THIRD PARTY REVIEW

Department of Central Management Services
Bureau of Communication and
Computer Services

July 2006

TABLE OF CONTENTS

REPORT DIGEST

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES BUREAU OF COMMUNICATION AND COMPUTER SERVICES

THIRD PARTY REVIEW
For the Year Ended:
June 30, 2006

Release Date:
July 12, 2006

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

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

This Report Digest and Full Report are also available on the worldwide web at http://www.state.il.us/auditor

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 98 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 CCF 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 3, 2006 to May 26, 2006. 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	2006
Mainframes	3 Units Configured as 10 Production Systems and 4 Test Systems 1 Unit Configured for Disaster Recovery
Services/Workload	Impact Printing – 3.79 Million Lines per Month Laser Printing – 16 Million Pages per Month
State Agency Users	98
Bureau Employees	2003 -- 307 2004 -- 303 2005 -- 775* 2006 -- 777 * Increase due to IT consolidation into the Department per Public Act 93-25
Historical Growth Trend**	2003 -- 2,700 -- MIPS 2004 -- 3,614 -- MIPS 2005 -- 3,217 -- MIPS 2006 -- 3,217 -- 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 Deputy Director/Bureau Manager: Jay Carlson (7/1/2005 to 11/7/2005) Currently: Director: Paul Campbell Deputy Director/Bureau Manager: Tony Daniels (11/8/2005 to present)

REPORT SUMMARY

We identified two reportable conditions for which we could not obtain reasonable assurance over the controls.

Change Management Process

Risk of unauthorized and not suitably tested changes to systems

The Department did not follow the approved change management process it implemented in 2004, has not updated its change management policies and procedures, and has not developed a mechanism to ensure all changes follow the approved process.

In addition, the approved change management process has not been implemented across all platforms. As a result, the current change management process lacks consistency and does not ensure all changes are sufficiently controlled.

The lack of compliance with the approved change management process leaves the Department exposed to the risk of unauthorized and not suitably tested changes to systems. The Department should update policies and procedures to govern the approved change management process and ensure compliance. (page 6)

The Department concurred with our recommendation. Department officials stated the Bureau is in the process of implementing a formal change management framework.

Security Framework

Security framework not sufficiently developed or implemented

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

The security framework has not been sufficiently developed or implemented to ensure security is adequately addressed from a Statewide or Departmental perspective.

The Department had not updated the various security-related documents since at least February 2003. As a result, the documents do not reflect the current technological environment, and have not been updated to 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. In addition, the Department should formally approve and implement a comprehensive security administration framework, and ensure sufficient resources are allocated to support the framework. (pages 6-7)

The Department concurred with our recommendation. Department officials stated a Policy Review Board will establish

updated enterprise policies and procedures that address the legacy and consolidated environments.

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

Disaster Contingency Planning

State lacks preparedness

Although the Department has 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 plans are outdated, do not adequately address regional recovery facilities, and have not been adequately tested to determine if the plans would effectively guide recovery efforts in the event of a disaster.

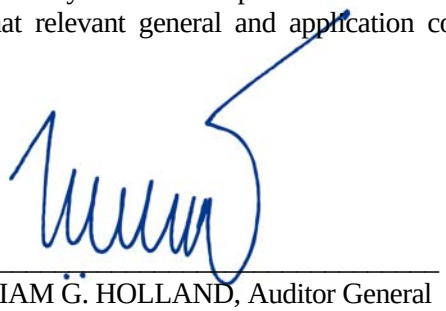
The State is placing great reliance on the Department's ability to provide data processing and network services in the event of a disaster. As such, comprehensive and thoroughly tested disaster contingency plans are an essential component of recovery efforts.

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 7-8)

The Department concurred with our recommendation. Department officials stated a comprehensive exercise of all Category One applications is scheduled for July 2006.

AUDITORS' OPINION

With the exception of the two reportable conditions 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:ap

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 organization's internal control structure 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 organizations applied the controls contemplated in the design of the Department's controls; and (3) such controls had been placed in operation as of May 26, 2006. Our review, started in July 2005 and primarily performed between January 3, 2006 through May 26, 2006, 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 considered necessary under the circumstances to obtain a reasonable basis for rendering our opinion.

The accompanying description states the Department uses two separate procedures relating to the change management process: the mainframe and all other environments. Based on inquiries of staff and inspection of activities, we determined the process is not employed.

Additionally, the description states the Department has several security policies relating to the IT environment. Based on inquires of staff and inspection of activities, we determined those policies do not address the current IT environment.

In our opinion, except for the matters referred to in the preceding paragraphs, the accompanying description of the aforementioned systems and procedures presents fairly, in all material respects, the relevant aspects of the Department's controls that had been placed in operation as of May 26, 2006. 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 organizations 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 3, 2006 through May 26, 2006. 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 organizations and to their auditors to be taken into consideration, along with information about the internal control at user organizations, when making an assessment of control risk for user organizations. In our opinion, 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 3, 2006 through May 26, 2006. However, the scope of our engagement did not include tests to determine whether control objectives at the consolidated agencies were achieved.

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

The description of controls at the Department is as of May 26, 2006, and information about tests of the operating effectiveness of specified controls covers the period from January 3, 2006 through May 26, 2006. 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 Lovejoy, CPA, CISA
Information Systems Audit Manager

May 26, 2006

THIRD PARTY REVIEW

Department of Central Management Services
Bureau of Communication and
Computer Services

July 2006

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 98 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.

Public Act 93-25 authorized the Department of Central Management Services to consolidate Information Technology (IT) functions of State government. In order for the Department to carry out the consolidation activities, an IT Rationalization project was initiated. The IT Rationalization/Consolidation project has been a primary focus of the Department as it consolidates IT functions.

In conjunction with the consolidation, the Department has assumed the responsibility for the IT environments of 11 significant State agencies. We noted the consolidation has reallocated resources, functions, and personnel from the historical practices and controls, which has led to some of the deficiencies outlined within the report. We also noted the Department failed to assure the roles and responsibilities for key functions and assigned personnel were clearly defined and adequately communicated, which appears to have resulted in confusion among personnel.

The CCF 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. 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.

Reportable Conditions

We identified several control deficiencies that appear in pages 29 through 82; in addition, we noted two issues for which we could not obtain reasonable assurance over the controls.

Change Management Process

The Department did not follow the approved change management process it implemented in 2004, has not updated its change management policies and procedures, and has not developed a mechanism to ensure all changes follow the approved process.

In addition, the approved change management process has not been implemented across all platforms. As a result, the current change management process lacks consistency and does not ensure all changes are sufficiently controlled.

The lack of compliance with the approved change management process leaves the Department exposed to the risk of unauthorized and not suitably tested changes to systems. The Department should update policies and procedures to govern the approved change management process and ensure compliance. (See pages 47-48 for additional information)

Department Response

The Department concurs with the recommendation. The Bureau is in the process of implementing a formal change management framework. The Enterprise Change Management team is currently updating and implementing policies and procedures to govern changes to legacy and consolidated systems. The Enterprise Change Management solution will assure consistency across all platforms as well as the appropriate governance and monitoring of all requests.

Security Framework

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

The security framework has not been sufficiently developed or implemented to ensure security is adequately addressed from a Statewide or Departmental perspective.

The Department had not updated the various security-related documents since at least February 2003. As a result, the documents do not reflect the current technological environment, and have not been updated to 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. In addition, the Department should formally approve and implement a comprehensive security administration framework, and ensure sufficient resources are allocated to support the framework. (See pages 49-53 for additional information)

Department Response

The Department concurs with the recommendations. The Bureau is acting accordingly to address the controls for security administration.

The Bureau is implementing a Policy Review Board (PRB) to establish updated enterprise policies and procedures that address the legacy and consolidated environments. The PRB will coordinate the development, review, approval, publishing, and maintenance of policies, procedures, and standards related to information technology (IT) and telecommunication (telecom) assets and services.

As part of the consolidation initiative, the Bureau is redefining the organizational structure to better define roles and responsibilities and improve communications among the shared services teams.

Other Control Deficiencies

Although not covered under audit standards as a reportable condition, 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 has 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 plans are outdated, do not adequately address regional recovery facilities, and have not been adequately tested to determine if the plans would effectively guide recovery efforts in the event of a disaster.

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 41-43 for additional information)

Department Response

The Department concurs with the recommendations. A comprehensive exercise of all Category One applications is scheduled for July 2006. Ongoing testing is to continue at the Harris Computing Facility (HCF) in a manner consistent with guiding recovery efforts in the event of an actual disaster.

Contingency planning is being project-managed to leverage involvement with key customer stakeholders. Additionally, recovery activation plans and procedures are being updated to reflect the new shared services environment.

The Bureau continues to pursue a permanent alternate regional recovery site; however, in the near term interim risk mitigation solutions will be implemented using the existing environments.

The Department responses were provided on June 23, 2006, by Tony Daniels, 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 9 through 28) consists of text provided by the Department of Central Management Services.

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

The Bureau has six Divisions, which are further broken into subdivisions:

- Chief of Staff
    - Workforce Development and Logistics
    - Procurement
- Executive Program Management Office
- Agency Relations
- Business Services
- Infrastructure and Applications
    - Network Services
    - Enterprise Architecture and Strategy
    - Common Applications
    - Infrastructure Services
    - Risk Management
- Customer and Account Management
    - Customer Service Center
    - ISP Radio
    - Service Delivery

Chief of Staff

The Chief of Staff handles high-profile projects, special requests and assignments for the Bureau. In addition, the Chief of Staff oversees the Bureau's Procurement Unit, which is responsible for all procurement activities, and the Workforce Development and Logistics Unit, which oversees employee training and development functions, moves, and liaisons with the Department's Bureau of Personnel for personnel matters.

Executive Program Management Office

The Executive Program Management Office (EPMO) is responsible for maintaining and managing the Department project portfolio and providing project management support. The EPMO also develops and implements consistent and standardized project management processes. They directly manage large, complex projects at the direction of Department management.

Agency Relations

Agency Relations (AR) is tasked with providing customer service to agencies who receive services from the Department. Their number one goal is to know and understand the customer's needs.

