentation to determine if State Agency Category One applications met the Department's recovery requirements. We found multiple instances where Category One applications were not adequately tested. In addition, it appeared many recovery plans supporting these Category One applications were outdated.

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

Department's Description of Control: The Department utilizes a regional off-site storage facility for storage of critical information.

Tests Performed: Reviewed off-site storage facility.

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

During our tour of the off-site facility we reviewed the contents of the disaster recovery boxes and noted several documents were outdated or in draft form.

Although a regional off-site storage facility existed, some of the recovery documentation was outdated.

Department Description of Control: The Bureau has developed scripts and/or procedures for the recovery of operating system platforms.

Tests Performed: Reviewed scripts/procedures.

Test Results: The Department developed the Disaster Recovery Cookbook, which provided recovery procedures for the Department's mainframe operating system. In addition, the Department developed the Data Processing Guide to assist in the recovery of the mainframe environment.

The Department had not developed recovery procedures for the Department's midrange environment.

Procedures existed to promote the recovery of mainframe operating systems; however, procedures to promote the recovery of midrange operating systems had not been developed.

OVERALL CONCLUSION

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

The Department had not implemented and tested procedures to protect critical information resources, minimize the risk of unplanned interruptions, and ensure the availability of critical information resources within acceptable timeframes. In particular, plans and procedures to recover the midrange environment had not been adequately addressed.

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

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

PHYSICAL SECURITY - BCCS

CONTROL OBJECTIVE

Management should ensure that appropriate physical security controls are established to protect the information systems hardware and other assets.

EXISTING ENVIRONMENT

Department Description of Control: The Department utilizes an access card system to provide control over access to many of its facilities. The system controls and logs the use of access cards at the Central Computer Facility (CCF), Communications Building, the Benefits Building, and the Business Services Building.

Tests Performed: Reviewed facilities.

Test Results: The Central Computer Facility, Communications Building, the Benefits Building, and the Business Services Building were secured by an access card (badge) system. In addition, the CCF and Communications Building had security guards on-site 24 hours a day.

No significant exception noted.

Department Description of Control: For the above facilities, all employees, visitors, vendors/contractors, and State agency representatives are required to be assigned an access card with appropriate access privileges. Requests for access cards are submitted to the Risk Management (RM) division for activation. Individual access privileges are based on job duties. The RM division houses an issuance document outlining how to control the adding and modifying of credentials in the system.

Tests Performed: Reviewed process for requests, requests, appropriateness of access rights, and interviewed staff.

Test Results: An access card was required to enter the facilities.

To obtain an access card for an employee or contractor, the following process was outlined in the issuance document. Upon notification from the Department's Personnel Liaison, the Risk Management division forwards a request to the appropriate authorized individual to obtain authorization for the individual's access rights.

The Department had not developed a formal policy and did not routinely document approval of the access rights. We reviewed 20 employee/contractor requests, noting documentation of the approval was not maintained. Department management stated approvals come in the form of emails or phone calls and were not documented.

Although a process existed to assign access cards, a formal policy had not been developed. In addition, documentation supporting the approval of access rights was not maintained.

Department Description of Control: Visitors and employees who forget their access card are required to sign-in and register at the guard's desk.

Tests performed: Reviewed the building admittance registers and interviewed staff.

Test Results: Any individual without an authorized access card was required to sign the Building Admittance Register to gain admittance.

We reviewed the Building Admittance Register for the Communications Building and the Central Computer Facility for a two month period, noting the Register was generally completed.

No significant exception noted.

Department Description of Control: The H/V system is pre-populated with certain data fields to serve as a control when entering new data.

Tests Performed: Interviewed staff.

Test Results: When the Risk Management division received a request, a record was created in the access card (H/V) system. The record was reviewed and updated when the individual appeared for the creation of their access card.

No significant exception noted.

Department Description of Control: Other critical controls are employee pass-back and the establishment of absentee limits, which are in use at (and between) the CCF, CCC, and Benefits Building.

Tests Performed: Interviewed staff and auditor observation.

Test Results: The Department set an absentee limit in the access card system to deactivate an access card after a predefined period of inactivity. In addition, the Department implemented pass-back technology to prevent individuals from following ("piggy backing") others into the facility.

We verified the absentee limit in the access card system, and observed the pass-back technology in place at the CCF and Communications Building.

No significant exception noted.

Department Description of Control: The system also produces routine access listings to display who has access to which doors and door groups, so management can determine if the list is accurate.

Tests Performed: Reviewed appropriateness of individual access rights and interviewed staff.

Test Results: Department Management stated detailed reviews of access rights were conducted of the CCF and the Business Services Building during the audit period. In addition, a review of the access rights to the Network Services area in the Communications Building was also conducted during the audit period.

Additionally, over the last year, the Department migrated to a different type of access card. As a result, anyone who did not receive a new card, no longer has access rights to the facilities.

We reviewed 37 employee's access rights to the Central Computer Facility, noting no exceptions.

No significant exception noted.

Department Description of Control: The badges are FIPS 201-1 compliant and contain the proper test to outline cardholder responsibilities as well as instructions on what to do if a lost badge is found by someone other than the owner.

Tests Performed: Reviewed access cards and interviewed staff.

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

- Photo of the individual,
- Name,
- Anti-counterfeit feature, and
- Issue and expiration date.

The access cards also provided instructions for the postage free return to the Department if lost and found.

No significant exception noted.

Department Description of Control: It is also CMS policy to recover employee badges upon employee termination/separation.

Tests Performed: Reviewed policy and interviewed staff.

Test Results: According to the DCMS Policy Manual, Chapter 2, Section 13, dated September 1, 1998, "all state owned items are to be returned to the State when an employee separates service with the Department." Additionally, "the Supervisors are responsible for collecting a separated employee's telephone credit card, door and desk keys, parking lot stickers, data center admittance cards...."

Risk Management staff stated access rights are terminated upon receiving the access card. Once the access card is received by the Risk Management division, the rights are terminated and the individuals file is deleted.

We reviewed 37 separated individuals noting one individual had not been deleted from the system. However, upon notification, the Department removed the access rights.

No significant exception noted.

Department Description of Control: Non-personal badge credentials are inventoried 3 times per day to ensure no CMS credentials are in the wild.

Tests Performed: Reviewed inventory registers and interviewed staff.

Test Results: At the start of each shift of the security guards, the temporary badge inventory is to be completed to ensure all badges are accounted for.

We reviewed the temporary badge inventory sheet for the CCF and the Communications Building for the period of July through December 2006, noting three shifts during this period did not complete an inventory sheet.

No significant exception noted; however, the temporary badge inventory sheet was not completed for three shifts.

Department Description of Control: Tape-based backups for the H/V system are done on a periodic basis, but they are currently not stored in an offsite location.

Tests Performed: Interviewed staff.

Test Results: Risk Management staff stated the access card (H/V) system is backed up daily and maintained on-site.

No significant exception noted; however, backups were maintained on-site.

Department Description of Control: Video surveillance cameras are located on the exterior of CMS facilities, as well as strategic locations within the interior.

Tests Performed: Reviewed the location of video surveillance camera.

Test Results: The Department maintained camera within and on the exterior of the CCF, Communications Building, and the Business Services Building. The security guards had the ability to monitor the cameras at all times.

No significant exception noted.

OVERALL CONCLUSION

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

- Develop formal policies to administer access card rights.
- Document the approval of access card rights.
- Maintain a copy of the backup of the access card system at an off-site location.

RISK MANAGEMENT – TECHNICAL SAFEGUARDS

CONTROL OBJECTIVE

Management should ensure that an appropriate security structure is established to make certain that information assets and resources are adequately protected from unauthorized or accidental disclosure, modification, or destruction.

EXISTING ENVIRONMENT

Background Provided by the Department: The Technical Safeguards Unit (TSU) conducts vulnerability scans to evaluate network components for vulnerabilities using plans, procedures and specific tools.

Department's Description of Control: During the vulnerability scans, the team conducts security assessments to determine if baseline standards for servers (and desktops as appropriate) are being implemented. The assessments include confirming that patches have been applied in a timely manner and validating that password best practices are in use.

Tests Performed: Reviewed Security Analysis Reports and interviewed staff.

Test Results: The TSU conducted five detailed vulnerability scans of the Department's environment during the audit period.

No significant exception noted.

Department's Description of Control: The team also performs external penetration testing of the relocated servers to identify vulnerabilities, focusing on the servers, infrastructure, and underlying software to complete a comprehensive analysis of the environment. Vulnerabilities within the environment are then identified, enumerated, and the implications assessed. Mitigation strategies are created and forwarded to the appropriate Bureau team for remedial action.

Tests Performed: Reviewed Security Analysis Reports and interviewed staff.

Test Results: The TSU performed five external penetration tests of the Department's environment.

Upon completion of the testing, the TSU completed a Security Analysis Report which detailed the specific server tested, test conducted, and the outcome. The Security Analysis Report was forwarded to the Infrastructure Services-WinTel group for remediation. It is the responsibility of the WinTel group to develop a remediation plan and open the applicable change and/or help desk tickets. No follow-up was conducted to determine if the remediation plan was completed and implemented.

No significant exception noted.

Department's Description of Control: Under direction of the Risk Management Executive, the team participates in the development and assemblage of computerized material for use in any investigations, litigations, or other informational requests initiated by State Agency Management, Illinois Inspector General, Illinois State Police, Illinois Attorney General or other law enforcement entities.

Test Performed: Interviewed staff.

Test Results: The TSU worked with federal and state enforcement agencies to support investigations. The TSU utilized a variety of tools to assist in the investigations.

No significant exception noted.

OVERALL CONCLUSION

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

CHANGE MANAGEMENT – MAINFRAME ENVIRONMENT

CONTROL OBJECTIVE

Management should ensure an appropriate structure is established to ensure changes to system software and/or application software are sufficiently controlled to confirm only tested and authorized changes are executed.

EXISTING ENVIRONMENT

The change management process in the mainframe environment continues to follow the historical practices associated with INFOMAN.

Department Description of Control: INFOMAN is limited to mainframe changes, incidents and notifications.

Tests Performed: Reviewed policies, change requests, and interviewed staff.

Test Results: The Information Management System Policy (Policy), revised December 2004, provided a step-by-step guide on how to enter a problem ticket or a change request into INFOMAN. The Policy contained the “Change Process Flow Schematic,” section which outlined the process for change requests.

We reviewed 29 INFOMAN change requests and found general compliance with the Policy. The change requests complied with all aspects of the Policy, with the exception of documentation of testing. Of the 29 INFOMAN change requests, 23 required testing. We reviewed the testing documentation, noting seven requests did not have detailed testing documentation. Department staff stated appropriate testing was conducted; however, the staff responsible for testing documentation did not always retain it.

No significant exception noted; however, documentation supporting testing was not always maintained.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should ensure that testing documentation is developed and retained.

ADMINISTRATIVE SAFEGUARDS

CONTROL OBJECTIVE

Management should ensure that an appropriate security structure is established to make certain that information assets and resources are adequately protected from unauthorized or accidental disclosure, modification, or destruction.

EXISTING ENVIRONMENT

Department Description of Control: The Policy Review Board (PRB) was formally established in October 2006 with the signing of the Charter by CMS executive management, and accompanying bylaws and policy submittal instructions clarify the processes.

Tests Performed: Reviewed PRB Charter and bylaws.

Test Results: The Department established a Policy Review Board, which reviewed and approved policies and procedures for the Department.

The PRB Charter, dated October 2006, states the mission of the PRB as:
“The CMS/BCCS Policy Review Board coordinates the development, review, approval, publishing, and maintenance of policies, procedures, and standards related to information technology and telecommunication assets and services. Scope is limited to IT and telecom assets and service for which CMS/BCCS has management authority and operational responsibility.”

The PRB bylaws, dated November 11, 2006, outlined the roles and responsibilities of the PRB board members and non-board members.

No significant exception noted.

Department Description of Control: The PRB Sharepoint site serves to track and monitor PRB activity.

Tests Performed: Reviewed Sharepoint site.

Test Results: The PRB Sharepoint site tracked and monitored the PRB’s activity.

No significant exception noted.

Department Description of Control: An Access database has been developed to accommodate policy issuance tracking.