Under the direction of the Agency Relations Manager, AR staff are advocates for the agency in:

- Resolving issues;
- Assisting with the governance process; and
- Proactively informing agencies of upcoming initiatives and project status.

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) and the Communications Revolving Fund (CRF). The Bureau operates these two internal service funds, which include billing operations.

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, secure cards, 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. 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.

During the current fiscal year the Department will be implementing a new billing system, EMS.11.

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.

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 six sections.

The ICN obtains public Internet services from the following Internet providers: Sprint; WilTel; 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 - Customer Management Center (CMC)

The CMC is responsible for all Tier 2 trouble resolutions, network surveillance and ongoing technical support. The CMC is operational 24x7, and handles the after hours provisioning calls of the Customer Service Center (CSC). The CMC is located in the JRTC in Chicago. The CMC utilizes Remedy to record tickets.

All escalated tickets to the CMC are done on the managerial level. Once escalated to the CMC it becomes the responsibility of the CMC to continue managing the vendor, customer and any other applicable party. At 5:00 PM the CSC sends a detailed email to the CMC with turnover detailing the tickets and issues that need to be managed during the off-hours. In return, the CMC sends as equally detailed email to the CSC at 8:00 AM of every business day identifying what issues need their attention. Both the CMC and CSC escalate all T1 and circuits tickets hourly to vendor management. The CSC and CMC escalate every two hours on Illinois Lottery or other DS0 services.

The CMC is also responsible for Change Management. Once a planned event is scheduled by the Network Operations team an email is sent to the CMC identifying the requirement for the work. In addition, event timeframe, affected customers, outage window as well as other critical information is provided. The CMC gathers all this information and engages the Department's Change Management process. Affected users are notified and preparations are made based on the severity of the downtime identified.

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. 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 serve 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 Network Services.

Network Operations 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. Network changes to routers, switches and firewalls are managed in the ICN Remedy system as well as the Department's Change Management System.

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, filtering and the School to Home system. WAN services support includes installation, configuration, maintenance and support.

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

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

Transmissions are sent from the users' Mobile Data Computer (MDC), equipped with the client software Premier MDC, to the nearest cellular tower equipped with CDPD equipment via a dedicated channel. The Department has a contract with Verizon Wireless (Verizon) to provide cellular towers throughout the State, as well as with Motorola to provide the software utilized by the IWIN network. Once the cellular tower has received the transmission from the user's MDC, the transmission is then forwarded to a Verizon -owned and -operated messaging switch. From the messaging switch, the transmission is forwarded to one of the Department's redundant

Premier MDC Servers and then to the Department's network for access to the appropriate data. Redundant routers, maintained by SBC Ameritech, connect the Department's Premier MDC Servers to the Verizon Network.

Network Services - Field Operations

Field Operations is responsible for maintaining the nine Regional Technology Centers and assisting Network Operations in POP site maintenance. Responsibilities are varied and include circuit termination, VOIP, video conferencing, wireless, fiber, UPS, and for dispatching employees for repairs at POP and constituent sites. Field Operations performs tier 2 and 3 technical support for the CMC and directly to constituents.

Field Operations is responsible for providing a variety of services to constituents. Functions include customer consultation, customer and distribution router configuration, ongoing maintenance, head-end router installations/troubleshooting, making equipment and connectivity recommendations, performing equipment installation/recovery at all customer sites, and the provisioning for new circuits, moves and changes. Remedy is used for trouble ticketing and problem tracking.

Field Operations uses both centralized and local management tools to maintain a variety of work flow tasks. These include constituent and POP site equipment inventory, maintaining a database of all constituent, circuit and inventory records, and performing sales, billing, and rollout and support for services including filtering, quality of service, IP video, DNS, Erate, School to Home, IP addressing, bandwidth monitoring (MRTG), collocation and multicast. Local DNS servers and records, and circuit monitoring using What's Up are also managed.

Field Operations uses the Department's Change Management procedures to maintain control for all POP site work, distribution and customer router maintenance, UPS/power maintenance, and any work that will, or could, cause any interruption of service. All work is documented and tracked using Remedy trouble tickets.

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 merged agencies LAN network, which includes: firewalls, routers, switches, hubs, IDS and wireless switches. Until the physical consolidation of the merged agencies, the LAN network infrastructures are being maintained under the respectful agencies policies.

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.

LAN services backs up firewall configurations to a files, which is then included as a part of the normal LAN backup schedule. Incremental backups are performed nightly and full backups are preformed weekly then rotated off-site.

Configuration changes are managed through the Department's change management and the network services change configuration policies.

Policies are currently being developed for the LAN networking services group. The group is not fully implemented and in the process of transitioning personnel and thus will require rewriting of policies and procedures.

Network Services - Architecture and Planning

The Architecture and Planning section works closely with the Design and Security group to research new technologies, develop new product offerings and develop technical specification for IFB, RFI and RFP's. Additionally this section works closely with executive management on enterprise strategy.

Enterprise Architecture and Strategy

The Department has established an IT and Telecommunications Governance model to help oversee rationalization, standardization, centralization and consolidation efforts. The Governance model is a set of political processes, driven by business and technology principles to ensure that IT investments meet the following objectives:

- Alignment of IT/Telecom with the Enterprise goals and realization of the promised benefits;
- Use of IT/Telecom to enable the enterprise by taking advantage of opportunities;
- Optimize use of IT/Telecom resources; and
- Management of IT/Telecom-related risks.

The Architecture Rationalization Board (ARB) 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 assure alignment of the IT portfolio, and adherence to standards concerning the deployment of IT and Telecom. It is not intended as a review process to challenge or critique Agency direction. The goal is to assure that Agency initiatives are aligned with the State of Illinois IT Master Plan, and that the resultant products conform to established IT Standards and architecture."

The Enterprise Architecture and Strategy (EA&S) 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 Executive Team and the ARB, EA&S help create the IT Strategy and Enterprise Architecture vision, develop standards and reference architectures, create IT transition plans, and provide assistance to the central IT organization."

Common Applications

The Department's Infrastructure and Applications Division is responsible for the development of computer systems, which are available for use by user agencies and by the Department.

The Department has developed the Application System Development Methodology (Methodology), and the Standards and Documentation Requirements guide new system developments and modifications to existing systems. The Methodology provides a structured process for the design, development and implementation of new systems, enhancements,

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 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 Department established a Standards Committee to review and approve changes to the Methodology and the Standards and Documentation Requirements.

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

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

The Department's Methodology documents user involvement in all four 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 questionnaire may be used in the fourth phase.

The Department has developed a Quality Assurance Team to monitor and verify that projects adhere to the Methodology. The QA Review Procedural Manual (Manual) provides guidance to Quality Assurance staff for each phase of a development/modification. In addition to the Manual, Quality Assurance utilizes a checklist to identify required tasks for each project.

Library Control is responsible for all mainframe movement of programs in a production library. The Program Library Procedures provide guidance for ensuring new programs or modifications are documented and approved before production moves are performed. A Library Control Form must be completed and approved before a move is made.

Common Applications-Enterprise Applications

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

- Accounting Information System (AIS),
- Central Inventory System (CIS),

- Central Payroll System (CPS), 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 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 Payroll System (CPS)

CPS is an online and batch system that standardizes payroll procedures for State agencies. CPS enables State agencies to maintain automated pay records and provides 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).

The Department has developed a user manual, the CPS 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. CPS has online edit checks and corresponding messages which are displayed online when an error occurs. The error must be corrected before finalization of the transaction. The Department has procedures in place to handle errors that occur during processing.

For each pay period there are six standard reports that are printed and provided to agencies. The reports are printed at the Central Computer Facility for agency pickup. Twice a year agencies are requested to update the Tape, Print and Diskette Authorization Listing. Individuals must be listed in order to pick up reports. Retention of the 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 Time And Attendance System (CTAS)

CTAS is an online system used to maintain current 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 CPS.

The Department has developed a user manual, the CTAS 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. CTAS has edit checks to alert users of errors. Transaction 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.

Infrastructure Services - Recovery Services

The Department is mandated to provide computing services to agencies of the State of Illinois. In the event a disaster, the Department is to provide disaster recovery service in order to minimize the risk of disrupted services or loss of resources.

The Department has compiled several contingency plans for the restoration of its various environments:

- State of Illinois, DCMS, BCCS, Risk Management, Continuity Methodology-Effective January 3, 2005,
- State of Illinois, DCMS, BCCS, ISD, Risk Management, Recovery Activation Plan-Effective December 20, 2004,
- State of Illinois, DCMS, BCCS, Infrastructure Services, Recovery Activation Plan-Effective August 11, 2004, and
- State of Illinois, DCMS, BCCS, Network Services, Recovery Activation Plan-Effective April 11, 2002.

The Department has arranged for satellite facilities in the Springfield area for providing disaster recovery services. The Department's satellite facilities are available to any State agency for recovery purposes. It is the responsibility of the State agency to contact the Department for usage of a satellite facility. In addition, the Department has contracted with a disaster recovery service provider for out-of-state recovery locations, in the event of a regional disaster.

The Department conducts testing at the out-of-state recovery locations annually. Additionally, testing is conducted at the Department's satellite locations. State agencies may conduct testing at any of the Department's satellite locations.

The Department maintains a Statewide Critical Application Listing based on information received from State agencies. State agencies are 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 Services (Category Two)-Resources that directly impact the well being of Illinois citizens;
- Non-Welfare Human Services (Category Three)-A human service resource that directly impacts the welfare of Illinois citizens;
- Administrative State Functions & Processes (Category Four)-Resources that support the administration of state processes; and
- Support of Specific Agency Functions & Processes (Category Five)-Resources related to the maintenance of a specific agency function or a process.

In the event of a regional disaster the Department will only recovery Category One applications for those State agencies that have met the requirements. State agencies with Category One applications are required to conduct testing at one of the Department's satellite facilities on an annual basis. Additionally, the State agencies are to provide the Department with a copy of their

disaster recovery plans and submit results of their annual tests.

The Department conducts nightly backups of its environment. State agencies' data residing on the Department's mainframe are backed up with the Department's nightly cycle. The Department utilizes a regional off-site storage facility for storage of critical information.

The Department has developed procedures for the restart and recovery of applications and systems. Restart and recoveries may occur for various reasons other than a disaster, such as hardware failure, new maintenance levels, new software releases, and job failures. Departmental staff are continuously updating and training in regards to the procedures.

Infrastructure Services-Midrange Services-WinTel

WinTel Services is responsible for the configuration and monitoring of the Department's Local Area Network. Additionally, this group is responsible for the merged agencies' LANs. Until the physical consolidation of the merged agencies, the LAN network infrastructures are being maintained under the respectful agencies policies.

WinTel Services are responsible for the backup of the servers. Incremental backups are performed nightly and full backups are preformed weekly then rotated off-site.

Configuration changes are managed through the Department's change management process.

Policies are currently being developed for the WinTel services group. The group is not fully implemented and in the process of transitioning personnel and thus will require rewriting of policies and procedures.

Infrastructure Services-Midrange Services-Unix

The Unix Services Group is responsible for the configuration and monitoring of the Department's Unix environment. Additionally, this group is responsible for the merged agencies Unix servers. Until the physical consolidation of the merged agencies, the infrastructures are being maintained under the respectful agencies policies.

The Unix Services Group is responsible for the backups. Incremental backups are performed nightly and full backups are preformed weekly then rotated off-site.

Configuration changes are managed through the Department's change management process.

Policies are currently being developed for the Unix Service Group. The Group is not fully implemented and in the process of transitioning personnel and thus will require rewriting of policies and procedures.

Infrastructure Services - Change Control

The Department currently has two separate processes relating to the change management process; the mainframe environment; and all other environments.

The Data Processing Guide and the Problem/Change Management System procedures provide characteristics and guidelines for mainframe changes as well as procedures for emergency mainframe change requests. Emergency changes do not adhere to the normal change procedures since emergency changes require immediate implementation and have unique characteristics.

All mainframe change requests are assessed by each technical area to determine any adverse issues. The policies and procedures list the change management testing levels, scope of tests, and the extent of testing required for each level. Due to the various types of changes, each section throughout the Bureau has its own policy/procedure for testing and maintaining documentation. Each section manager determines the method, extent, and retention period of testing.

The Change Management Database is used to track all changes that do not relate to the Department's mainframe environment. As part of the Enterprise Wide Change Management Solution Project the Department is developing policies and procedures.

The change process is initiated by completing a Change Management Request in the Change Management System. The Change Advisory Committee meets weekly to review changes requested. Request for change documents are reviewed and approved or denied. Approved requests are scheduled to be completed on their Estimated Implementation Date. Change requests that are not approved may be modified, rescheduled or more fully justified and brought back before the Change Advisory Committee.

Infrastructure Services - Data Center Operations

The mission of the Command Center is to provide continuous monitoring and operation of the Department'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. The monitoring of systems is divided among the operators.

The Command Center is responsible for documenting all daily actions and events that 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 Department maintains several reports that record the Command Center activities. The following reports provide a complete record of all operator actions: SYSLOG, Shift Change Checklist, Telephone Report, Weekly Telephone Summary, and the Daily Shift Report. In addition, the Department utilizes Infoman, a management tool, to record and monitor the progress of problem resolutions.

Additionally, the Department 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.
- Command Center Telephone Calls and Print Shop Report - reflects the number of calls received and the volume of printing.

Infrastructure Services - Systems Programming

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 Department utilizes security software to secure libraries, protect resources, and datasets in the z/OS environment. Additionally, the System Management Facility secures the necessary documentation of the activity in the installation.

System changes follow the Department's Info Change and Problem Management procedures. There are three types of changes that may occur to the z/OS environment: 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.

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.

User agencies must go through the Department to submit and obtain a VM User ID. User agencies are assigned IDs with the most restrictive security rights. The VM directory, which contains information regarding user IDs, mini-disk size and location, and operating functions, is restricted.

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 user and a password to verify the user's identity. The Department maintains a log of all access attempts, which is used to monitor unauthorized access attempts and identify areas of weakness. User agencies are responsible for protecting their own programs and data.

The Department has appointed staff with primary responsibility for the implementation and administration of the security software. The Department has an informal procedure in place for the monitoring of security violations. The Data Security Administrator reviews violations and select violation reports are distributed to users requesting explanations and are required to be returned with an explanation.

Infrastructure Services - Database Management

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 and the Department's off-site location.

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 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. DB2 internal security verifies access rights to specific data. The Department authorizes one user ID at each user 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 monitor specific application problems when users call. System performance is monitored on a continuous basis. The Department's Information Management System is utilized to report and document problems.

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.

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

- **Level One** – The Department supports only the CICS software. The user agency is responsible for all security for their user-owned CICS regions.
- **Level Two** – The Department supports the CICS software, and maintains CICS System Definition File (CSD)/table definitions for the user agency. 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.

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.

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." Currently, there are three production IMS regions with 10+ testing regions.

Infrastructure Services - 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 "Library Services Vault Transmittal Procedures" outline the procedures to be conducted during the movement of media. The user agency is responsible for sending a request for movement of their media. The Tape Management System is utilized to track and record the location of media.

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.

Risk Management

The Department's Central Computer Facility was built in 1980, and was designed to meet the State's data processing needs. The Central Computer Facility is monitored 24 hours a day, 7 days a week. Access is restricted at all times.

The Department has several security policies relating to information technology:

- CMS Policy Manual (each section is dated);
    - CMS Information Technology Security Policy (dated April 26, 2002) included as Chapter 4, Section 3 of the CMS 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); and
- CMS LAN Office Systems Procedures Guide (dated February 2003).

Due to the IT Rationalization project, the Department is developing enterprise wide security policies.

The Department's Regional Offices, the Communications Building, the Business Services Building, Benefits Building and the Central Computer Facility each have Facility Managers.

The Department utilizes an access card system to provide control over access to many of its facilities. The system's readers are proximity readers that control and log the use of all access cards throughout the day at the Central Computer Facility, Communications Building, the Benefits Building, and the Business Services Building.

The Statewide Information Security Policy requires all employees, visitors, vendors/contractors, and State agency representatives to be assigned an access card with appropriate access rights. Requests for cardkeys are submitted to the Risk Management Division for approval. An individual's access rights are based on their job duties. Visitors and employees who forget their access card are required to sign-in and register at the guard's desk.

The Department has installed a fire suppression and detection system (System) at the Central Computer Facility. The System is approved by the Underwriters Laboratory, and utilizes an environmentally friendly gaseous agent. Additionally, 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 each have fire detection and suppression systems, smoke detectors and fire extinguishers.

The Department has contracted with a janitorial service to perform duties on a daily, weekly, and monthly basis. The contract outlines the duties and timing of the duties to be performed. The janitorial employees are granted access to all areas throughout the facilities. The Department conducts background checks and training for each janitorial employee.

Customer Account Management

Customer Solution Center (CSC)

The CSC is responsible for Tier I maintenance and provisioning of voice, video, data, and wireless systems and services. The CSC is operational from 8am to 5pm Monday through Friday, excluding State holidays. During non-operational hours, the Customer Management Center is responsible for the service desk calls. Remedy is utilized to track tickets. The CCF Command Center is responsible for mainframe and PKI calls and after-hour IT calls. The CCF Command Center utilizes InfoMan to track tickets.

The Department has converted six of twelve agencies (CMS, EPA, REV, DCEO, DNR, AG) to the Remedy ticketing system as part of the enterprise wide service desk rollout. The remaining six agencies (DFPR, DES, DOT, DPH, HFS and DHS) are targeted to convert within the current fiscal year. During the next fiscal year, the Department plans to implement standard service desk methods and procedures across all twelve agencies service desks, physically relocate the staff to a single location within Springfield and Chicago, and to begin cross training among the staff dedicated to a specific agency. As part of the physical consolidation, all Tier 1 IT support calls will be directed through the CSC including PKI, which is currently handled by the CCF Command Center.

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) form. Paging requests require a Paging Service Request (PSR) form. IWIN requests require a Wireless Service Request (WSR) form.

The Department has developed procedures for telecommunication changes, as documented in the CSC Methods & Procedures documents and Workflow documents. These documents are available on a shared network drive for use by all CSC staff.

User agencies are provided with the instructions for completing the telecommunications request forms and are provided guidance if the forms are incorrectly completed. When a change is needed to a user telecommunications system, the user will request the change.

Changes to the data communications equipment include moving, adding, or changing data circuits, modems, and routers while changes to voice communications include moving voice lines, adding voice mail, installing new lines, etc. Each agency has a designated person that is responsible for approving the telecommunications requests. The provisioning process for telecommunications equipment and services is documented in the Methods and Procedures and Workflow documents. Network Services assists with the review of TDRs and determines what type of equipment or facilities an agency will receive for all requests for new service, MAC (move, add, change) requests, requests for speed change, requests for addition of equipment only, and requests for Timeplex changes.

The MONIES system tracks all ordered and installed facilities and telecommunications equipment. The system does not track an item's cost but does provide location information along with user name, tag number, serial number, au code, vendor description, catalog description and model description.

Data equipment is received either by the Department at the Springfield office or at the node location, depending upon the size of the item while voice equipment is sent directly to the site. New data entries in MONIES for data communications equipment are uploaded into the Central Inventory System (CIS) Suspense File, nightly by a batch job. Before the telecommunication item's invoice is sent to Accounting for processing and entry into CIS, the Property Control Form (PCF) is filled out; the item is tagged for property control, and is entered into the MONIES system for inventory management.

When a telecommunications order is completed (the equipment is installed or picked up), the MONIES system inventory is updated. Anytime a piece of equipment moves from a location, an order must be approved thru the approval process and entered into the MONIES system.

Telecommunications equipment listed in MONIES is reconciled to the listed equipment in CIS annually. Discrepancies are reported to management and investigated. Appropriate action is then taken.

The Department has a project in place to upgrade MONIES to EMS.11 (asset management tool) and to implement Remedy (in order to track requests).