Tests Performed: Interviewed staff.

Test Results: An Access database had been developed to track policy issuance.

No significant exception noted.

Department Description of Control: The following IT security policies/procedures have been approved:

- Shared Services Standard Glossary
- IT Security Policy
- Use Policy
- IT Users Procedures
- Standard of Relevant Laws and Regulations
- Data Classification Standard
- Availability Policy

Tests Performed: Reviewed policies and interviewed staff.

Test Results: The preceding IT security policies/procedures were approved by the PRB on December 22, 2006. However, the new IT security policies/procedures had not been implemented or disseminated.

Although new IT security policies/procedures were approved in December 2006; they had not been implemented.

Department Description of Control: Until the PRB publishes new policies, the following IT security policies remain in effect:

- Department Policy Manual (each section is dated);
 - Information Technology Security Policy (dated April 26, 2002) included as Chapter 4, Section 3 of the Department Policy Manual
- Statewide Internet Security Policy (dated December 11, 2001)
- Information Security Policy - Local Area Network (LAN)/Office Automation (OA) (dated May 26, 1995)
- Statewide Information Security Policy BCCS/CCF Internal (dated February 4, 2003)
- Office Automation Coordinators Manual (dated February 2003)

Tests Performed: Reviewed policies.

Test Results: The current IT security policies posted on the Department's Intranet site had not been updated since at least February 2003.

The IT security policies that were in effect did not reflect the current technological environment or address current security concerns.

Department Description of Control: This unit recommends system development guidelines to help ensure the security of information, which is processed, stored, maintained, or transmitted on computing systems managed by the Bureau Enterprise Business Applications Systems (EBAS)

team. The Illinois Office of Internal Audit (IOIA) and the EBAS team have been furnished with the Risk Management Minimum Security Controls for Applications Development Systems document.

Tests Performed: Interviewed staff.

Test Results: The “Application Development Security, Minimum Security Controls” were provided to the EBAS and IOIA teams as guidelines for system developments.

No significant exception noted.

Department Description of Control: The unit also serves as Bureau liaison to the Department Chief Operating Officer (COO) in the ongoing development of the Department Continuity of Operations Plan (COOP). The work is mapped against a checklist provided by the CMS Chief Operations Officer (COO) staff in charge of the COOP.

Tests Performed: Interviewed staff.

Test Results: Administrative Safeguard’s staff assisted with the development of the Department-wide COOP plan.

No significant exception noted.

OVERALL CONCLUSION

Although new IT security policies/procedures were approved in December 2006; they had not been implemented or disseminated.

The Department has the primary responsibility for providing IT services to State Government. Thus, it is imperative the Department implement a framework to promote and apply prudent, comprehensive, and effective security practices. The Department should thoroughly review and update security policies to address the current technological environment, consolidation issues, and present-day risks. If the IT security policies/procedures approved by the PRB on December 22, 2006 are suitable, then the policies/procedures should be implemented, formally communicated, and disseminated to all appropriate parties.

CUSTOMER AND ACCOUNT MANAGEMENT

CONTROL OBJECTIVE

Management should ensure procedures exist to register, track, and address all user queries.

EXISTING ENVIRONMENT

Background Provided by the Department: Field Operations, within the Bureau's Customer and Account Management unit, consists of a decentralized staff operating out of nine statewide Regional Technology Center (RTC) offices.

The CMC is the 24/7 network support center for the State of Illinois. The CMC supports the backbone and customer access circuits for all legacy ICN customers such as the educational community, which includes K-12 schools as well as libraries, museums, hospitals and other non-for-profit organizations. The CMC also supports consolidated agencies, the multiple boards and commissions, and non-consolidated agencies.

The CSC is responsible for providing Tier 1 support for Telecommunications and IT services. The CSC IT Service Desk is responsible for providing Tier 1 IT technical and end user support to the consolidated agencies as well as the multiple boards, commissions, and non-consolidated agencies.

The Telecommunications Service Desk is comprised of four units; Help Desk, Provisioning, Consulting and Procurement, and Quality Assurance.

Department Description of Control: Field Operations utilize two versions of Remedy for constituent connectivity provisioning. Agency provisioning is via a Bureau version of Remedy, where all other constituent and non-agency records, provisioning and trouble ticketing is via ICN Remedy.

Tests Performed: Reviewed Remedy systems and interviewed staff.

Test Results: Field Operations received tickets for work to be completed, which were opened by the CMC or the CSC. Field Operations staff were responsible for updating the ticket after the work was completed.

We reviewed 25 ICN Remedy tickets and 21 Bureau Remedy tickets, noting no exceptions.

No significant exception noted.

Department Description of Control: Tools used to complete tasks include the following:

- Solar Winds and What's Up monitor constituent connections and local services.
- Solar Winds and MRTG monitor bandwidth utilization for internal and constituent access.

Tests Performed: Reviewed the various tools and interviewed staff.

Test Results: The Department utilized Solar Winds, What's Up, and MRTG for monitoring system problems.

No significant exception noted.

Department Description of Control: Illinois.net (www.illinois.net) is used to house all non-agency forms and information distributed to constituents, announcements of new services, conferences and policy meetings, costs and bandwidth allocations, instructions on how to access services, and historical data about the network and associated committees. Any customer information is housed at <http://www.cms.il.gov/telecom/default.htm>.

Tests Performed: Reviewed websites and interviewed staff.

Test Results: The Department maintained various types of information on the Illinois.net website, such as the type and pricing of services.

The cms.il.gov/telecom website was the website for the Customer Solution Center. This website provided the various forms utilized by the agencies for services, along with contact information.

No significant exception noted.

Department Description of Control: The CMC staff provides status to our customer on an hourly basis, and escalates if required, to our vendors until an issue is resolved (service restored). Upon every escalation, our CMC staff updates the end-user or affected party of status.

Tests Performed: Reviewed escalation procedures and interviewed staff.

Test Results: The Department developed several escalation procedures for Department staff and the vendors. The procedures outlined the escalation process, which is dependent on the priority of the problem.

Department staff were required to contact the vendor and the customer on an hourly basis, and record each contact.

No significant exception noted.

Department Description of Control: All of this is captured and documented via ticketing tools.

Tests Performed: Reviewed ICN Remedy tickets.

Test Results: We reviewed 25 ICN Remedy tickets, noting no exceptions.

No significant exception noted.

Department Description of Control: The Help Desk currently uses multiple systems to record incidents (VOTS, MONIES and Bureau Remedy).

Tests Performed: Reviewed VOTS, MONIES, and Remedy tickets and interviewed staff.

Test Results: VOTS was used to record all voice incidents. We reviewed 25 VOTS tickets, noting no exceptions.

MONIES was used to record non-ICN data incidents. We reviewed 25 MONIES tickets, noting no exceptions.

Bureau Remedy was used to record wireless incidents. We reviewed 21 Remedy tickets, noting no exceptions.

No significant exception noted.

Department Description of Control: Procedures exist for the Help Desk task.

Tests Performed: Reviewed procedures.

Test Results: The Department developed several methods and procedures (M&P) in order to provide guidance to staff. We reviewed a sample of the M&Ps noting the VOTS and MONIES procedures did not reflect the current process.

No significant exception noted; however, the VOTS and MONIES M&Ps had not been updated to reflect the current process.

Department Description of Control: All telecommunications changes require a request form. Different forms are required for different services.

Tests Performed: Reviewed telecommunication change requests and interviewed staff.

Test Results: The Telecommunications Data/Intercity Service Request (TDR) form was to be completed for data requests. We reviewed ten TDRs, noting four were incomplete.

The Telecommunications Service Request (TSR) form was to be completed for voice and cellular requests. We reviewed ten TSRs, noting all ten were incomplete.

The Paging Service Request (PSR) form was to be completed for paging service requests. We reviewed nine PSRs, noting seven were incomplete.

The Wireless Service Request (WSR) form was to be completed for IWIN requests. We reviewed ten WSRs, noting four were incomplete.

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

Department Description of Control: The Coordinator Access database is maintained by the CSC Administration staff and an alternate.

Tests Performed: Reviewed database.

Test Results: The Department maintained a database which documented each agency's telecommunication coordinator's contact information.

No significant exception noted.

Department Description of Control: The coordinators can locate the instructions for completing these forms on the Telecom Website (www.state.il.us/cms/telecom) and are provided guidance by the Provisioning staff when necessary.

Tests Performed: Reviewed website.

Test Results: The Department developed the Telecom website, which provided the various telecommunication change request forms and instructions. Additionally, the website provided contact information for user agencies.

No significant exception noted.

Department Description of Control: Procedures exist for the Provisioning task.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: The Department developed several M&Ps to assist with specific problems/tasks performed by staff.

We reviewed a sample of the M&Ps noting some procedures did not reflect the current process.

No significant exception noted; however, the Provisioning M&Ps had not been updated to reflect the current process.

Department Description of Control: The MONIES system tracks ordered and installed facilities and telecommunications equipment. Anytime an inventoried piece of equipment is installed, removed or moves from one location to another, an order is entered into the MONIES system to update the system inventory.

Tests Performed: Reviewed telecommunication change requests and interviewed staff.

Test Results: In order to track the various telecommunication change requests, staff enter the requests into MONIES. Additionally, the agency telecommunication coordinators have access to MONIES, which allows them to track their agency requests.

We reviewed the corresponding MONIES tickets for each TDR, TSR, PSR and WSR we tested, noting no exception.

No significant exception noted.

Department Description of Control: The CSS2s are responsible for managing non-routine service requests. Procedures exist for the Consulting and Procurement unit tasks.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: The Department developed a draft “Procurement Procedures Guide” which “provides complete directions on the methods documented and processes required for purchasing goods and services both against master contracts and non-master contracts.”

No significant exception noted; however, the procedures for the Consulting and Procurement Unit had not been finalized.

Department Description of Control: The Quality Assurance (QA) unit analyzes the information gathered from MONIES to generate monthly reports based on a fiscal year to track and monitor vendor performance levels for completion of voice orders in the Springfield and Chicago dedicated areas, the non-dedicated areas, non-routine orders and the overall vendor performance level. These figures are reconciled with the appropriate vendor(s). Additionally, the QA unit generates a monthly voice incident report based on a fiscal year from the VOTS system to monitor the vendor(s) performance levels for voice related services. These figures are reconciled with the appropriate vendor(s). The CSC managers and QA staff attend a quarterly meeting with the vendor(s) to review task related reports.

Tests Performed: Reviewed monthly reports, meeting agenda/minutes and interviewed staff.

Test Results: Each month the QA unit generated reports from MONIES and VOTS to review vendor performance levels. These reports were utilized to determine if the vendor met stated levels of service. In addition, each month, the QA unit met with the respective vendor to discuss their performance levels.

No significant exception noted.

Department Description of Control: The QA unit generates monthly reports based on a fiscal year from the Avaya phone system to track the monthly CSC Telecommunications Service Desk and CMC performance levels. Task related reports are available.

Tests Performed: Reviewed monthly reports and interviewed staff.

Test Results: Each month the QA unit generated a report that tracked CSC and CMS performance levels. The report documented the number of calls received, call abandoned, and the average time it took to answer a call. For the period of July 2006 through February 2007, we noted the CMC and CSC abandonment rate was 6.65%. Total calls for the same period were 73,935.

No significant exception noted; however, the Department's abandonment rate of 6.65% was higher than 5% rate outlined in the Service Level Agreements.

Department Description of Control: An Avaya phone report for the IT Service Desk that tracks the weekly cumulative performance levels by agency. An Avaya Split/Skill phone report that provides a weekly view of individual phone agent statistics by agency.

Tests Performed: Reviewed reports and interviewed staff.

Test Results: Each week the QA unit generated a report that tracked IT Service Desk performance levels. The report documented the number of calls received, calls abandoned, and the average time it took to answer a call. For the period of Oct 22, 2006 through April 15, 2007 the average abandonment rate was 6.26%.

No significant exception noted; however, the Department's abandonment rate of 6.26% was higher than 5% rate outlined in the Service Level Agreements.

Department Description of Control: A weekly report from Remedy on the ESR process. (The reports provide a detailed view of all open ESRs by agency.) As a separate tab of this weekly report, a cumulative view of all ESR's is provided as the "ESR Agency Digest".