ISP Radio

The Department has delegated responsibility for the provisioning and vendor management of radio communications equipment and services to the Illinois State Police via Interagency Agreement. Under the Agreement, the Department provides funding for staff resources to perform these delegated functions. ISP Radio staff are responsible for maintaining master contract agreements for radio equipment, towers, and spectrum licenses. Equipment contracts are processed through Procurement Services while tower and spectrum licenses are processed through the Department using the Remedy system in accordance with the Communications Revolving Fund Procurement Procedures.

Agency requests for equipment are processed using IGPS. ISP Radio staff review and approve all orders, providing assistance to agencies as needed. All vendor invoices are submitted directly to

ISP Radio staff for review, tracking, dispute resolution and finally distribution to the appropriate agencies.

Service Delivery

The Department has developed three agreements, which outline the terms and conditions under which the Department will provide specified IT services to an agency. The objective is to provide a basis and framework for the delivery of high quality services that meets the needs of the agency.

According to the Service Level Agreement (SLA), the "Standard Services" the Department will provide include:

- Mainframe Services,
- Midrange Services,
- Desktop/End User Support Services,
- Security Management Services,
- Data Communication-LAN Services,
- Data Communication-WAN Services,
- Telecom-Voice/Video Conference Services,
- Help Desk Services,
- Backup, Recovery, and IT Recovery Services,
- Common Application Services, and
- PIM Services.

In addition to outlining the services, the SLA delineates the terms and conditions between the Department and each agency. The objective of the SLA "is to provide a basis and framework for the delivery of high quality services."

The Department and the agencies mutually review the SLA on a quarterly basis to identify updates and modifications. Agency change requests are received by the Service Level Management Team who updates the SLA document and routes the proposed changes to the Shared Services Managers for approval. The SLA change approval process is documented in the Service Level Agreement and Update Approval Routes.

Since the IT infrastructure has not physically merged into the Department, the agencies are responsible for the collection and reporting of data. Each month the Infrastructure Leads are responsible for their agency's data collected and reporting to the Service Level Management Team. Currently, the only data collected by the agencies relates to Help Desk calls, LAN up/down times, and Midrange up/down times. Additionally, the Department is collecting data on Mainframe up/down times.

The consolidated agencies were provided an Excel template outlining the monthly statistics to be collected. However, there is not a methodology outlining the precise data or how the data is to be collected. Currently, agencies are obtaining the data from reviewing logs or estimating. The Department is in the process of developing a standard methodology for calculating performance

data as well as implementing an enterprise-wide tool to monitor and collect performance data. The standardized process and tool is targeted to be operational next fiscal year.

The agencies submit their data to the Service Level Management Team in an Excel spreadsheet. The Service Level Management Team then imports the data into PBViews. PBViews is a web based reporting system, which allows management teams to view the performance measures and analysis trends.

The Interagency Agreement outlines the responsibility of the agencies in relation to the employees, assets, contracts, and appropriations affected under the IT consolidation. Until employees and assets are physically moved to the Department, they will remain at the agencies, but under the Department's control.

The Department and agencies, which receive federal funding for IT services, entered into a Federal Funding Interagency Agreement. The Agreement outlines the transfer of Infrastructure Leads, Infrastructure Employees, and Infrastructure Assets.

These Agreements outline criteria for the billing of services and require the Department to provide the agency with documentation regarding Infrastructure expenditures, which the agency may submit to the federal government for reimbursement.

The following agencies have agreements with the Department:

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

In addition to the Bureau, various other divisions within the Department assist the Bureau in providing service.

Illinois Office of Internal Audit

A statewide Information Technology (IT) audit function was developed as part of the Illinois Office of Internal Audit (IOIA) to address 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.

Department of Central Management Services Accounting

The Billing Allocation System (BAS) is a web-based system the Department utilizes to bill agencies for recently 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 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.

Facility Management

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

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 and Application Controls sections of this report.

This Page Intentionally Left Blank

GENERAL CONTROLS

General controls are the methods, policies, and procedures adopted by an organization to ensure the protection of assets, promotion of administrative efficiency, and adherence to management's standards and intentions.

The general controls review consisted of an evaluation of the controls in seven distinct areas:

- Administration;
- Continuous Service;
- Computer Operations;
- Security;
- Application Systems Development;
- Telecommunication; and
- Systems Software.

The Third Party Review addresses each general control area in a separate control section of this report.

This Page Intentionally Left Blank

ADMINISTRATION CONTROLS

Administration controls include the procedures necessary to ensure that resources are used efficiently and in accordance with management's intentions. They encompass the overall operation of the computer facility.

Administration controls also include functions that maximize organizational efficiency and productivity. Organizational efficiency can be directed through long-range planning efforts and effective personnel policies. Productivity in the computer facility is enhanced by adherence to standards.

We reviewed administration controls and noted the following:

Personnel Policies and Procedures

Control Objective - Management should ensure that personnel policies, procedures and practices provide for clearly defined position descriptions.

Tests Performed - We reviewed position descriptions and interviewed staff members.

Results – The Department maintains job class specifications and position descriptions. The position descriptions contain the position title, effective date, location, agency, division within the agency, description of responsibilities and percentage of time spent on each duty, name of the immediate supervisor and position title, and qualifications required for the position. However, we found numerous employees with position descriptions that did not represent actual duties, including job descriptions that listed Department staff working for other State agencies.

Staffing Levels and Training

Control Objective - Management should ensure adequate staffing and qualifications, clearly define roles and responsibilities, and implement satisfactory training programs.

Tests Performed - We interviewed staff and reviewed staffing levels and qualifications.

Results - Our review of the Department identified staffing issues and a lack of defined roles and responsibilities. We found:

- Staffing shortages or undefined responsibilities in critical areas such as security, recovery services, help desk, computer operations, and application development.
- Over-reliance on key staff members without properly trained backup personnel.

Additionally, the Department has not developed formal training policies.

Interagency Agreements

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.

Tests Performed - We reviewed interagency agreements and documents associated with the IT Rationalization project. We also reviewed actual versus target performance measures included in Service Level Agreements.

Results - Public Act 93-25 authorized the Department of Central Management Services to consolidate Information Technology (IT) functions of State government. In order for the Department to carry out the consolidation activities, an IT Rationalization project was initiated. The goal of the IT Rationalization project is to centralize IT functions for agencies under the Governor; thus, enhancing the Department's efforts as a service bureau.

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.

To implement the consolidation of IT functions, the Department developed three types of agreements.

Interagency Agreements

Interagency agreements outline the responsibility of the agencies in relation to the employees, assets, contracts, and appropriations affected under the IT consolidation. Until employees and assets are physically moved to the Department, they will remain at the agencies; however, under the Department's control.

Federal Funding Interagency Agreements

The Department and agencies, which receive federal funding for IT services, entered into Federal Funding Interagency Agreements. These agreements outline criteria for the billing of services, and require the Department to provide the agency with documentation regarding infrastructure expenditures, that the agency may submit to the federal government for reimbursement.

Service Level Agreements

These agreements outline the terms and conditions under which the Department will provide specified IT services to an agency. The objective is to provide a basis and framework for the delivery of high quality services that meets the needs of the agency.

According to the agreement, the "Standard Services" the Department will provide include:

- Mainframe Services;
- Midrange Services;
- Desktop/End User Support Services;
- Security Management Services;
- Data Communication-LAN Services;
- Data Communication-WAN Services;
- Telecom-Voice/Video Conference Services;
- Help Desk Services;
- Backup, Recovery, and IT Recovery Services;
- Common Application Services; and
- Personal Information Management (PIM) Services.

The following terms and conditions are included in the agreements between the Department and each agency:

- Defining the services;
- Minimum service levels;
- Availability, reliability, and growth;
- Continuity planning;
- Security requirements;
- Change procedures for any portion of the agreement;
- Content and frequency of performance reporting; and
- Charges for services.

Although the Service Level Agreement concept is well-founded, the current documents appear to lack applicability, value to agency operations, and enforceability. The Service Level Agreements have been in place for over a year, and very little progress has been made to ensure the Agreements achieve their original intent and objectives. For instance, target performance measures outlined in the Agreements were not always achieved. In addition, although a detailed process existed to promote frequent and formal reviews of the Agreements, no Agreements have been revised to more accurately reflect actual practices since June 2005.

Long-Range Planning

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

Tests Performed - We reviewed the Information Technology and Telecommunication Strategic Plan.

Results – Public Act 93-25 authorized the consolidation of the State's IT services in the Department. The Department developed the *FY 2006 - Information Technology and Telecommunications Strategic Plan* to assist with consolidation efforts.

Project Management

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.

Tests Performed - We interviewed staff and reviewed projects for compliance with the Governance process.

Results - The Executive Program Management Office (EPMO) is responsible for maintaining and managing the Department's project portfolio, and providing project management support. The EPMO directly manages large, complex projects at the direction of Department management using a consistent and standardized project management processes.

The IT Governance model has been established to help oversee the management of projects. The Governance model is a set of political processes, driven by business and technical principles to ensure IT investments meet the following objectives:

- Alignment of IT with the enterprise goals and realization of the promised benefits.
- Use of IT to enable the enterprise by taking advantage of business opportunities.
- Optimization use of IT resources.
- Management of IT related risks.

The Enterprise Architecture and Strategy was developed to ensure IT investment decisions are aligned with vision and goals and deliver outcomes that keep in step with the accelerating pace of business changes.

The Architecture Rationalization Board (ARB) is a multi-agency member authority established to facilitate the IT Governance process. The intent of the ARB is to assure alignment of the IT portfolio, and adherence to Standards concerning the deployment of IT. The goal is to assure the resultant products conform to established IT Standards and architecture.

Although a governance framework has been developed, the Department should develop detailed project management guidelines and ensure all applicable projects conform to the guidelines.

Internal Audit Coverage of Information Systems

Control Objective - Management should ensure that Internal Audit routinely reviews information technology integrity and security issues. Management should also ensure that the Internal Audit division complies with the statutory mandate (30 ILCS 10/2003 (a) (3)) to review the design of major new systems and major modifications to existing systems before their installation to ensure that the systems provide for adequate audit trails and accountability.

Tests Performed - We reviewed planning documents, the Annual Report, and a listing of audits completed and in-progress.

Results - On March 31, 2003, the Governor signed Executive Order 2003-10 to consolidate internal auditing activities under the Department of Central Management Services. On October 1, 2003, the Illinois Office of Internal Audit (IOIA) was officially established as the internal auditor for executive agencies.

The Fiscal Control and Internal Auditing Act (FCIAA) (30 ILCS 10/2003) requires each designated State agency to develop a "two-year plan, identifying audits scheduled for the pending fiscal year." The IOIA developed an audit plan for fiscal years 2005 and 2006, which was approved by the Governor's Office on June 29, 2004. The IT sections of the audit plan are based on the IT risk assessment, the FCIAA risk assessment, and the database of system development projects. The two-year audit plan included audits of general controls, security, applications and system development reviews.

On September 30, 2005, IOIA submitted the required Annual Report to the Director and the Governor's Office, which outlined their accomplishments for fiscal year 2005 and objectives for fiscal year 2006.

The IOIA has requested executive agencies to inform them of in-progress or planned system development projects. Once informed, the IOIA reviews the project and performs a risk assessment. If the project is determined to be high-risk, the system will be reviewed.

During fiscal year 2006, the IOIA performed general IT work in various areas of the Department.

The Department oversees a vitally significant, multi-million dollar computer operation, and relies heavily on information technology to provide services to other agencies and to perform its own functions. The increased use of information technology and consolidation efforts reinforce the need for independent reviews to ensure that all risks and security issues have been adequately addressed.

The Department should ensure that an effective process exists to identify and monitor information technology activities to ensure that integrity and security issues are adequately addressed.

Billing System

Control Objective - Management should ensure that 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.

Tests Performed - We reviewed the Department's billing procedures and user agency bills. Additionally, we reviewed the process of issuing credits and the collection of outstanding balances.

Results - The Department is statutorily authorized to provide data processing services for State agencies. The Department, State agencies, and users of the CCF share the costs of those services. Each month, agencies make payments to the Statistical Services Revolving Fund (SSRF) and the Communications Revolving Fund (CRF) for services rendered on their behalf.

We reviewed the invoices from four agencies for the month of December 2005, and identified no discrepancies.

The Department has two forms to process credit requests: the Credit Adjustment Form (CAF) and the Accounts Receivable Credit Memorandum (ARCM). The CAF is used to process credits due to hardware or software failures at the Data Center that cause a program to fail. The user agency is responsible for completing the CAF and submitting supporting detail. After approval, the credit is sent to Accounting for manual entry into the billing system to adjust the user agency's next invoice.

The second form, the ARCM, is used to process credits that are the result of errors on user agencies' billing invoices. The user agencies, or Department personnel, complete the credit memo. All credit memos must be submitted with supporting detail. The form and supporting detail are reviewed by the billing staff supervisor and then forwarded to Accounting for posting.

We reviewed the credit log for the months of July 2005 through April 2006, noting no duplicate credits and the credits appeared reasonable. In addition, we reviewed seven credits for proper approval, supporting documentation, and correspondence to the credit log, noting no exceptions.

Each month, the Department receives billing information from several different vendors either in hardcopy or electronic format. This information is then reformatted and loaded into the Management of Network Income Expense Services (MONIES) system. MONIES is the billing, order management, and inventory system that the Department uses to process, track and bill telecommunications services. We reviewed the reconciliation between the vendor files and MONIES for December 2005, and identified no exceptions.

The Accounting Department is responsible for pursuing outstanding SSRF and CRF accounts receivable. The Department has written procedures for accounts receivable for the SSRF and CRF. The Accounts Receivable Posting System is used to track accounts receivable for both the SSRF and the CRF. According to the *Illinois Administrative Code (74 Ill. Adm. Code Part 1000)*, the Department is to send out catch-up billings in the subsequent fiscal year for accounts receivable of the prior fiscal year. Catch-up billings are to be sent monthly beginning in November of the subsequent fiscal year. We reviewed 25 catch-up billings, noting no exceptions.

If any agency persists in not paying a delinquent account, the Department may submit the customer to the Comptroller's Offset System. According to the "CMS Billing Manual," the Department's Director may also prepare a letter to the Director of the delinquent agency requesting attention to the matter. The letter states failure to resolve the outstanding amounts could result in curtailment of future services. If a non-state agency continues to be delinquent, the account is referred to the Debt Collection Board. During our audit, we noted the Director Letters have not been prepared for delinquent accounts for the last three fiscal years.

As of December 31, 2005, the accounts receivable (for State and non-state entities) for the SSRF and CRF were $31.6 million and $19.5 million, respectively. The accounts receivable for the SSRF and CRF increased $14.3 million and $1.6 million, respectively from December 31, 2004.

After 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, provided by IBiS, are the foundation for agencies to make payments to the Department. Additionally, the statements provide documentation for agencies to use for Federal Fund Participation purposes.

Each month, IBiS generates a bill for consolidated services: Facility Management, Communication Managers, Graphic Designers, and IT. Total IBiS billings for July 2005 through March 2006 were $40,446,501.

Under the Federal Funding Interagency Agreement, the Department is required to ensure the expenditures charged to the agency are actual expenditures attributable to the specific agency. However, in our review, we identified several billing practices that warrant additional analysis.

The Department developed the IBiS System Administration Guide, which outlines the billing compilation of the consolidated services. However, detailed policies and procedures to ensure the appropriate level of documentation to support billing statements had not been developed.

Although reasonable administration controls existed, we recommend the Department:

- Assess current staffing and technical experience levels, and develop a staffing plan to address any deficiencies.

- Ensure staff are adequately trained and critical positions have trained backup personnel.

- Ensure position descriptions accurately reflect duties. Additionally, the Department should ensure staff roles and responsibilities are formally documented and communicated.

- Develop and implement a formal training policy and program.

- Thoroughly review the Service Level Agreements and ensure the agreements meet the original intent and objectives. Specifically, the Department should ensure the terms, performance measures, and responsibilities are realistic, achievable, monitored, and enforced.

- Continue monitoring the IT Rationalization/Consolidation, and ensure that the long term needs of the State's IT environment are adequately addressed.

- Review the IBiS billing process and ensure it accurately reflects actual expenditures incurred for the agency. The Department should develop policies and procedures to ensure adequate documentation is available to support agency billing statements.

This Page Intentionally Left Blank

CONTINUOUS SERVICE CONTROLS

Continuous service controls include the procedures necessary to ensure that information processing resources will be available even if the primary facility is not useable. These controls encompass the entire planning and testing process associated with comprehensive contingency planning activities.

As the Department places more reliance upon computer operations, the ability to continue critical processing is of prime importance.

The Department is mandated to provide computing services to State agencies that depend on a continuation of computing services in order to fulfill their duties, missions, and goals. A contingency plan is essential for an organization to minimize service disruptions and fully restore operations in the event of a disaster. Continuity service protection encompasses the areas of contingency planning, backup and recovery procedures, disaster recovery testing, recovery priorities, and designation of an alternate processing facility.

Procedures should be developed and tested to minimize the risk of unplanned interruptions and ensure the availability of critical information resources within acceptable timeframes.

We reviewed continuous service controls and noted the following:

Disaster Contingency Plans

Control Objective - Management should maintain a written plan for restoring critical applications.

Tests Performed - We reviewed the following continuity plans:

- State of Illinois, DCMS, BCCS, ISD, Continuity Methodology-Effective January 3, 2005;
- State of Illinois, DCMS, BCCS, ISD, Recovery Activation Plan-Effective December 20, 2004; and
- State of Illinois, DCMS, LAN, Recovery Activation Plan-Effective August 11, 2004.

Results - The Department has compiled three contingency plans for the restoration of its various environments; however, the plans were not updated during the audit period and do not reflect the current environment.

Testing Recovery Procedures

Control Objective - Management should ensure that plans and procedures are adequately tested.

Tests Performed - We reviewed documentation associated with tests conducted.

Results - The Department conducted a limited exercise at the out-of state service provider's site in June 2005. However, the exercise was not comprehensive, significant difficulties were encountered, and limited documentation was available to support the exercise.

In addition, the tornados that afflicted the Springfield area in March 2006 illustrated some deficiencies in the current contingency planning. After the tornados, the Department presented a "lessons learned" to State agencies, which identified several weaknesses in the recovery process.

Alternate Data Processing Facilities

Control Objective - Management should arrange for alternate data processing facilities.

Tests Performed - We interviewed staff, reviewed contracts for alternate facilities, and visited local facilities.

Results - The Department dismantled the local recovery site; thus, it was no longer a viable recovery site. In 2005, the Department was in the process of planning for a new backup data center. However, management stated the proposed backup data center had not materialized, and the Department was currently pursuing other alternatives. Thus, a local or regional recovery site does not exist.

The Department has 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.

Statewide Critical Application Listing

Control Objective - Management, based on criticality and sensitivity of data and operations, should determine and prioritize applications and data.

Tests Performed - We reviewed the process used to prioritize applications.

Results - The Department maintains 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 that have been tested would be considered for recovery. Agency disaster recovery information is maintained in the Statewide Disaster Recovery File, which is stored off-site at the regional vault.

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. During the audit period, the information had not been updated; therefore, the likelihood of recovery of these critical application was diminished.

Backup and Off-site Storage

Control Objective - Management should ensure that critical resources are backed up on a regular basis and stored off-site.

Tests Performed - We visited facilities and tested for availability of backup materials and data.

Results - The Department currently utilizes off-site storage facilities, and procedures exist to routinely backup critical data. Physical security and environmental controls were present at the off-site storage facilities.

Backup Power Source

Control Objective - Management should ensure an uninterruptible power supply (UPS) for critical applications is available.

Tests Performed - We reviewed backup power sources, maintenance agreements, and backup power tests.

Results - The electrical power for the CCF is from two different utility-supplied power grids. If one source fails, a system will transfer to the other power source. If both power sources fail, the building's power will be supplied from the CCF's UPS. In the short term, a battery bank will supply the needed electrical power. This period of time allows the diesel-powered turbines to be started. The turbine generators can supply electrical power until utility-supplied power is restored.

A service contract agreement, effective July 1, 2005 through June 30, 2006, has been established to provide routine preventive maintenance on the UPS components located at the CCF.