Tests Performed: Reviewed Remedy reports and interviewed staff.

Test Results: The Department utilized ESRs to track requests for software and hardware. During the period of July 2006 through April 2007, there were 834 ESRs submitted.

No significant exception noted.

Department Description of Control: The IT Service Desk utilizes the Bureau's Remedy to record and track incidents and service requests.

Tests Performed: Reviewed incident and service requests.

Test Results: When the IT Service Desk received a request, the request was to be logged into the Bureau's Remedy system. We reviewed 25 Remedy tickets, noting no exceptions.

No significant exception noted.

Department Description of Control: The IT Service Desk has processes and guidelines in place for enterprise-wide incident management, escalation and notifications, and other operational needs. These are included in the “IT Service Desk Guide to Daily Operations”.

Tests Performed: Reviewed Guide.

Test Results: The “IT Service Desk Guide to Daily Operations,” dated October 18, 2006 detailed the location and hours of operations, staffing contact information, ticket response matrix, escalation procedures, and the ticket process.

In addition, the Department developed the CSC IT Service Desk Remedy Training Manual/Guide, dated April-May 2006, which outlined the roles and responsibilities for escalations. Additionally, the Guide outlined the process for entering a ticket into Remedy.

No significant exception noted.

Department Description of Control: Procedures are in place for processing Enterprise Service Requests. Service requests are submitted via email using the Bureau’s Enterprise Service Request (ESR) form.

Tests Performed: Reviewed procedures, ESR forms and interviewed staff.

Test Results: The Department developed the Enterprise Service Request (ESR) Instructions, revised April 18, 2007. The Instructions provided guidance to the agency initiator, and the IT Service Desk staff.

The instructions required consolidated agencies to submit an ESR form to request a change to hardware or software. Upon receipt of an ESR form, IT Service Desk staff were to enter the data from the ESR form into the Remedy system.

We reviewed 25 requests from the Remedy system, noting 24 did not have the corresponding ESR form.

No significant exception noted; however, ESR forms were not being properly completed.

OVERALL CONCLUSION

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

- Ensure all forms are properly completed.
- Review, update, and finalize procedures.

SERVICE ENGINEERING – SERVICE LEVEL MANAGEMENT

CONTROL OBJECTIVE

Management should establish a service level agreement process/framework/methodology, which formalizes the performance criteria against which the quantity and quality of service will be measured.

EXISTING ENVIRONMENT

Public Act 93-25 (20 ILCS 405/405-410) authorized the Department of Central Management Services (Department) to consolidate Information Technology (IT) functions of State government. The IT Rationalization project was initiated to centralize IT functions for select agencies under the umbrella of the Department.

As a result of the consolidation, the Department's role as a service bureau has expanded; however, agencies (as the owner of data and applications) and the Department share in the responsibility to ensure an acceptable framework exists.

The following agencies were participating in the consolidation project:

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

Department Description of Control: Signed SLAs and any service related inter-agency agreements are maintained and recorded by Service Level Management.

Tests Performed: Reviewed service level agreements (SLAs), interagency agreements, and federal funding interagency agreements.

Test Results: The Department entered into three agreements with the consolidated agencies, which outlined the services provided and associated responsibilities.

Service Level Agreement (SLA)

The SLAs outlined the terms and conditions under which the agencies would receive specified IT

services from the Department. The objective of the SLA was to provide a basis and framework for the delivery of high quality services which meet the needs of the agencies.

According to the SLA, the Department was to provide the agencies “standard services”. The SLA broke down each service area based on the agency’s need/requirements. Additionally, the SLA provided for “non-standard services” and “out of scope services.”

The Department of Healthcare and Family Services did not have a signed SLA. The other ten agencies participating in the consolidation had a signed SLA. However, all but one of the agreements were signed before July 2005 and had not been updated during the audit period.

We identified numerous weaknesses in the content of the SLAs. During our review, we noted sections which did not apply to governmental entities and other sections which did not reflect the actual practice of the agencies and the Department. For example, per the Department’s Recovery Coordinator, the Recovery Services sections in approved SLAs were inaccurate and no longer in effect.

As a result, the current documents appeared to lack applicability, value to the agency operations, and enforceability.

Interagency Agreement

The Interagency agreement outlined the responsibility of the agencies in relation to the employees, assets, contracts, and appropriations affected under the IT consolidation. The agreement stated until employees and assets were physically moved to the Department, they would remain at the agency, but under the Department’s control.

All agencies participating in the consolidation had a signed Interagency Agreement; however, only 3 of the 11 agreements included an effective date.

Federal Funding Interagency Agreement

The Department and the agencies, which receive federal funding for IT services, entered into a Federal Funding Interagency Agreement. The Agreement outlined the transfer of Infrastructure Leads, Infrastructure Employees, and Infrastructure Assets.

The Agreement outlined criteria for the billing of services and required the Department to provide the agency with documentation regarding Infrastructure expenditures, which may be submitted to the federal government for reimbursement.

The Department of Revenue did not have a signed Federal Funding Interagency Agreement. The other ten agencies participating in the consolidation had a signed agreement. However, only four of 10 agreements included an effective date.

Consolidation activities must be effectively managed to ensure all federal funding requirements are met to preserve the receipt of federal funds. Agency compliance with these requirements are included in audits performed pursuant to OMB Circular A-133, the Single Audit Act.

It is ultimately the Department's and the agencies responsibility to ensure federal funds are spent and accounted for according to federal requirements.

Three agreements outlined the services provided and associated responsibilities for the Department and consolidated agencies. However, the SLAs appeared to lack applicability, value to agency operations, and enforceability.

Department Description of Control: SLAs are subject to periodic review and change. Any SLA changes proposed undergo the Department's internal approvals and are documented and tracked by Service Level Management.

Tests Performed: Reviewed Service Level Management tracking mechanism and changes for internal approval.

Test Results: As outlined above, all but one of the SLAs were signed before July 2005 and had not been updated during the audit period.

The Department developed an approval process to support changes to SLAs. However, the process had not been implemented and although 10 changes to SLAs were requested by agencies, none had been formally approved by the Department.

The approval process to promote changes to SLAs had not been implemented. As a result, SLAs had not been subject to timely updates.

Department Description of Control: SLAs are subject to discussion and changes on a quarterly basis.

Tests Performed: Interviewed Service Level Management staff and reviewed documentation.

Test Results: According to Service Level Management and Agency Relations Management, the quarterly meetings were to be facilitated by Agency Relations, with the assistance of Service Level Management, if required. However, for fiscal year 2007 neither Agency Relations nor Service Level Management had conducted quarterly meetings or any meeting with agencies to review Service Level Agreements.

The process to review SLAs on a quarterly basis had not been implemented. As a result, SLAs had not been subject to timely review and updates.

Department Description of Control: The service elements to be measured are reflected within the Service Level Agreement. Data gathering, to allow generation of service metrics, varies across Client agencies ranging from some automated methods available to a purely manual tracking and reporting process. Service metric reviews between the Department/Bureau and Client agencies are scheduled and conducted.

Tests Performed: Compared measurements outlined in the SLA with the measurements indicated in measurement reports, reviewed data gathering methods, and reviewed service metric reviews.

Test Results: Each SLA included a method to define and measure service elements provided by the Department to the agency.

The Department generally defined nine performance measures in each SLA. However, the Department was not reporting on three of the nine performance measures for all agencies and in other cases, select performance measures were not being reported for some agencies.

Meetings to discuss service metrics were not held in the audit period. Additionally, on October 31, 2006 the Department sent a memorandum to consolidated agencies notifying them of the temporary discontinuation of service metric meetings.

The process to gather data, report on performance measures and conduct routine meetings had not been fully implemented. As a result, agencies were not being provided with a formal mechanism to discuss service metrics and determine if the Department was complying with the requirements outlined in the SLA's.

Department Description of Control: Metrics are reported and published on a monthly basis via an online tool. The monthly "online" report is also available for viewing by the Client agency.

Tests Performed: Reviewed monthly reports and interviewed Service Level Management.

Test Results: Some monthly measures were reported via an online reporting tool. The Department was supposed to have the previous months report available online by the tenth of the next month.

Each agency had selected staff which had access to the online reporting tool in order to review its monthly measurement reports.

We reviewed the monthly reports, noting they were not always available by the tenth of the month.

Although not a significant exception, monthly reports were not always available by the tenth of each month.

Department Description of Control: Historical monthly metric data is maintained by Service Level Management.

Tests Performed: Reviewed historical data.

Test Results: We reviewed online reports from July through December 2006 and reviewed historical data.

No significant exception noted.

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

Tests Performed: Interviewed Service Level Management and staff at consolidated agencies.

Test Results: In order to obtain an understanding of the current environments and practices, we held meetings with the Department and the Chief Information Officers (CIOs) of consolidated agencies. During these meetings, both the Department and the consolidated agencies were unable to provide a clear picture of the assignment and control of day to day IT activities. For example, during our preliminary analysis of generally accepted IT controls, the Department and the consolidated agencies had to perform research to determine the current practices and responsibilities.

Problems with communication and planning were frequently addressed during the meetings. In one instance, the lack of planning and communication caused a critical agency application (requiring 24x7 availability to support required services) to be unavailable for an extended period.

The process to adequately plan and communicate objectives to agencies had not been implemented. As a result, agencies were not always aware of significant activities and changes that could impact their internal operations.

OVERALL CONCLUSION

The SLAs had been in place for over two years, and very little progress had been made to ensure the agreements achieved their original intent and objectives. The processes to communicate with agencies, report on service metrics, and ensure objectives are met were not implemented or achieved.

The SLAs outlined the terms and conditions under which the Department would provide services to the agencies. The “objective is to provide a basis and framework for the delivery of high quality services that meet the needs of the agency.” In order for the needs to be met, the SLAs must accurately reflect the environment and responsibilities.

In order to ensure the delivery of “high quality services,” the Department and agencies must work together to ensure the SLAs reflect the actual environment, responsibilities, and services to be provided. Once the SLAs reflect such, accurate and actual performance measurements must be reported in order to provide the Department and agencies substantiation of the actual services provided.

Additionally, in order to ensure each party is aware of the goals and directions of each other, an effective communication network must be in place. Each party must be aware of changes that are

occurring in order to assess the impact on operations and ensure problems are communicated and addressed in a timely manner.

The Department should thoroughly review the SLAs and ensure the agreements meet the original intent and objectives. The Department should ensure the terms, performance measures, and responsibilities are communicated, realistic, achievable, monitored, and enforced. Specifically, the Department must develop a mechanism to track and approve requested changes to the SLAs.

SERVICE ENGINEERING – BUSINESS PROCESS ENGINEERING

CONTROL OBJECTIVE

Management should ensure project teams and business owners adequately outline their business processes.

EXISTING ENVIRONMENT

Background Provided by the Department: Business Process Engineering is assigned the following responsibilities:

- Develop BPE process framework which includes the team's processes, policies, procedures, standards, tools, work instructions, metrics and required competencies/skill sets.
- At the direction of Bureau leadership, BPE supports project teams and/or process owners in the design, development and potential reworking of new or existing IT service delivery and service support processes.

Department Description of Control: Currently operational direction and guidance for meeting said responsibilities is provided through a documented process overview and corresponding form templates.

Tests Performed: Reviewed process overview, project documentation, and interviewed staff.

Test Result: Business Process Engineering became operational in November 2006. Since becoming operational, Business Process Engineering developed a "Process Design Model" which identified each step/activity to be completed during a project.

No significant exception noted.

OVERALL CONCLUSION

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

ILLINOIS OFFICE OF INTERNAL AUDIT

CONTROL OBJECTIVE

Management should ensure that Internal Audit, or another independent audit source, routinely reviews information technology integrity and security issues. Management should also ensure that the Internal Audit division complies with statutory mandate -- 30 ILCS 10/2003 (3) to review the design of major new systems and major modifications to existing systems before their installation to ensure that the systems provides for adequate audit trails and accountability.

EXISTING ENVIRONMENT

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

Department Description of Control: IOIA has established a process for identifying major new systems and major changes to existing systems for system development audits to determine which systems development projects are major and require an audit. Periodically, IOIA contacts each agency to update the information and request a list of new planned projects.

Tests Performed: Reviewed procedures and interviewed staff.

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

Additionally, at the beginning of each budget year, the IOIA's IT Audit Manager reviewed the budget book to identify funds allocated to new systems or programs.

Under the current process, it is the agencies' responsibility to inform IOIA of new system developments or major modifications.

No significant exception noted.

Department Description of Controls: IOIA has developed a database of system development projects for all agencies under the Governor.

Tests Performed: Reviewed database and interviewed staff.

Test Results: Upon notification of a new development or major modification, projects were added to the IOIA database. The database documented the agency and a summary of the project.

No significant exception noted.

Department Description of Controls: Based on the implementation date, IOIA performs a risk assessment for the project.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: Once a new system development or major modification was identified, IOIA staff would contact the agency to request information regarding the project. IOIA staff would complete a risk matrix and questionnaire and make a determination on whether the project met the criteria for a major development or modification. If the IOIA determined a project was major, a letter would be sent to the Agency Director informing them IOIA would be reviewing the system. If the IOIA determined a project was not major, a letter would be sent to the Agency Director informing them a review by IOIA was not warranted.

According to the IOIA's IT Audit Manager, the Bureau did not have any projects which met the criteria for the completion of the risk matrix and questionnaire during the audit period.

No significant exceptions noted.

OVERALL CONCLUSION

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

DCMS ACCOUNTING - INTERNET BILLING SYSTEM (IBiS)

CONTROL OBJECTIVE

Management should ensure that the application has policies, procedures and methods to ensure that all transactions are entered, processed and reported correctly. Management should ensure a billing system exists, which accurately charges users for computer services, provides for sufficient audit trails, and supplies users with sufficient information to determine the accuracy of the individual billings.

EXISTING ENVIRONMENT

The Department of Central Management Services, Bureau of Computer and Communications Services (Bureau) developed a web-based application that is used by Accounting to provide billing for various Department service funds. Due to the consolidation of various functions of State government into the Department, IBiS was developed to provide a mechanism to bill agencies for consolidated services. The billing invoices are the foundation for agencies to make payments to the Department. Additionally, the invoices are to provide documentation for agencies to use for Federal Fund participation purposes.

IBiS was utilized by the consolidated agencies:

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

The Department bills for the following consolidated services through IBiS:

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

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

Department Description of Control: The system is generally available 24 hours a day, seven days a week, except for downtime scheduled for production moves.

Tests Performed: Reviewed downtime reports.

Test Results: Our review of the IBiS downtime report for July through December 2006 showed no unscheduled downtime.

No significant exception noted.

Department Description of Control: Changes are handled through the Department's Change Management process (Lotus Notes).

Tests Performed: Reviewed IBiS changes and interviewed staff.

Test Results: According to management changes to IBiS followed change management procedures

During the audit period there were no completed changes to IBiS.

No significant exception noted.

Department Description of Control: BAS/IBiS access is secured with security software and internal system role-based security.

Tests Performed: Reviewed granting of rights and appropriateness of individuals with access to the Department's IBiS.

Test Results: To obtain access to IBiS, the Department's Accounting Division was required to receive an "Internet Billing System Security Request Form" approved by an agency CFO.

The Department's Accounting Division was responsible for the creation, maintenance, and deletion of internal security IDs.

We reviewed access rights for six Department staff noting, access rights appeared appropriate.

No significant exception noted.

Department Description of Control: Billing data is compiled by the various entities and provided in a structured layout form to the Bureau. Files loaded to IBiS must successfully pass the load program edits that ensures the file is balanced.

Tests Performed: Reviewed load program edits and file balance report.

Test Results: Each file loaded to IBiS must pass eight program edits. If a file did not pass the load program edits, an error message was created and the file must be corrected prior to resubmission.

No significant exception noted.

Department Description of Control: Accounting is provided load reports, and Accounting is responsible for the release of the billing to the user agency community along with notification of the release of the billing.

Tests Performed: Reviewed load and EXP5T reports.

Test Results: Information from the accounting and payroll systems was uploaded into IBiS each month. After the upload was completed a load report was produced. The load report was then verified to the EXP5T report to ensure the load was complete and accurate. We reviewed the load reports and the EXP5T reports for the period of July through December 2006, noting they agreed.

No significant exception noted.

Department Description of Control: Accounting is responsible for the release of the billing to the user agency community along with notification of the release of the billing.

Tests Performed: Reviewed billing notifications.

Test Results: Upon completion of the monthly IBiS billings, the Department's Accounting Division sent an email to consolidated agencies' CFOs and IBiS users indicating the billings were ready for review and processing.

No significant exception noted.

Department Description of Control: The ARPS load program ensures the load file passes all pre-edits prior to the load of receivables.

Tests Performed: Reviewed ARPS load report.

Test Results: Each file loaded to ARPS must pass four program edits. At the end of each load an error report was generated and sent to Accounting for review and correction. We reviewed the December 2006 error report, noting no errors.

No significant exception noted.

Department Description of Control: BAS/IBiS has an on-line user manual available for the Bureau's Financial home page.

Tests Performed: Reviewed BAS/IBiS User Guide.

Test Results: The Department developed the Billing Allocation System User Guide, dated December 10, 2004. The Guide provided guidance on obtaining access, logging in, completion of the billing and help desk contacts. However, during our review we noted the Guide was based on the BAS process, not the current IBiS process.

A User Guide existed; however, the Guide had not been updated to reflect the current process.

Department Description of Control: Instructions on how to use the IBiS functionality were distributed by Accounting.

Tests Performed: Reviewed IBiS Instructions.

Test Results: The IBiS instructions provided users with detailed steps on accessing and using IBiS.

No significant exception noted.

Department Description of Control: BAS/IBiS is backed up at varying intervals.

Tests Performed: Reviewed backup schedules.

Test Results: Backups were automatically scheduled to be completed daily, weekly and monthly.

No significant exception noted.

Department Description of Control: The backups are on disk and maintained at the Department's Central Computer Facility.

Tests Performed: Reviewed backups maintained at the CCF.

Test Results: The backups were retained at the CCF.

No significant exception noted.

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

Tests Performed: Reviewed payroll cost charged to agencies and interviewed staff.

Test Results: The Service Center Allocation System (SCAS) was the primary source to bill consolidated agencies for specific services provided to agencies by Department employees. A formal methodology clearly documenting the allocation of Department employee charges to consolidated agencies did not exist. If consolidated agencies request reimbursement from federal funds for these Department employee charges, the lack of a formal methodology may make it difficult to verify the appropriateness of charges.

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

From July through December 2006, Department employee costs specifically charged to the consolidated agencies were \$13,782,249.

We reviewed the process to allocate charges to consolidated agencies and found:

- Employees who were exempt from entering time into SCAS; however, 100% of their time was charged to a consolidated agency.
- Documentation supporting the appropriateness of employees exempt from entering time into SCAS was lacking. In addition, we interviewed 22 of these employees and found that 20 employees listed duties that appeared unsuitable for their allocation of time.
- Multiple charges to two consolidated agencies that we were unable to verify appropriateness or reconcile to employee time records.

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

Department Description of Control: Accounting verifies that the total of the extract and EXP5T report agree.

Tests Performed: Reviewed extract and EXP5T reports.

Test Results: IT billings were comprised of Accounting Information System (AIS) data and payroll data. The AIS data consisted of actual expenditures incurred by the Department on behalf of the consolidated agency. The payroll data consisted of the actual payroll cost associated with the individuals who transferred to the Department during the IT consolidation. The extract and the EXP5T reports were reviewed to verify that all expected data was transferred to IBiS.

We reviewed the extract and EXP5T reports for the period of July through December 2006 and reconciled the AIS and payroll data to IBiS, noting no exceptions.

No significant exception noted.

Department Description of Control: Upon verification from the Accounting Division that billings in IBiS are correct, an ARPS load request form is completed and sent to Operations to load billing into ARPS.

Tests Performed: Reviewed Accounts Receivable Posting System (ARPS) load request forms.

Test Results: We reviewed the Run Execution Request (ARPS load) for the period of July through December 2006, noting no exceptions.

No significant exception noted.

Department Description of Control: Business Services downloads the AIS billing file. The file is sorted by agency, and a spreadsheet file is created for each agency. This detail file lists each invoice that was paid on behalf of the agency that month and includes the agency service center, the cost center, DOC, voucher control number, voucher date and number, vendor name, vendor invoice number, beginning and ending dates of the service, a description of the services, and the amount.

Tests Performed: Reviewed the AIS billing file and interviewed staff.

Test Results: The Department reviewed and approved all invoices. When an invoice was for services rendered to a consolidated agency, a copy was provided to the appropriate agency and the invoice was entered into AIS and allocated to the agency.

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

On a monthly basis, the Department provides the agencies a billing statement. The billing statement did not provide details regarding the expenditure.

We reviewed 20 AIS invoices, noting:

- Four invoices (\$19,044.18) were for consultant charges; however, sufficient detail was not included to determine the appropriateness of the charges. Additionally, the consultant contracts did not provide a statement of work to help determine the appropriateness of charges.
- Two invoices (\$648.71) were charges relating to training and travel; however, sufficient detail was not included to determine the appropriateness of the charges. Additionally, upon discussion with the staff member who attended the training, it appeared the charges should not have been billed to the agency.
- An invoice for consultant work (\$5,909.12) indicated it was for work conducted on the FY 06 Department of Children and Family Services' Statewide Automated Child Welfare Information System (SACWIS) project; however, the charges were billed to the Department of Healthcare and Family Services.
- Interest charges of \$6,001 were billed to consolidated agencies for the period of July through December 2006. Our review of the supporting documentation indicated the interest charges were the result of the Department's delay in processing payments to vendors.

It was the agencies responsibility to review the monthly billing statement and verify the accuracy of charges. If agencies determine a charge was inaccurate they may request a credit. For the period of July through December 2006, the Department issued \$82,032 in credits.

Total IBiS billings for July through December 2006 were \$26,511,065.90.

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

Department Description of Control: Payments are posted to the Billing and Accounting Receivable Cash Management System (BARCS) and to Accounts Receivable Posting System (ARPS).

Tests Performed: Reviewed payments posted in BARCS and ARPS.

Test Results: We reviewed two agencies billing statements and payment postings to BARCS and ARPS for the period of July through December 2006, noting no exceptions.

No significant exception noted.

Department Description of Control: Segregation of duties ensure that cashier functions and billing/accounts receivable duties are performed by different Accounting employees.

Tests Performed: Reviewed segregation of duties.

Test Results: A staff member opened and date stamped mail and forwarded all warrants and checks to another staff member (cashier). The cashier endorsed warrants and checks, prepared the deposit slip, and entered the data into BARCS. The deposit slip was sent to a separate staff member for processing.

No significant exception noted.

Department Description of Control: Accounting reconciles receipts to Comptroller SB04 Report and reconciles accounts receivable to ARPS.

Tests Performed: Reviewed reconciliation.

Test Results: On a monthly basis the receipts were reconciled to a Comptroller's report (SB04 report). Additionally, on a monthly basis, ARPS data was reconciled to the accounts receivable listing.

We reviewed the receipts and accounts receivable reconciliations for the period of July through December 2006, noting no exceptions.

No significant exception noted.

Department Description of Control: Internal controls exist within Accounting systems edits to prevent fraud.

Tests Performed: Interviewed staff.

Test Results: The BARCS and ARPS systems had edit checks built into the system to promote data integrity and completeness.

No significant exception noted.

OVERALL CONCLUSION

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

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

- Develop and implement a formal methodology to clearly document the billing rate structure and allocation of charges.
- Develop a process to review and verify the accuracy of billing statements.
- Provide adequate documentation to agencies to support billing statements and comply with federal fund reimbursement guidelines established by OMB circular A-87.
- Update the BAS/IBiS User Guide to reflect the current process.

PHYSICAL SECURITY - BUREAU OF PROPERTY MANAGEMENT (BOPM)

CONTROL OBJECTIVE

Management should ensure that appropriate environmental and physical security controls are established to protect the information systems hardware and other assets.

EXISTING ENVIRONMENT

The Department utilizes four facilities to conduct IT operations for the State; Central Computer Facility (CCF), the Communications Building, the Business Services Building, and the James R. Thompson Center (JRTC). The Department is responsible for the maintenance and security for all the facilities, except the JRTC.