As outlined above, we identified several significant weaknesses, which will have a major impact on the State in the event of a disaster.

The Department is mandated to provide computing services to the agencies of the State; therefore, it is imperative the Department take action to minimize risk over the various environments.

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. In order to minimize risks associated with a loss of service, the Department should:

- Prioritize the development of an effective business continuity plan that incorporates the recovery of computer services.
- Ensure adequate plans, facilities, and equipment are available to recover all critical applications.
- Perform annual comprehensive tests of the recovery plans.
- Obtain a suitable regional alternate location for recovery services.

This Page Intentionally Left Blank

COMPUTER OPERATIONS CONTROLS

The command center unit of computing services is the focal point of data processing for the CCF. The control and management of computer operations are vital to overall data processing effectiveness.

Computer operations management must be aware of all facets of the operating environment and be able to control it. Department management must ensure that processing meets specifications, thereby making the review of operations a primary concern. Therefore, Department management must require the logging of all actions initiated by computer operators and all actions performed by computer software.

We reviewed computer operations controls and noted the following:

Activity Logs

Control Objective - Management should ensure that sufficient information is stored in operations logs to enable reconstruction, review, and examination of activities.

Tests Performed - We reviewed Daily Shift Reports, Shift Change Checklists, Incident Reports, and Call Log Reports.

Results - The CCF maintained several reports that record Command Center activities. The Daily Shift Report, Shift Change Checklist, Incident Report, and systems logs are utilized to record Command Center activities.

We reviewed the Shift Change Checklists for a one-week period, and determined the checklists were properly completed and reviewed by a supervisor. Additionally, we reviewed 25 Incident Reports and 25 Daily Shift Reports, and identified no significant exceptions.

In addition, we reviewed the Call Log Report for December 2005 and three days in April 2006. We found the number of unanswered calls for each time period reviewed exceeded the Department's abandonment threshold of less than 5%.

Help Desk Activities

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

Tests Performed - We reviewed the tracking systems, which log and manage incident calls and requests, the associated procedures, and performance measures.

Results - The Department employed a service desk approach and organized three divisions to provide support for users:

- Customer Service Center (CSC). The CSC is responsible for maintenance and provisioning of voice, data, videoconferencing, and wireless systems and services. In

addition, the CSC, through the IT Service Desk, provides trouble-shooting and service desk functionality to multiple agencies under the Governor.

- Customer Management Center (CMC). The CMC is responsible for all trouble resolution, network surveillance, and ongoing technical support for private line connectivity and the Illinois Century Network (ICN).
- Command Center. The Command Center is responsible for mainframe and PKI problem resolution. As outlined in the Activity Logs section, several reports and logs are utilized to record Command Center activities.

The Department uses several systems to log and track incident calls to ensure adequate monitoring and resolution of the incident. In our testing of incident calls, we found problems with tracking logs, inconsistencies between the separate systems, and missing data. Department management stated they are in the process of implementing an asset management tool, which will interface with a new help desk module for the three service desks.

The CSC Methods and Procedures, along with workflow documents, provide staff with guidance on the various types of service desk calls. In addition, the CSC Escalation Procedures provide guidance on when to implement escalation procedures based on standard completion times.

The CMC has developed several Methods and Procedures, which address the various types of problems including the escalation of problems.

Each month, the Department reports performance measures for the CMC and CSC. We reviewed the reports for August 2005 through December 2005, and found the number of unanswered calls for each time period reviewed exceeded the Department's abandonment threshold of less than 5%. In addition, IT Service Desk calls are not tracked in the system or included in the performance measures reports.

Staff Training

Control Objective - Management should ensure that staff is adequately trained on start-up procedures and other operations tasks.

Tests Performed - We reviewed operational procedures and conducted interviews with Department management.

Results - Designated daily training periods are assigned to each operator. During the review period, the following activities were conducted:

- Ongoing review of the Data Processing Guide;
- Use of computer-based training tools;
- Presentation of courses at the training facility; and
- Hands-on training conducted by supervisory staff.

The Command Center staff utilizes two separate procedural guides: the Data Processing Guide and the Notes Guide. The Notes Guide is considered the updated version of the Data Processing Guide. However, the guides lack consistency, and not all procedures from the Data Processing

Guide have been incorporated into the Notes Guide. Since the guides contain both similar and differing procedures, staff may not be able to locate and execute the proper procedures.

In addition, we noted the contact information to support the timely resolution of system problems was outdated.

Performance Monitoring

Control Objective - Management should ensure that systems performance is assessed and meets the short and long-range needs of the agency.

Tests Performed – We reviewed the system performance monitoring tools and conducted interviews with Department management.

Results - Command Center staff utilize two software products to monitor systems performance.

Change Control

Control Objective - Management should ensure that an appropriate structure is established to ensure changes to system software and/or application software are sufficiently controlled to confirm that only tested and authorized changes are executed.

Tests Performed - We interviewed staff and reviewed change management policies and procedures.

Results - In November 2004, the Department implemented a new change management process to control all significant or major changes. All changes having the potential to impact any Departmental services or customers are subject to the new process.

Although the Department should be following the change management process implemented in 2004, the policies have not been updated. In addition, the Department has not developed a mechanism to ensure all changes followed the approved process. Management was unable to provide documentation or provide assurance that all changes adhered to the approved process.

The approved change management process has not been implemented across all platforms. As a result, the current change management process lacks consistency and does not ensure all changes are sufficiently controlled. Department management stated they are in the process of implementing Enterprise-Wide Change Management tools and policies.

As a result of the deficiencies identified above, we were unable to perform detailed tests of compliance with the approved change management process. However, during our review and testing of the mainframe, midrange, LAN, and application environments, we did not identify significant issues attributed to the deficiencies in the current change management process.

The lack of a formal change management process leaves the Department exposed to the risk of unauthorized and not suitably tested changes to systems.

The Department is mandated to provide computing services to the agencies of the State; therefore, it is imperative the Department take action to minimize change control risks.

To improve Computer Operations controls, we recommend the Department:

- Ensure the number of unanswered calls meets the Department's abandonment threshold of less than 5%.
- Implement a comprehensive system to consistently register, track, and address all user queries.
- Ensure Data Processing Guide and Notes Guide contain consistent, current, and accurate information.
- Update policies and procedures to govern the approved change management process and ensure staff compliance.
- Ensure all changes follow the approved change management process.
- Expedite the development and implementation of the Enterprise-Wide Change Management Solution.

SECURITY CONTROLS

The presence of security controls reduces or prevents disruption of service, loss of assets, and unauthorized access to equipment. An effective security program is a prerequisite to effective computer security.

Security measures include controlling access to computer facilities, controlling visitors within the facility, and establishing appropriate security policies and procedures.

As computers become increasingly integrated into the delivery of State services, and contain critical and confidential information, security becomes increasingly essential. New initiatives introduce security concerns that must be continually, adequately, and globally addressed. In addition, since the Department functions as a computer service bureau for State agencies, there is an inherent leadership role regarding technology and security issues. In addition, the Department's responsibility regarding security has increased as a result of the agencies' IT environment consolidation. Therefore, we strongly believe that an effective security administration function is critical to the overall security and integrity of the State's computing environment.

We reviewed security controls and noted the following:

Security Policies

Control Objective - Management should have a written plan that clearly describes the department's security program, policies, and procedures.

Tests Performed - We reviewed policies and procedures and interviewed staff regarding security-related functions.

Results - The Department has several security-related documents:

- CMS Policy Manual (dated by section),
  - CMS Information Technology Security Policy (dated April 26, 2002) included as Chapter 4, Section 3 of CMS 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), and
- CMS LAN Office Systems Procedures Guide (dated February 2003).

The documents have not been updated since at least February 2003. As a result, the documents do not reflect the current technological environment and have not been updated to address current security concerns. In addition, the Department has not developed security policies to address the consolidation of agencies into its IT environment.

Security Administration

Control Objective - Management should coordinate a security management structure and clearly assign responsibilities.

Tests Performed - We reviewed the organizational chart and interviewed staff to obtain an understanding of the current security organizational structure.

Results - A risk management structure has been established and defined; however, the security positions have not been staffed to proposed levels. As a result, the goals associated with the new risk management structure have not been realized.

Personnel Policies

Control Objective - Management should have a written personnel policy that includes procedures relating to hiring, transferring and terminating employees.

Tests Performed - We reviewed personnel policies and practices for hiring, transferring, and terminating employees, including guidelines to update or remove access privileges.

Results - It is the Department's practice to require all new personnel to undergo a security screening investigation prior to the start of employment and sign the appropriate release forms to allow the security staff to obtain any necessary documentation.

According to the CMS Policy Manual, "The bureau is responsible for notifying the Office of Internal Personnel of an employee leaving the agency." In addition, "Supervisors are responsible for collecting a separated employee's telephone credit card, door and desk keys, parking lot stickers, Data Center admittance cards, identification cards, vehicles and special equipment. The supervisor is also responsible for contacting the Data Processing Manager if the employee had terminal or operator access to data bases."

We found that guidelines did not exist to notify all appropriate security staff of personnel changes to update or eliminate physical and logical access rights.

Security Awareness

Control Objective - Management should ensure that staff are aware of their roles and responsibilities.

Tests Performed - We reviewed policies and procedures, assessed security awareness, and reviewed practices to communicate policies to staff and contractors.

Results - It is the Department's practice to require employees to sign a statement of understanding that they have read and agree to act in accordance with select policies and sign statements of understanding, and require contractors to sign a confidentiality and access authority agreement.

Our testing indicated not all required statements of understanding were signed at the start of employment or contractual services.

There are no requirements for employees to routinely attend security-awareness training and no training was conducted during the audit period.

Security Lists

Control Objective - Management should establish guidelines governing security authorization lists.

Tests Performed – We reviewed guidelines and procedure governing security authorization lists.

Results - Semiannually, the Department sends user agencies a memo requesting a verification and update of security authorization lists. The lists include information on agency staff authorized for security and media transactions. The Department requested updated information from agencies in September 2005 and all agencies complied with the request.

Security Violations

Control Objective - Management should have policies and procedures for identifying, reviewing, and addressing security violations.

Tests Performed - We reviewed the policies and procedures for identifying, reviewing, and addressing suspected security violations.

Results - The Department has not developed or implemented comprehensive policies and procedures for identifying, reviewing, and addressing suspected security violations.

Physical Security

Control Objective - Management should ensure that physical access to computer resources is restricted.

Tests Performed - We reviewed policies and procedures, assessed physical security, and tested compliance with procedures regarding the assignment of temporary badges.

Results - Controls existed to restrict physical access to computer resources.

The CCF was constructed in 1980, and designed to meet the State's data processing needs. The CCF was built with pre-cast concrete, has a steel structure, and a shell that is non-combustible. The CCF is monitored 24 hours a day, 7 days a week, by security guards, surveillance cameras, proximity badge readers, and alarms. The Command Center is protected by both a fire detection and suppression system and a water detection system. The Department's Information Security Policy states the area housing the Command Center of the CCF is intended to be under tight security at all times.

The Communications Center is monitored 24 hours a day, 7 days a week, by security guards, surveillance cameras, proximity badge readers, and alarms.

Procedures exist for the issuance of badges and for granting visitor and guest access to the CCF and Communications Center. Different types of temporary badges can be issued to visitors and guests, depending on their access needs. Visitors, or employees who forget their badge, are required to sign-in and register with security guards to gain access to the facility.

Physical security and environmental controls were present at the auxiliary and off-site storage facilities.

Tape Management

Control Objective - Management should develop procedures relating to data storage to ensure the accuracy of inventory counts of physical movement and storage of media.

Tests Performed - We reviewed tape management procedures and practices and rotation of tapes to off-site storage locations.

Results - The Department has formal tape procedures in place to control the movement of magnetic tapes to and from the CCF. In addition to agency tapes being rotated to the off-site storage location, CCF staff physically rotate operating system backups to the local and regional off-site storage locations. Agencies also have been provided with the capability to electronically transmit backup data to an alternate location.

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

Although security controls were addressed at the Department, the security administration framework has not been sufficiently developed or implemented to ensure security is adequately addressed from a Statewide or Departmental perspective. To enhance security, the Department should:

- Thoroughly review and update security policies to address the current technological environment, consolidation issues, and present-day risks. In addition, the Department should ensure all policies are updated annually and dated, and all employees and contractors have access to the current versions of policies.

- Formally approve and implement a comprehensive risk management framework. Special emphasis should be placed upon the allocation of sufficient resources to support the framework.

- Develop and implement comprehensive policies and procedures for identifying, reviewing, and addressing suspected security violations.

- Formally promote security awareness and require training to keep users informed and aware of security issues, and periodically assess compliance with established policies and procedures.

- Develop procedures to ensure that access authorization rights are periodically reviewed and updated to ensure access rights align with job requirements and are updated upon the termination of employment or contracts.

This Page Intentionally Left Blank

APPLICATION SYSTEMS DEVELOPMENT CONTROLS

Application systems development is a critical part of the data processing function. A structured systems development process helps to ensure system reliability, quality, predictability, and user satisfaction.

The acceptance of a structured systems development methodology ensures that system design meets the requirements of system users. A structured approach includes the use of standards for systems design, documentation, testing, and post-implementation review. It also ensures that all new and enhanced computer systems meet organizational requirements.

The Department is responsible for the development of computer systems (common systems) that are available for use by the user agencies, as well as those systems used by the Department.

We reviewed application systems development controls and noted the following:

Systems Development Methodology

Control Objective - Management should have a documented systems development methodology that details the procedures that are to be followed when applications are being designed and developed, as well as subsequently modified**.**

Tests Performed - We reviewed the Application System Development Methodology (Methodology) and the Standards and Documentation Requirements (Standards).

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

The Methodology outlines 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.

Phase I (problem definition and systems planning) is the initial phase and examines the feasibility and benefit of a project. Requirements for a cost/benefit analysis of new applications or major system enhancements are included in the Methodology.

Phase II (design) is intended to document, propose, and obtain approval of the design. A security statement, database layouts, sample input documents, sample output, system narratives, diagrams, backup requirements, and conversion plans are developed. The Methodology states a user committee will be formed to assist with system analysis and design.

In **Phase III** (development and implementation), the project will be developed based on the system specifications documented in Phase II. The Methodology states all aspects of the system must be thoroughly tested and reviewed prior to implementation.

According to the Methodology, **Phase IV** (post-implementation review), if required, will be conducted within 30 to 180 days after the system is in production. The purpose of a post-implementation review is to review the production system and evaluate its actual benefits, performance, and cost.

The service request form is used to initiate system development projects. The Service Request Registration System (SRRS) registers projects and records the status of the project. There are four categories of system development projects: a new development, enhancement, maintenance, or ad hoc request. A new development is the development of new applications or systems when no system is in production, or a rewrite of an entire existing system. An enhancement is a routine change or the addition of a new feature to an existing system. Maintenance requests are emergency changes or required changes to an existing system that do not change system functionality. An ad hoc request is a one-time request for reports or programs.

Development Process Oversight

Control Objective - Management should establish roles and responsibilities for planning, developing, reviewing, implementing and auditing the development process.

Tests Performed - We reviewed the Application System Development Methodology (Methodology) and the Standards and Documentation Requirements (Standards).

Results - The Methodology addresses the roles and responsibilities of the development group, technical support, Quality Assurance, and Internal Audit. The development group is responsible for mainframe and LAN systems design, coding, program walk-through, testing, documentation, implementation, database administration and ongoing production application support. Technical support provides resources for database technical reviews and security software. Quality Assurance monitors and verifies project teams adhere to the Methodology. Users are to participate in each phase of systems development, assist with defining business rules and designing the system, and executing systems tests. Internal Audit determines its own level of involvement in projects.

Project Management

Control Objective - Management should have management tools for the tracking of projects.

Tests Performed - We interviewed management and reviewed pertinent documents to determine what project management tools were utilized. Additionally, we reviewed service request forms to determine if they were properly completed, approved, and categorized.

Results - The Department utilizes several tools to aid in tracking system projects, assignments and the scheduling of time.

One tool is the SRRS, which is used to track projects involving application system enhancement, development, or change. A service request form is used to record the request and input information into the SRRS.

We reviewed 30 service request forms and determined all were properly completed.

Test Plans

Control Objective - Management should require that a test plan be created for developments, implementations, and modifications.

Tests Performed - We reviewed the Application System Development Methodology (Methodology) and the Standards and Documentation Requirements (Standards).

Results - The Department requires 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. Users are to participate in each phase of system development and assist with defining the business rules and designing the system. Users are responsible for developing and executing system tests according to the business rules.

The Methodology requires the Project Manager to request users to develop unit, system, and integration test plans.

Training Plans

Control Objective - Management should require that training plans be created for projects.

Tests Performed - We reviewed the Application System Development Methodology (Methodology) and the Standards and Documentation Requirements (Standards).

Results - According to the Methodology, a training schedule is to be developed and training sessions are to be conducted during Phase III (development and implementation).

Quality Assurance

Control Objective - Management should ensure that the responsibilities of the Quality Assurance personnel include a review of general adherence to the systems development methodology and objectives of the project.

Tests Performed - We reviewed the Quality Assurance Review Procedural Manual.

Results - The Methodology includes the Quality Assurance Review Procedural Manual, which addresses the quality assurance function. It is Quality Assurance's responsibility to monitor and verify that project teams adhere to the Methodology during each phase of a systems development project.

Program Movement

Control Objective - Management should ensure that access to production libraries is limited and movement of programs is controlled.

Tests Performed - We reviewed a sample of move requests to determine if moves to production were completed in compliance with the Program Library Procedures.

Results - The Program Library Procedures state "Library Control is to maintain program library security and perform special assignments, when required." Library Control staff control all movement of programs in a production library. The procedures are to ensure that new programs and modifications to existing programs are thoroughly documented and signed off by a manager before production moves are performed. The process of requesting a change be moved to production is automated.

We reviewed 14 move requests and determined all were completed in compliance with the Program Library Procedures.

TELECOMMUNICATION CONTROLS

Telecommunication systems control the transmission of messages between users and the computer. Through the telecommunication network, users at remote sites can access computer programs at the computer facility. The majority of devices interface with the computer facility by a telecommunication device. Control over the telecommunication network is necessary to ensure that only authorized users have access to the computer facility.

Telecommunication network controls should encompass the network's operating performance and security.

The Department has a statutory obligation to "provide for and control the procurement, retention, installation, and maintenance of telecommunications equipment or services used by State agencies in the interest of efficiency and economy." (20 ILCS 405/405-270*)*

The Department operates in a manner similar to a telephone company and utilizes a combination of State and vendor services. The Department provides local telephone service, telecommunications equipment, software, installation, maintenance, and networking services to State agencies. The statewide telecommunications network is comprised of thousands of miles of voice and data lines serving the State.

The Department's Division of Network Services is responsible for management and oversight of the Illinois Century Network (ICN), Local Area Networks (LAN) for select agencies, the Illinois Wireless Information Network (IWIN), and all engineering responsibilities related to State of Illinois telecommunications services.

We reviewed telecommunication controls and noted the following:

Network Documentation

Control Objective - Management should ensure that the telecommunications networks are adequately documented.

Tests Performed - We reviewed network diagrams and configurations, and interviewed staff regarding the structure of the network.

Results - The Department maintains network diagrams; however, a unified network diagram or topology accurately depicting all components of the statewide network did not exist.

Security Structure

Control Objective - Management should coordinate a telecommunications security management structure and clearly assign responsibility.

Tests Performed - We reviewed documentation provided by management and interviewed staff to obtain an understanding of the current security management structure.

Results - As a part of the IT Rationalization project, the Department has assumed the responsibility for various telecommunication services and realigned the functions to separate divisions:

- Network Services
  - Customer Management Center (CMC)
  - Design and Security
  - Network Operations
  - Field Operations
  - LAN Services
  - Architecture and Planning
- Infrastructure Services
  - Recovery Services
  - Change Control
- Customer Service Center (CSC)

Network Design

Control Objective - Management should ensure the network is designed and controlled to reduce adverse impacts on the Department's systems and data.