Department Description of Control: The Department has installed a fire suppression and detection system at the Central Computer Facility (CCF). The System utilizes an environmentally friendly gaseous agent.

Test Performed: Toured facility and interviewed staff.

Test Results: The CCF computer room had a fire suppression and detection system that was Underwriter Laboratory approved and utilized an environmentally friendly gaseous agent, FM-200.

During our tour of the CCF, we noted the fire suppression and detection system was inspected in April 2006.

No significant exception noted.

Department Description of Control: The Department has installed smoke detectors which are connected to the alarm system and the local fire/police departments. The Department's Communication Building and the Business Services Building also have fire detection and suppression systems, smoke detectors and fire extinguishers. These controls are tested periodically to ensure operational efficiency.

Test Performed: Toured facilities and interviewed staff.

Test Results: The Department had smoke detectors throughout the facilities. In addition, the Communication Building and the Business Services Building contained fire detection and suppression systems and/or fire extinguishers.

During our tour of the facilities, we noted the fire detection and suppression systems and fire extinguishers were inspected within the last year.

No significant exception noted.

Department Description of Control: The Department has contracted with janitorial services to perform duties on a daily, weekly, and monthly basis. The contracts outline the duties and timing of the duties to be performed. The Department conducts background checks and training for each janitorial employee.

Test Performed: Reviewed background checks, training records, and interviewed staff.

Test Results: The Department contracted for janitorial services for the facilities.

During the audit period, there were 16 individuals assigned to the facilities for janitorial services. Per Department staff, a background check was only performed on one individual and no training was conducted. After notification, Department management stated background checks would be completed for all individuals assigned to the facilities for janitorial services.

The Department had not conducted background checks or provided training for janitorial employees.

Department Description of Control: In order to mitigate the risk of a power failure, the Department's data center is supplied by two different sources. In addition, the Department has installed an uninterruptible power supply (UPS). Within an allotted time the Department's generators will engage. The Department has in place a service contract for the UPS to provide routine preventive maintenance and remedial service as required.

Test Performed: Reviewed contracts, toured facility, and interviewed staff.

Test Results: The electrical power for the CCF was from two different utility-supplied power grids. If one source failed, a system would transfer to the other power source. If both power sources failed, the building's power would be supplied from the CCF's UPS. In the short term, a battery bank would supply the needed electrical power. This period of time would allow the diesel-powered turbines to be started. The turbine generators could supply electrical power until utility-supplied power is restored.

The Department has a service contract in place to provide routine preventive maintenance on the UPS components.

In the past year over 775 servers were transferred to the Department from agencies participating in the consolidation project. Planning for the transfer of approximately 370 additional servers was underway with relocation starting in May 2007.

The increase in equipment significantly increased electrical and cooling demands, and during the audit period, the Department experienced some difficulties meeting its cooling requirements. Department Management stated there is a project underway to determine capacity and utilization rates for "live" power and "backup" power.

No significant exception noted in the current environment; however, power and cooling demands were increasing.

Department Description of Control: The CCF, Telecommunication Building, and the Business Services Building are designed to have BCCS individuals assigned the responsibility of handling real property keys and to collaborate with Property Management to ensure the keys are properly allocated and tracked, but the identity of these individuals is either unknown or the individuals are not aware of any forms or procedures necessary to accomplish this task.

Test Performed: Reviewed key listing and interviewed staff.

Test Results: The Department's Bureau of Property Management was responsible for the management of real property keys; however, responsibility had been assigned to an individual at each of the facilities.

During our testing, we identified some deficiencies in tracking and maintaining real property keys.

Although not a significant exception due to the card-key system, procedures to effectively track and maintain real property keys had not been implemented.

Department Description of Control: The Department maintains a master contract with E.L.A. Security, Inc. This contract states the agencies, which utilize E.L.A. Security, Inc. guards, are required to provide a Post Order Manual for the guards at each location. This is to ensure communication between the guards and their respected duties at each facility.

Test Performed: Reviewed contract and interviewed staff.

Test Results: The Department entered into a master contract with E.L.A. Security, to provide security guards at State facilities.

During our review, we requested the Post Order Manual; however, the Department stated the Manual had not been created.

No significant exception noted; however, the Post Order Manual had not been created and provided to guards.

OVERALL CONCLUSION

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

- Ensure all janitorial employees undergo a background check and training.
- Conduct a detailed analysis of the Data Center's power and cooling requirements to ensure short and long term needs are adequately addressed.
- Develop and implement procedures to effectively track and maintain real property keys.
- Create the Post Order Manual as outlined in the security contract.

This Page Intentionally Left Blank

APPLICATION CONTROLS

Application controls are the methods, policies, and procedures adopted by an organization to ensure all transactions are entered, processed, and reported correctly. Application controls ensure data being entered, processed, and stored are complete and accurate. They ensure the output from the computer application is timely and accurate.

Application controls can be grouped into three areas: input; processing; and output. Input controls ensure the data entered into the system are authorized and accurate. These controls include both manual and computerized techniques. Processing controls are those that are coded into the software program. Manual procedures often supplement the programmed controls to verify that all processing has taken place as intended. Output controls govern the printing and distribution of reports.

The Department has developed several applications for use by State agencies. As part of the Third Party Review, we reviewed four of the applications used by multiple State agencies.

The applications reviewed were:

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

This Page Intentionally Left Blank

COMMON APPLICATIONS – ENTERPRISE APPLICATION ACCOUNTING INFORMATION SYSTEM

CONTROL OBJECTIVE

Management should ensure that the application has policies, procedures and methods to ensure that all transactions are entered, processed and reported correctly. Management should ensure that application systems are configured and controlled to promote security, integrity, and availability.

EXISTING ENVIRONMENT

The Accounting Information System (AIS) is an online, menu-driven, mainframe application that provides an automated expenditure control and invoice/voucher processing system. Invoice processing allocates invoice amounts by cost centers and sub-accounts and groups common invoices for payment according to the Comptroller's Statewide Accounting Management System (SAMS) procedures.

AIS was implemented in 1995. AIS was utilized by 50 entities (see page 189 for the list of user agencies).

Department Description of Control: The AIS is secured using security software.

Tests Performed: Reviewed granting of security software rights, reviewed the appropriateness of individuals with access to the Department's AIS, and interviewed AIS staff.

Test Results: Access to AIS was controlled through security software (Resource Access Control Facility (RACF)), in addition to AIS' internal security. Users were required to have a properly authorized security software user ID and password to gain access to the operating environment. Once access to the operating environment had been granted, a separate application user ID, password, and schedule number was required to gain access to AIS.

Assignment, authorization, and maintenance of access rights were the responsibility of each agency's security administrator.

No significant exception noted.

Department Description of Control: AIS has internal security in addition to security software.

Tests Performed: Reviewed granting of rights and appropriateness of individuals with access to the Department's AIS.

Test Results: We reviewed 15 individuals with access rights for the Department, noting three individuals who no longer needed access rights to AIS. After notification, the Department removed the RACF access rights.

The Department did not have a formal process to ensure access rights were appropriate.

Department Description of Control: Users must have an authorized ID and password to gain access.

Tests Performed: Reviewed ID and password requirements.

Test Results: Security software password change and content requirements were acceptable.

No significant exception noted.

Department Description of Control: Changes to AIS are controlled through the EBAS Methodology.

Tests Performed: Reviewed changes for compliance with EBAS Methodology.

Test Results: During the audit period, AIS had five closed service requests; enhancements and maintenance. We reviewed the five requests noting they complied with the EBAS Methodology. The EBAS Methodology required maintenance SRs to have a completed service request form and enhancements to have a completed SR and comply with the Methodology development standards.

No significant exception noted.

Department Description of Control: A Service Request Form is to be completed for each change.

Tests Performed: Reviewed service request forms.

Test Results: We reviewed five service request forms relating to AIS requests, noting they had been completed.

No significant exception noted.

Department Description of Control: Each change requires approval and testing before implementation.

Tests Performed: Reviewed changes for approval and testing.

Test Results: We reviewed three maintenance requests noting each had been approved; however, the maintenance requests selected did not require testing to be conducted.

In addition, we reviewed two enhancement requests noting each had been approved and required testing was conducted.

No significant exception noted.

Department Description of Control: Library control moves changes to production.

Tests Performed: Reviewed Library control move authorizations.

Test Results: AIS had five closed requests, of which only two required a Library control move authorization. Our review indicated the changes had been properly approved.

No significant exception noted.

Department Description of Control: AIS is backed up at varying intervals.

Tests Performed: Reviewed backup schedules.

Test Results: Backups were automatically scheduled to be completed daily, weekly and monthly.

No significant exception noted.

Department Description of Control: Backups are maintained at the CCF and an off-site storage location.

Tests Performed: Reviewed backups maintained at the CCF and at the off-site storage location.

Test Results: We reviewed the list of backup tapes and identified daily, weekly, and monthly backup tapes. We selected 31 backup tapes from the list and located all the tapes at the CCF or Regional Vault.

No significant exception noted.

Department Description of Control: The Department has developed a user manual, the AIS User Manual, which is located on the State's Enterprise Web Server. The manual provides guidance to the user when utilizing the various functions.

Tests Performed: Reviewed the AIS User Manual.

Test Results: The Department had a User Manual, which provided users with guidance on logging into the application, maintaining invoices, and help desk contacts.

No significant exception noted.

Department Description of Control: AIS was developed with edits that force correction of errors and completion of critical fields before a transaction is accepted.

Tests Performed: Reviewed edits of AIS and reviewed agency data.

Test Results: Data entered into the system was the responsibility of user agencies. AIS had numerous edit checks built into the system to notify the users of any exceptions. Errors were required to be corrected before the transaction was accepted.

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 19,172 data records tested were entered properly and complied with date composition standards. During our testing of AIS data, we did not identify any significant weaknesses.

No significant exception noted.

Department Description of Control: AIS provides various on-line and batch reports to assist in the balance of transactions.

Tests Performed: Reviewed AIS User Manual.

Test Results: AIS provided various on-line and batch reports to assist in the balance of transactions. A complete listing of the various reports was available in the AIS User Manual.

No significant exception noted.

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

Tests Performed: Reviewed disaster recovery plan for AIS.

Test Results: The Department developed the Financial Application Disaster Recovery Plan, revised December 2006.

The Plan provided guidelines on the restoration of the financial applications, staff of the different applications, and tape listings. Additionally, the document outlined the Financial Systems Disaster Recovery Team members and their backups, contact information as well as the job functions for each individual.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should periodically review access rights to AIS and ensure access is appropriate.

Department records listed the following entities as users of the Accounting Information System.

1. Board of Higher Education
2. Capital Development Board
3. Department of Agriculture
4. Department of Central Management Services
5. Department of Corrections
6. Department of Financial and Professional Regulation
7. Department of Human Rights
8. Department of Labor
9. Department of Juvenile Justice
10. Department of Military Affairs
11. Department of Natural Resources
12. Department of Public Health
13. Department of Veterans' Affairs
14. Department on Aging
15. Environmental Protection Agency
16. General Assembly Retirement System
17. Guardianship and Advocacy Commission
18. Historic Preservation Agency
19. Human Rights Commission
20. Illinois Arts Council
21. Illinois Commerce Commission
22. Illinois Community College Board
23. Illinois Council on Developmental Disabilities
24. Illinois Criminal Justice Information Authority
25. Illinois Deaf and Hard of Hearing Commission
26. Illinois Educational Labor Relations Board
27. Illinois Labor Relations Board
28. Illinois Law Enforcement Training and Standards Board
29. Illinois Office of the State's Attorneys Appellate Prosecutor
30. Illinois Prisoner Review Board
31. Illinois Procurement Policy Board
32. Illinois Student Assistance Commission
33. Illinois Violence Prevention Authority
34. Illinois Workers' Compensation Commission
35. Judges' Retirement System
36. Judicial Inquiry Board
37. Office of Management and Budget
38. Office of the Attorney General
39. Office of the Auditor General
40. Office of the Executive Inspector General
41. Office of the Governor
42. Office of the Lieutenant Governor
43. Office of the State Appellate Defender
44. Office of the State Fire Marshal
45. Property Tax Appeal Board
46. State Board of Elections
47. State Employees' Retirement System
48. State Police Merit Board
49. State Universities Civil Service System
50. Supreme Court of Illinois

This Page Intentionally Left Blank

COMMON APPLICATIONS – ENTERPRISE APPLICATION CENTRAL PAYROLL SYSTEM

CONTROL OBJECTIVE

Management should ensure that the application has policies, procedures and methods to ensure that all transactions are entered, processed and reported correctly. Management should ensure that application systems are configured and controlled to promote security, integrity, and availability.

EXISTING ENVIRONMENT

The Central Payroll System (CPS) is an online and batch system that standardizes payroll procedures and processing for State agencies. The CPS enables State agencies to maintain automated employee pay records and provides them with payroll documents and a computer file that are submitted to the Office of the Illinois Comptroller for the production of the agencies' payroll warrants.

CPS was implemented in 1985. CPS was utilized by 75 entities (see page 196 for the list of user agencies).

Department Description of Control: CPS is secured using security software.

Tests Performed: Reviewed granting of security software rights, reviewed the appropriateness of individual with access to the Department's CPS, and interviewed CPS staff.

Test Results: Access to CPS was controlled through security software (Resource Access Control Facility (RACF)), in addition to CPS' internal security. Users were required to have a properly authorized security software user ID and password to gain access to the operating environment. Once access to the operating environment had been granted, a separate application user ID, password, and schedule number was required to gain access to CPS.

Assignment, authorization, and maintenance of access rights were the responsibility of each agency's security administrator.

No significant exception noted.

Department Description of Control: The CPS has internal security in addition to security software.

Tests Performed: Reviewed granting of rights and appropriateness of individuals with access to the Department's CPS.

Test Results: We reviewed individuals with access rights for the Department. The access rights appeared appropriate.

No significant exception noted.

Department Description of Control: Users must have an authorized ID and password to gain access.

Tests Performed: Reviewed ID and password requirements.

Test Results: Security software password change and content requirements were acceptable.

No significant exception noted.

Department Description of Control: Changes to CPS are controlled through the EBAS Methodology.

Tests Performed: Reviewed changes for compliance with EBAS Methodology.

Test Results: During the audit period, CPS had 16 service requests, of which 11 were closed. Of the 11 closed service requests, we reviewed four maintenance requests relating to CPS, noting they had been completed in accordance to the EBAS Methodology. The EBAS Methodology required maintenance requests to have a completed service request form.

Additionally, we noted there were no major changes to CPS in the past year.

No significant exception noted.

Department Description of Control: A Service Request Form is to be completed for each change.

Tests Performed: Reviewed service request forms.

Test Results: We reviewed four service request forms relating to CPS maintenance requests, noting they had been completed.

No significant exception noted.

Department Description of Control: Each change requires approval and testing before implementation.

Tests Performed: Reviewed changes for approval and testing.

Test Results: We reviewed four maintenance requests, noting each had been approved; however, the maintenance requests selected did not require testing to be conducted.

No significant exception noted.

Department Description of Control: Library control moves changes to production.

Tests Performed: Reviewed Library control move authorizations.

Test Results: We reviewed the Library control move authorizations for four CPS maintenance changes, noting they had been approved.

No significant exception noted.

Department Description of Control: CPS is backed up at varying intervals.

Tests Performed: Reviewed backup schedules.

Test Results: Backups were automatically scheduled to be completed daily, weekly and monthly.

No significant exception noted.

Department Description of Control: Backups are maintained at the CCF and an off-site storage location.

Tests Performed: Reviewed backups maintained at the CCF and at the off-site storage location.

Test Results: We reviewed the list of backup tapes and identified daily, weekly, and monthly backup tapes. We selected nine backup tapes from the list and located all the tapes at the CCF or Regional Vault.

No significant exception noted.

Department Description of Control: The Department has developed a User Manual to provide guidance.

Tests Performed: Reviewed the CPS User Manual.

Test Results: The Department had a User Manual, which provided users with guidance on logging into the application, recovery in the event of a disaster, backup cycle, adding/deleting employees, and the processing and completion of payroll.

No significant exception noted.

Department Description of Control: CPS has an edit feature which will reject invalid information.

Tests Performed: Reviewed edits of CPS and reviewed agency data.

Test Results: Data entered into the system was the responsibility of the user agency. The CPS had online edit checks to help prevent a user from entering a transaction with invalid data. If an error occurred during data entry, users were not allowed to continue until the error had been corrected.

During our review, we selected two agencies' CPS data and tested employee identification numbers, voucher numbers, warrant amounts and date fields for proper input, edits, and compliance with date standards. We determined that the 11,926 data records tested were entered properly and complied with date composition standards. During our testing of CPS data, we did not identify any significant weaknesses.

No significant exception noted.

Department Description of Control: The Department has procedures in place to handle error(s) which occur during processing.

Tests Performed: Reviewed the correction of errors.

Test Results: If an error occurred after the “close” of a payroll, a CPS application staff member was required to make the corrections. The corrections were documented and approved. Additionally, the Department developed a manual, How to Make Corrections, which documented procedures on the corrections of various errors.

No significant exception noted.

Department Description of Control: The CPS provides payroll reports/voucher(s) for agencies.

Tests Performed: Reviewed the reports/vouchers, CPS Manual, and interviewed CPS staff.

Test Results: Each pay period, the following six standard payroll reports were provided to agencies by CPS staff:

- *Personal Services Expenditure Report,*
- *Expenditure Report with Insurance Reimbursement,*
- *Employer Pickup of Employee Retirement Contributions,*
- *Translog Report,*
- *Alpha Change Listing, and*
- *Warning Report from Payroll Calculations.*

No significant exception noted.

Department Description of Control: Only authorized individuals are allowed to pick up payroll reports.

Tests Performed: Reviewed the Payroll Release Log.

Test Result: Reports were printed by I/O Control and delivered to the CPS staff. The CPS staff separated the reports, and provided the reports to the security guards for distribution.

Security guards were provided with both Payroll Pickup Procedures and a list of individuals authorized to pick up payroll reports. We reviewed two months of the Payroll Release Log, noting no significant exception.

No significant exception noted.

Department Description of Control: The authorized pick up listing is reviewed periodically.

Tests Performed: Reviewed the listing and memos sent to agencies.

Test Results: The list of individuals authorized to pickup payroll information was last updated in November 2005.

No significant exception noted.

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

Tests Performed: Reviewed disaster recovery plans.

Test Results: Disaster recovery guidance was communicated to user agencies through the CPS Manual. In the event of an emergency, Central Payroll would submit to the Comptroller the last correct version of the payroll file for payment. User agencies were responsible for supplying the last correct version of the hardcopy voucher, without the Comptroller would not produce warrants for that agency. User agencies were responsible for retaining the hardcopy payroll voucher for the three most current pay periods.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should review and update the authorized pickup listing at least annually.

Department records listed the following entities as users of the Central Payroll System.

1. Board of Higher Education
2. Capital Development Board
3. Commission on Government Forecasting and Accountability
4. Court of Claims
5. Department of Agriculture
6. Department of Central Management Services
7. Department of Children and Family Services
8. Department of Commerce and Economic Opportunity
9. Department of Corrections
10. Department of Financial and Professional Regulation
11. Department of Human Rights
12. Department of Labor
13. Department of Military Affairs
14. Department of Natural Resources
15. Department of Public Health
16. Department of Revenue
17. Department of Veterans' Affairs
18. Department on Aging
19. East St. Louis Financial Advisory Authority *
20. Emergency Management Agency
21. Environmental Protection Agency
22. Executive Ethics Commission
23. Guardianship and Advocacy Commission
24. Historic Preservation Agency
25. House of Representatives
26. Human Rights Commission
27. Illinois Arts Council
28. Illinois Civil Service Commission
29. Illinois Commerce Commission
30. Illinois Community College Board
31. Illinois Council on Developmental Disabilities
32. Illinois Criminal Justice Information Authority
33. Illinois Deaf and Hard of Hearing Commission
34. Illinois Educational Labor Relations Board
35. Illinois Labor Relations Board
36. Illinois Law Enforcement Training and Standards Board
37. Illinois Math and Science Academy
38. Illinois Office of the State's Attorneys Appellate Prosecutor
39. Illinois Prisoner Review Board
40. Illinois Procurement Policy Board
41. Illinois State Board of Investment *
42. Illinois State Police
43. Illinois Student Assistance Commission
44. Illinois Violence Prevention Authority
45. Illinois Workers' Compensation Commission
46. Joint Committee on Administrative Rules
47. Judges' Retirement System
48. Judicial Inquiry Board
49. Legislative Audit Commission
50. Legislative Ethics Commission
51. Legislative Information System
52. Legislative Printing Unit
53. Legislative Reference Bureau
54. Legislative Research Unit
55. Medical District Commission *
56. Office of Management and Budget
57. Office of the Architect of the Capitol
58. Office of the Attorney General
59. Office of the Auditor General
60. Office of the Executive Inspector General
61. Office of the Governor
62. Office of the Lieutenant Governor
63. Office of the Secretary of State
64. Office of the State Appellate Defender
65. Office of the State Fire Marshal
66. Office of the Treasurer
67. Property Tax Appeal Board
68. Sex Offender Management Board
69. State Board of Education
70. State Board of Elections
71. State Employees' Retirement System
72. State of Illinois Comprehensive Health Insurance Board
73. State Police Merit Board
74. State Universities Civil Service System
75. Teachers' Retirement System of the State of Illinois

* Agency payroll information is entered into the system by CPS staff.

COMMON APPLICATIONS – ENTERPRISE APPLICATION CENTRAL INVENTORY SYSTEM

CONTROL OBJECTIVE

Management should ensure that the application has policies, procedures and methods to ensure that all transactions are entered, processed and reported correctly. Management should ensure that application systems are configured and controlled to promote security, integrity, and availability.

EXISTING ENVIRONMENT

The Central Inventory System (CIS) is an online and batch system that allows agencies to maintain records of inventory to comply with the Department's Property Control Division's rules of reporting and processing. Transactions (additions of new inventory items, deletions of inventory items being surplus, and updates of existing inventory items) are primarily entered into CIS online real-time, meaning users' inventory data is updated immediately to reflect the transactions entered. CIS has the ability to utilize an optical scanner to read bar code labels during physical inventory.

The Central Inventory System was implemented in 1998. CIS was utilized by 24 entities (see page 201 for the listing of user agencies).

Department Description of Control: CIS is secured using security software.

Tests Performed: Reviewed granting of security software rights and reviewed the appropriateness of individuals with access to the Department's CIS, and interviewed CIS staff.

Test Results: Access to CIS was controlled through security software (Resource Access Control Facility (RACF)), in addition to CIS' internal security. Users were required to have a properly authorized security software user ID and password to gain access to the operating environment. Once access to the operating environment had been granted, a separate application user ID and password was required to gain access to CIS.

Assignment, authorization, and maintenance of access rights were the responsibility of each agency's security administrator.

No significant exception noted.

Department Description of Control: CIS has internal security in addition to security software.

Tests Performed: Reviewed granting of rights and appropriateness of individuals with access to the Department's CIS.

Test Results: We reviewed 15 individuals with access rights for the Department, noting 6 individuals who no longer needed access rights to CIS. After notification, the Department removed the RACF access rights.

The Department did not have a formal process to ensure access rights were appropriate.

Department Description of Control: Users must have an authorized ID and password to gain access.

Tests Performed: Reviewed ID and password requirements.

Test Results: Security software password change and content requirements were acceptable.

No significant exception noted.

Department Description of Control: Changes to CIS are controlled through the EBAS Methodology.

Tests Performed: Reviewed changes for compliance with EBAS Methodology.

Test Results: During the audit period, CIS had one closed maintenance request. We reviewed the maintenance request, noting it complied with the EBAS Methodology. The EBAS Methodology required maintenance requests to have a completed service request form.

Additionally, we noted there were no major changes to CIS in the past year.

No significant exceptions noted.

Department Description of Control: A Service Request Form is completed for each change.

Tests Performed: Reviewed Service Request Form.

Test results: We reviewed one service request form relating to CIS maintenance request, noting it had been completed.

No significant exception noted.

Department Description of Control: Each change requires approval and testing before implementation.

Tests Performed: Reviewed changes for approval and testing.

Test results: We reviewed one maintenance request, noting it had been approved; however, the maintenance requests selected did not require testing to be conducted.

No significant exception noted.

Department Description of Control: Library Control moves change to production.

Tests Performed: Reviewed Library control move authorizations.

Test results: CIS had one closed maintenance request, which did not require a Library control move authorization.

No significant exception noted.

Department Description of Control: CIS is backed up at varying intervals.

Tests Performed: Reviewed backup schedules.

Test results: Backups were automatically scheduled to be completed daily, weekly and monthly.

No significant exception noted.

Department Description of Control: Backups are maintained at the CCF and an off-site storage location.

Tests Performed: Reviewed backups maintained at the CCF and at the off-site storage location.

Test results: We reviewed the list of backup tapes and identified daily, weekly, and monthly backup tapes. We selected 30 backup tapes from the list and located all the tapes at the CCF or Regional Vault.

No significant exceptions noted.

Department Description of Control: The Department has developed a user manual, the CIS User Manual.

Tests Performed: Reviewed the CIS User Manual.

Test results: The Department had a User Manual, which provided users with guidance on logging into application, adding/deleting transactions and various reports which were available.

No significant exception noted.

Department Description of Control: CIS has several edit checks to alert users of errors.

Tests Performed: Reviewed edit checks of CIS and reviewed agency data.

Test results: Data entered into the system was the responsibility of the user agency. CIS had on-line edit checks to help prevent a user from entering a transaction with invalid data. If an error occurred during data entry, the on-line edit would display a message and prompt the user for correct data. Errors must be corrected before the transaction was accepted.

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 8,133 data records tested were entered properly and complied with date composition standards. During our testing of CIS data, we did not identify any significant weaknesses.

No significant exception noted.

Department Description of Control: The Department generates a Location Balance Report nightly to determine whether transactions processed correctly.

Tests Performed: Reviewed Location Balance Report.

Test results: The Location Balance Report provided information on inventory location codes, number of items with value less than \$100, number of items with value greater than \$100, and items that were capitalized and owned.

No significant exception noted.

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

Tests Performed: Reviewed disaster recovery plans.

Test Results: The Department had not developed a formal disaster recovery plan; however, JCL procedures were in place which would be utilized to recover CIS in the event of a disaster.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should periodically review access rights to CIS and ensure access is appropriate.

Department records listed the following entities as users of the Central Inventory System.

1. Capital Development Board
2. Department of Agriculture
3. Department of Central Management Services
4. Department of Employment Security
5. Department of Human Rights
6. Department of Military Affairs
7. Department of Natural Resources
8. Department of Public Health
9. Department of Transportation
10. Department of Veterans' Affairs
11. Department on Aging
12. Environmental Protection Agency
13. Historic Preservation Agency
14. Illinois Deaf and Hard of Hearing Commission
15. Illinois Educational Labor Relations Board
16. Illinois Law Enforcement Training and Standards Board
17. Illinois Office of the State's Attorneys Appellate Prosecutor
18. Illinois Procurement Policy Board
19. Illinois Violence Prevention Authority
20. Illinois Workers' Compensation Commission
21. Office of Management and Budget
22. Office of the Attorney General
23. Office of the Governor
24. Office of the Lieutenant Governor

This Page Intentionally Left Blank

COMMON APPLICATIONS – ENTERPRISE APPLICATION CENTRAL TIME AND ATTENDANCE SYSTEM

CONTROL OBJECTIVE

Management should ensure that the application has policies, procedures and methods to ensure that all transactions are entered, processed and reported correctly. Management should ensure that application systems are configured and controlled to promote security, integrity, and availability.

EXISTING ENVIRONMENT

The Central Time and Attendance System (CTAS) is an online system that provides a comprehensive system for recording and managing employee benefit time. CTAS transactions are entered online in a real-time environment. CTAS provides for attendance information to be recorded using either the positive or exception method. The positive method of recording daily attendance requires the time keeper to enter or confirm an employee's general attendance information. The exception method assumes that an employee scheduled work time is the correct attendance unless the timekeeper enters something different.

CTAS was implemented in 1992. CTAS was utilized by 31 entities (see page 207 for the list of user agencies).

Department Description of Control: CTAS is secured using security software.

Tests Performed: Reviewed granting of security software rights, reviewed the appropriateness of individuals with access to the Department's CTAS, and interviewed CTAS staff.

Test Results: Access to CTAS was controlled through security software (Resource Access Control Facility (RACF)), in addition to CTAS' internal security. Users were required to have a properly authorized security software user ID and password to gain access to the operating environment. Once access to the operating environment had been granted, a separate application user ID, password, and schedule number were required to gain access to CTAS.

Assignment, authorization, and maintenance of access rights were the responsibility of each agency's security administrator.

No significant exception noted.

Department Description of Control: CTAS has internal security in addition to security software.

Tests Performed: Reviewed granting of rights and appropriateness of individual with access to the Department's CTAS.

Test Results: We reviewed 50 Department staff with access rights to CTAS, noting all appeared appropriate based on job duties.

No significant exception noted.

Department Description of Control: Users must have an authorized ID and password to gain access.

Tests Performed: Reviewed ID and password requirements.

Test Results: Security software password change and content requirements were acceptable.

No significant exception noted.

Department Description of Control: Changes to CTAS are controlled through the EBAS Methodology.

Tests Performed: Reviewed changes for compliance with EBAS Methodology.

Test Results: During the audit period, CTAS had five closed maintenance requests. We reviewed the five requests, noting they complied with the EBAS Methodology. The EBAS Methodology required maintenance requests to have a completed service request form.

Additionally, we noted there were no major changes to CTAS in the past year.

No significant exception noted.

Department Description of Control: A Service Request Form is to be completed for each change.

Tests Performed: Reviewed service request forms.

Test Results: We reviewed five service request forms relating to CTAS maintenance requests, noting they had been completed.

No significant exception noted.

Department Description of Control: Each change requires approval and testing before implementation.

Tests Performed: Reviewed changes for approval and testing.

Test Results: We reviewed five maintenance requests, noting each had been approved; however, the maintenance requests selected did not require testing to be conducted.

No significant exception noted.

Department Description of Control: Library control moves changes to production.

Tests Performed: Reviewed Library control move authorizations.

Test Results: CTAS had five closed requests, of which only one required a Library control move authorization. Our review indicated the move had been properly approved.

No significant exception noted.

Department Description of Control: CTAS is backed up at varying intervals.

Tests Performed: Reviewed backup schedules.

Test Results: Backups were automatically scheduled to be completed daily, weekly and monthly.

No significant exception noted.

Department Description of Control: Backups are maintained at the CCF and an off-site storage location.

Tests Performed: Reviewed backups maintained at the CCF and at the off-site storage location.

Test Results: We reviewed the list of backup tapes and identified daily, weekly, and monthly backup tapes. We selected 30 backup tapes from the list and located all the tapes at the CCF or Regional Vault.

No significant exception noted.

Department Description of Control: CTAS has edit checks to alert users of errors. Transactions with errors will be rejected.

Tests Performed: Reviewed edits of CTAS and reviewed agency data.

Test Results: Data entered into the system was the responsibility of the user agency. CTAS had hundreds of edit checks built into the system to notify the user of any exceptions. The system performed an online edit check and would reject all transactions that did not meet the edit criteria. During the 'close' process, CTAS generated an error report, a reconciliation report, and a file maintenance activity report. All discrepancies were to be reconciled before a 'close' could be finalized.

During our review, we selected two agencies' CTAS data and tested date fields, vacation balances, and the employee identification number for proper input, edits, and compliance with date standards. We determined that the 4,635 data records tested were entered properly and complied with date composition standards. During our testing of CTAS data, we did not identify any significant weaknesses.

No significant exception noted.

Department Description of Control: The CTAS provides online and batch reports that user agencies may use for reconciliation purposes. During the 'close' process, CTAS generates error reports, reconciliation reports, and file maintenance activity reports.

Tests Performed: Reviewed CTAS Manual.

Test Results: Before the agency completed the 'close' process a Pre-Close Report was generated to determine any errors, thus allowing the agency to correct any errors. Once the 'close' process was completed, a Close Report was generated.

No significant exception noted.

Department Description of Control: The CTAS User Manual provides guidance to the user when utilizing the various functions.

Tests Performed: Reviewed the CTAS User Manual.

Test Results: The Department had a User Manual, which provided users with guidance on logging into the application, adding/deleting employees, and the processing and completion of transactions.

No significant exception noted.

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

Tests Performed: Reviewed disaster recovery plans.

Test Results: The Department developed the CTAS Production Database Recovery Instructions, dated May 22, 2000 and the Business Continuity Plan CTAS, dated December 30, 2006.

The Instructions provided steps necessary to recover the CTAS database in the event of a disaster. The Plan identified the Technical Support Staff who was responsible for the recovery of CTAS.

No significant exception noted.

OVERALL CONCLUSION

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

Department records listed the following entities as users of the Central Time and Attendance System.

1. Capital Development Board
2. Department of Agriculture
3. Department of Central Management Services
4. Department of Commerce and Economic Opportunity
5. Department of Financial and Professional Regulation
6. Department of Human Rights
7. Department of Labor
8. Department of Natural Resources (Division of Mines and Minerals)
9. Department of Public Health
10. Department of Revenue
11. Department of Veterans' Affairs
12. Department on Aging
13. Environmental Protection Agency
14. Guardianship and Advocacy Commission
15. Human Rights Commission
16. Illinois Civil Service Commission
17. Illinois Criminal Justice Information Authority
18. Illinois Deaf and Hard of Hearing Commission
19. Illinois Educational Labor Relations Board
20. Illinois Law Enforcement Training and Standards Board
21. Illinois Planning Council on Developmental Disabilities
22. Illinois Procurement Policy Board
23. Illinois Workers' Compensation Commission
24. Office of Management and Budget
25. Office of the Attorney General
26. Office of the Executive Inspector General
27. Office of the Governor
28. Office of the State Appellate Defender
29. Office of the State Fire Marshal
30. Property Tax Appeal Board
31. State Board of Elections

This Page Intentionally Left Blank

APPENDIX A

COMPLEMENTARY USER ORGANIZATION CONTROLS

Users of the State's Central Computer Facility are responsible for complying with prescribed requirements and for using available security mechanisms to protect the security and integrity of their data. During the course of our review, we identified several areas of user agency responsibility that should be reviewed by user agencies and their internal and external auditors.

Disaster contingency plans are needed.

Due to the fact agencies rely on the Department for computing services, they should take steps to reduce the risks associated with disruption or loss. Agencies should:

- Submit a listing of critical applications with all pertinent information to the Department, at least annually.
- Submit formal disaster recovery plans to the Department.
- Ensure all data is backed up and stored off-site.
- Ensure all critical applications are tested at least annually. Additionally, agencies should submit detailed goals and results of the test to the Department.

Available security mechanism should be utilized.

To ensure that controls are functional at the agency level, agencies should:

- Effectively utilize security software features and perform periodic reviews of existing profiles to ensure that access rights are appropriate.
- Formally encourage users to include both alphabetic and non-alphabetic characters in their passwords, to protect the security of their account.
- Examine revoked IDs and delete IDs that are no longer necessary.
- Utilize the Department's password reset utilities for users who are required to have the ability to reset passwords. Powerful attributes should only be assigned to users who need administrative capabilities.

Security and Controls over the Internet should be reviewed.

To enhance security, agencies should:

- Regulate and monitor Internet web-based content by utilizing resources such as Internet content filtering and access logging.
- Develop and implement policies and procedures regarding appropriate Internet usage.
- Prohibit the insecure transmission of confidential or sensitive information across the Internet.
- Ensure the Department is notified of IWIN accounts that need to be deactivated in a timely manner.
- Monitor content transmitted through the IWIN network.

Security of Virtual Machine (VM) systems should be reviewed.

User agencies should review the use of security permissions that permit multi-write capabilities (which may cause data to be corrupted or lost) and have it eliminated from all minidisks where it is not absolutely essential.

Security of Customer Information Control System (CICS) should be reviewed.

We recommend user agencies:

- Coordinate with the Department to assure that automatic time-out settings for their CICS regions provide reasonable protection of the information resources for the agency, while considering their operational needs.
- Ensure their CICS regions are adequately protected using security software, including the use of recommended transaction level security.
- Ensure that powerful CICS commands are adequately restricted.
- Test current version of CICS and coordinate with the Department to update their region to the current version to assure adequate support is maintained.

Security of DataBase 2 (DB2) should be reviewed.

User agencies should provide timely notification to the Department's DB2 Application Support Administrator if the agency DB2 Coordinator changes. In addition, we recommend user agencies assign the usage of the "DB2 Coordinator ID" to a specific person to promote accountability for the use of the ID.

Bills for computer services should be reviewed.

User agencies should monitor the monthly billing to ensure charges are correct. Additionally, all user agencies should submit payment in a timely manner.

Accounting Information Systems (AIS) use should be reviewed.

We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, agencies using AIS should:

- Verify only accurate and authorized data are entered into AIS. It is the agency's responsibility to ensure only properly authorized transactions are entered into the system.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the users and user groups with access to AIS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.

Central Payroll System (CPS) use should be reviewed.

We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, agencies using CPS should:

- Verify only accurate and authorized data are entered into CPS. It is the agency's responsibility to ensure only properly authorized transactions are entered into the system.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the users and user groups with access to CPS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.

- Regularly review those authorized to pick up payroll reports, and inform appropriate CPS personnel of changes timely.
- Retain hardcopy payroll vouchers for at least the 3 most current pay periods, as specified by the CPS User Manual.

Central Inventory System (CIS) use should be reviewed.

We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, agencies using CIS should:

- Verify only accurate and authorized data are entered into CIS. It is the agency's responsibility to ensure only properly authorized transactions are entered into the system.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the users and user groups with access to CIS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.

Central Time and Attendance System (CTAS) use should be reviewed.

We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, agencies using CTAS should:

- Verify only accurate and authorized data are entered into CTAS. It is the agency's responsibility to ensure only properly authorized transactions are entered into the system.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the users and user groups with access to CTAS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up timekeeping reports, and inform appropriate CTAS personnel of changes timely.

Note: Additional information is available to assist user agencies and their internal and external auditors in the review of these complementary controls or other pertinent controls. Please feel free to contact the Office at 217-782-6046 or auditor@mail.state.il.us.

This Page Intentionally Left Blank

APPENDIX B

LIST OF USER AGENCIES

1. Board of Higher Education
2. Capital Development Board
3. Chicago State University
4. Commission on Government Forecasting and Accountability
5. Court of Claims
6. Department of Agriculture
7. Department of Central Management Services
8. Department of Children and Family Services
9. Department of Commerce and Economic Opportunity
10. Department of Corrections
11. Department of Employment Security
12. Department of Financial and Professional Regulation
13. Department of Healthcare and Family Services
14. Department of Human Rights
15. Department of Human Services
16. Department of Juvenile Justice
17. Department of Labor
18. Department of Military Affairs
19. Department of Natural Resources
20. Department of Public Health
21. Department of Revenue
22. Department of Transportation
23. Department of Veterans' Affairs
24. Department on Aging
25. East St. Louis Financial Advisory Authority
26. Eastern Illinois University
27. Emergency Management Agency
28. Environmental Protection Agency
29. Executive Ethics Commission
30. General Assembly Retirement System
31. Governors State University
32. Guardianship and Advocacy Commission
33. Historic Preservation Agency
34. House of Representatives
35. Human Rights Commission
36. Illinois Arts Council
37. Illinois Civil Service Commission
38. Illinois Commerce Commission
39. Illinois Community College Board
40. Illinois Council on Developmental Disabilities
41. Illinois Criminal Justice Information Authority
42. Illinois Deaf and Hard of Hearing Commission
43. Illinois Educational Labor Relations Board
44. Illinois Finance Authority
45. Illinois Housing Development Authority
46. Illinois Labor Relations Board
47. Illinois Law Enforcement Training and Standards Board
48. Illinois Math and Science Academy

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

APPENDIX C

IDENTIFIED DESCRIPTION OF CONTROL DEFICIENCIES

The Department's Description of Control identified several controls that were not accurate based on test work performed.

In addition, we do not express an opinion on control objectives not listed in the description of tests and operating effectiveness section (pages 63 to 207). Specifically, we do not express an opinion on:

- Infrastructure Services-Midrange Services-WinTel,
- Infrastructure Services-Midrange Services-Unix,
- Enterprise Capacity Performance and Storage (midrange environment), and
- Change Management (midrange environment).

The following table is a summary of specific deficiencies (beyond those identified above) noted in the Department's Description of Controls (pages 11 to 62).

Department's Description of Control	Test Results	Report Page
CHIEF OF STAFF-PROCUREMENT		
The Procurement Unit coordinates all Bureau purchase requests and contract renewals including Request for Purchase (RFP), Invitation for Bid (IFB), and Request for Information (RFI) for IT/Telecom items regardless of size or method of procurement that have been approved by management.	The Procurement Unit coordinated contract renewals and RFPs. The Bureau of Strategic Sourcing and Procurement (BOSSAP) coordinated IFBs and RFIs.	65
AGENCY RELATIONS		
Quarterly the AR Unit is rated via the Bureau's Overall Satisfaction Survey, sent out by the Service Level Management Team.	The Bureau's Overall Satisfaction Survey was not sent out.	77
BUSINESS ENTERPRISE APPLICATIONS - PERSONAL INFORMATION MANAGEMENT (PIM)		
The end user email account is secured using an aggressive password scheme. The password policy can be found in the PIM Policies document.	The Policies had not been approved and finalized.	91
SERVICE MANAGEMENT		
The software utilities used in this unit to produce and handle the reports and documents include SharePoint, Microsoft Project, Excel, Word, and Visio.	The utilities were not in place.	101

Department's Description of Control	Test Results	Report Page
WEB SERVICES AND LAN APPLICATION DEVELOPMENT		
Enterprise Content Management provides the capabilities to scan, import, store, secure, index, retrieve and route document-based information.	Still in development, the full functionality of Content Management was not in place.	105
RISK MANAGEMENT - RECOVERY SERVICES		
The following contingency plans address restoration of various client environments: <ul style="list-style-type: none"> ▪ Continuity Methodology, ▪ Recovery Activation Plan, ▪ Network Services, Recovery Activation Plan. 	The Network Services, Recovery Activation Plan had not been developed.	141
SERVICE ENGINEERING – SERVICE LEVEL MANAGEMENT		
SLAs are subject to discussion and changes on a quarterly basis.	The process to review SLAs on a quarterly basis had not been implemented.	164
Service metric reviews between the Department/Bureau and agencies are scheduled and conducted.	Reviews with the agencies were not conducted.	164
PHYSICAL SECURITY - BUREAU OF PROPERTY MANAGEMENT (BOPM)		
The Department has contracted with janitorial services to perform duties on a daily, weekly, and monthly basis. The contracts outline the duties and timing of the duties to be performed. The Department conducts background checks and training for each janitorial employee.	The Department did not conduct background checks or provide training for janitorial employees.	180
The Department maintains a master contract with E.L.A. Security, Inc. This contract states the agencies, which utilize E.L.A. Security, Inc. guards, are required to provide a Post Order Manual for the guards at each location. This is to ensure communication between the guards and their respective duties at each facility.	The Post Order Manual had not been created.	181

APPENDIX D

ACRONYM GLOSSARY

AFSCME – American Federation of State, County and Municipal Employees

AGR – Department of Agriculture

AIS – Accounting Information System

AR – Agency Relations

ARB – Architecture Rationalization Board

ARPS – Accounts Receivable Posting System

ASD – Application System Development

BAS – Billing Allocation System

BARCS – Billing and Accounting Receivable Cash Management System

BCCS – Bureau of Communication and Computer Services

BOSSAP – Bureau of Strategic Sourcing and Procurement

BPE – Business Process Engineering

BUM – Business Unit Manager

Bureau – Bureau of Communication and Computer Services

CAC – Change Advisory Council

CCC – Central Communications Center

CCF – Central Computer Facility

CEO – Department of Commerce and Economic Opportunity

CFO – Chief Financial Officer

CICS – Customer Information Control System

CIO – Chief Information Officer

CIS – Central Inventory System

CMC – Customer Management Center

CMS – Central Management Services

COO – Chief Operating Officer

COOP – Department’s Continuity of Operations Plan

CPO – Chief Procurement Officer

CPU – Central Processing Unit

CPS – Central Payroll System

CRF – Communication Revolving Fund

CSC – Customer Solution Center

CSD – CICS System Definition File

CSS2 – Communication Systems Specialist 2

CTAS – Central Time and Attendance System

DASD – Direct Access Storage Device

DB2 – DataBase 2

DCMS – Department of Central Management Services

Department – Department of Central Management Services

DES – Department of Employment Security

DHS – Department of Human Services

DNR – Department of Natural Resources

DNS – Domain Name Service

DOT – Illinois Department of Transportation

DP – Data Processing

DPH – Department of Public Health

EA&S – Enterprise Architecture and Strategy

EBAS – Enterprise Business Application Services

ECPS – Enterprise Capacity Performance and Storage

EPA – Illinois Environmental Protection Agency

EPM – Enterprise Project Management

EPMO – Enterprise Program Management Office

ESR – Enterprise Service Request

EUC – End User Computing

FCIAA – Fiscal Control and Internal Auditing Act

FIPS – Federal Information Processing Standards

FPR – Department of Financial and Professional Regulations

FY – Fiscal Year

GIMS – Transaction type for the Information Management System

GRF – General Revenue Fund

HFS – Department of Health and Family Services

HR – Human Resources

HSM – Hierarchical Storage Management

H/V – Hirsch Velocity

IBiS – Internet Billing System

IBM – International Business Machines

ICN – Illinois Century Network

ID – Identification

IFB – Invitation for Bid

ILCS – Illinois Compiled Statutes

IMS – Information Management System

INFO – Information

INFOMAN – Information Management for z/OS

I/O – Input/Output

IOC – Illinois Office of the Comptroller

IOIA – Illinois Office of Internal Audit

IQAM – Information Quality and Assurance Methods

IRB – Investment Review Board

ISD – Information Services Division

ISP – Illinois State Police

IT – Information Technology

ITG – Information technology Governance

ITSM – Information Technology Service Management

IWAS – Illinois Web Accessibility Standards

IWIN – Illinois Wireless Information Network

JCL – Job Control Language

LAN – Local Area Network

M&P – Methods and Procedures

MAS90 – Name of application utilized by Business Services

MDC – Mobile Data Computer

MONIES – Management of Network Income Expense Services System

MPLS – MultiProtocol Label Switching

MRB – Management Review Board

MRTG – Multi-Router Traffic Graph

NOMAD – Name of application utilized on VM

OA – Office Automation

OMB – Office of Management and Budget

PAR – Project Assessment Requirements

PARS – Production Authorization Release System

PBC – Procurement Business Case

PIM – Program Information Management

PM – Project Management

POP – Point Of Presence

PRB – Policy Review Board

PRV – Provisioning Request

PSR – Paging Service Request

QA – Quality Assurance

RACF – Resource Access Control Facility

RAD – Rapid Application Development

REV – Department of Revenue

RFC – Request for Change

RFI – Request for Information

RFP – Request for Proposal

RM – Risk Management

RMF – Resource Management Facility

RTC – Regional technology Center

SAMS – Statewide Accounting Management System

SCAS – Service Center Allocation System

SLA – Service Level Agreement

SMF – System Management Facility

SMS – System Management Storage

SNA – Systems Network Architecture

SOS – Secretary of State

SPM – Strategic Portfolio Management

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

TIMS – Transaction type for the Information Management System

TMS – Tape Management System

TRM – Technical Reference Model

TSO – Time Sharing Option

TSR – Telecommunications Service Request

TSU – Technical Safeguards Unit

TTS – Transient Tape System

UPS – Uninterruptible Power Supply

URL – Universal Resource Locator

VM – Virtual Machine

VOIP – Voice Over Internet Protocol

VOTS – Voice Teleconferencing Services

WAN – Wide Area Network

WSR – Wireless Service Request

z/OS – Zero Downtime Operating System

z/VM – Zero Downtime Virtual Machine