Tests Performed - We reviewed network diagrams and configurations, and interviewed staff regarding the design and security of the network.

Results - The Department's statewide network is comprised of three primary elements:

- The State of Illinois Backbone Network (Backbone).
- Springfield Computer Facilities.
- Illinois Wireless Information Network (IWIN).

The Backbone network provides access to the State Intra-Agency network, the State and Federal Inter-Agency network, county and municipal governments, and educational institutions.

The Springfield computer facilities provide intra-agency and inter-agency network and Internet communications.

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

The statewide network is extremely complex and responsibility for various components is spread across multiple groups. As a result, we identified differing configuration standards and processes, management approaches, and problem resolution and reporting. Such fragmentation may increase the potential for undetected security vulnerabilities.

Security

Control Objective - Management should ensure firewall and router rules are sufficient and current, to protect against unauthorized access to resources and denial of services.

Tests Performed - We performed a detailed review of firewall and router security parameters.

Results - Although no significant issues were identified, we discovered some parameters that should be reviewed to ensure security issues are appropriately addressed.

Internet Privacy Policy

Control Objective - Management should deploy a privacy policy on the Department's website informing users of tracking technologies that are utilized and contain provisions that disclose practices regarding Notice, Choice, Access and Security.

Tests Performed - We reviewed the Department's website for the existence of an Internet privacy policy. Additionally, we reviewed the privacy policy to determine if it adequately addressed the issues of Notice, Choice, Access, and Security.

Results - The Department's website contains a privacy policy (policy), dated May 2006. The policy informs users that personal information is not collected unless voluntarily provided by the user via email, online forms, survey response, or registration for a specific service. Users who choose not to participate in the above listed activities will still have the ability to utilize all other features of the website. The policy then includes a provision notifying users of their right to review any personal information that has been collected by the Department, and recommending changes to any inaccuracies.

The policy also states "The Department of Central Management Services, as developer and manager of this website, has taken several steps to safeguard the integrity of its communications and computing infrastructure, including but not limited to authentication, monitoring, auditing, and encryption."

We noted the policy contained provisions that disclosed practices regarding Notice, Choice, Access, and Security.

Local Area Network (LAN) Security

Control Objective - Management should ensure that LANs are configured and controlled to promote security and integrity.

Tests Performed - We reviewed policies and procedures related to LAN security.

Results - The Department has historically maintained and supported LANs for the Department, as well as the Department of Human Rights, Department of Labor, Human Rights Commission, Illinois Civil Service Commission, Illinois Educational Labor Relations Board, Illinois Prisoner Review Board, Judicial Inquiry Board, Office of Executive Inspector General, Office of the

Governor, Office of the Lieutenant Governor, and the State Police Merit Board. In addition, the Department provides LAN connections for email purposes to seven agencies.

Additionally, as a result of the IT Rationalization/Consolidation, the Department assumed the responsibility for the LANs for Department of Revenue, Department of Financial and Professional Regulation, Department of Commerce and Economic Opportunity, Department of Transportation, Department of Agriculture, Department of Natural Resources, Illinois Environmental Protection Agency, Department of Public Health, Department of Human Services, Department of Employment Security, and the Department of Healthcare and Family Services.

The Department was unable to provide a complete and accurate listing of all servers under its control. As a result, we were unable to generate a random sample of servers and assess the physical and logical security controls of the selected servers. However, the physical security controls over servers housed in the CCF, JRTC, and the Communications Center were acceptable. In addition, we did not identify any significant deficiencies in logical security controls on servers we were able to identify and test.

We also determined the Department has policies relating to LAN security; however, the policies had not been updated to reflect the current environment.

Although reasonable telecommunications controls existed, we recommend the Department:

- Develop a unified network diagram or topology that accurately depicts all components of the network.

- Formally review the network design and implement consistent configuration standards and processes to promote network security.

- Formally review firewall and router security parameters to ensure they provide adequate protection.

- Maintain a complete and accurate listing of all servers that includes data on location, operating systems, and purpose.

- Formally assign security and monitoring responsibilities to ensure comprehensive and consistent security over LANs.

SYSTEMS SOFTWARE CONTROLS

Systems software consists of computer programs and related routines that control computer processing. The operating system is the prime component of system software; it controls the execution of user application programs.

Each system software product can be tailored to meet user needs. System tailoring is accomplished by setting optional system parameters and, therefore, has an impact on system performance and security.

We reviewed systems software controls and noted the following:

Zero Downtime Operating System (z/OS)

Control Objective - Management should ensure that operating systems are configured and controlled to promote security and integrity.

Tests Performed - Our review of z/OS included reviewing operating system parameters, security profiles and access to sensitive libraries, and staffing allocations. We performed auditor observations, conducted interviews, and performed testing including the use of an online product that provides detailed information on the hardware and software environment of the system, as well as security parameters and control mechanisms.

Results - z/OS is the primary mainframe operating system used at the CCF. It is a complex operating system used on mainframe computers and functions as the system software that controls the initiation and processing of all work within the computer. The continuing integrity of z/OS is critical to maintain confidence in the accuracy and security of programs and data under its control.

Our general objective was to review the z/OS operating system to assess the level of security and the integrity of controls in place within the operating system environment. No significant weaknesses were identified in our review. However, we recommend the Department continue to assess security over its systems, datasets, and libraries.

Virtual Machine (VM)

Control Objective - Management should ensure that operating systems are configured and controlled to promote security and integrity.

Tests Performed - Our review of VM included assessing controls over the VM directory and reviewing security parameters, performance and monitoring tools, and procedures for authorizing and adding new users.

Results - The VM operating system is the secondary mainframe operating system used at the CCF. VM creates a virtual environment for each system user. As far as users are concerned, they are in total control of the computer, a virtual storage device, a virtual printer, and possibly such devices as telecommunication lines. The illusion is so complete that other operating systems can be run on a virtual machine under the control of VM.

VM differs from the z/OS system in the security available to users, the way users are defined, and the types of applications available on the system. VM is similar to z/OS in that VM controls the initiation and processing of work in the computer. The integrity of VM is critical to maintaining confidence in the accuracy and security of programs and data under its control.

Although security over the VM operating system was reasonably well instituted, the Department should continue to discourage user agencies from permitting multiple users to write to a disk simultaneously, and periodically review IDs that can bypass password change requirements.

DataBase 2 (DB2)

Control Objective - Management should ensure that operating systems are configured and controlled to promote security and integrity.

Tests Performed - Our review of DB2 included a review of any significant modifications to the DB2 environment; identifying established subsystems; identifying Department and user agencies' roles and responsibilities; assessing established security parameters; reviewing access to sensitive administrative IDs and other resources; and reviewing established backup procedures and performance monitoring.

Results - DB2 is a relational database management system that the Department makes available to user agencies. No significant weaknesses were identified in our review of DB2.

Customer Information Control System (CICS)

Control Objective - Management should ensure that operating systems are configured and controlled to promote security and integrity.

Tests Performed - Our review of CICS included a review of any significant modifications to the CICS environment; assessing security parameters to determine if security was adequate and implemented at the transaction level; reviewing access to sensitive transactions and other CICS-related resources; and identifying established CICS levels of support for user agencies.

Results - CICS is a program product that enables transactions entered into remote terminals to be processed concurrently by user-written application programs. The Department supports CICS and makes it available to user agencies. No significant weaknesses were identified in our review of CICS. However, we recommend the Department continue to assess and strengthen security controls.

Advanced Interactive eXecutive (AIX)

Control Objective - Management should ensure that operating systems are configured and controlled to promote security and integrity.

Tests Performed - Our review of AIX included interviewing management and reviewing staffing levels, policies and procedures, backup and recovery procedures, the patch management program, network and user access, security logs, and auditing settings.

Results - AIX is a Unix-based operating system the Department uses to provide database, web, encryption, and backup services. No significant weaknesses were identified in our review. However, we recommend the Department continue to assess and strengthen security controls, and develop AIX specific policies and procedures.

Security Software

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.

Tests Performed - Our review of security software included reviewing security parameters and features; security reports; restriction of access to production data; procedures to log, review, and monitor security violations; and administrative authority and access to sensitive resources.

Results - The Department uses security software to control and monitor access to data maintained on its mainframe computers and other resources. The security software operates as an extension of, and an enhancement to, the operating systems. It provides a mechanism for controlling access and monitoring secured computer resources.

The security software protects by exception; that is, the user individually defines each dataset to be protected. It provides security and integrity capabilities that allow authorized users access to a defined set of protected resources, deny access to all other protected resources, and permit regular access to unprotected resources. The product limits users to the pre-defined datasets for which they have access authorization. In addition, the product maintains a log of all access attempts, which is used to monitor unauthorized access attempts and identify areas where security may need to be strengthened.

The security software protects access and enforces 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. Under the current environment, user agencies are responsible for specifying which datasets are to be protected and for properly using the available security resources.

Although reasonable systems software controls existed, we recommend the Department:

- Ensure all security profiles clearly identify the person or device assigned to IDs. As individual accountability is a primary security objective, the Department should, wherever possible, avoid the use of generically assigned IDs, unassigned IDs, and shared IDs. While there are cases where the use of such IDs is necessary, it should generally be prohibited unless absolutely necessary.

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

ACCOUNTING INFORMATION SYSTEM

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 and is currently utilized by 49 entities (see page 71 for the list of user agencies).

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.

Tests Performed - Our review of AIS included reviewing input controls, logical access and security controls, security of output documents, retention practices, backup and recovery procedures, change management procedures, and modifications to AIS during the fiscal year. In addition, we performed data integrity testing on two agencies' AIS data.

Results - Data entered into the system is the responsibility of user agencies. AIS has numerous edit checks built into the system to notify the users of any exceptions. Errors must be corrected before the transaction is accepted. AIS provides various online and batch reports to assist in the balance of transactions.

Access to AIS is controlled through security software, in addition to AIS' internal security. Users must have a properly authorized user ID and password to gain access to the operating environment. Once access to the operating environment has been allowed, users must have a separate application user ID and password to gain access to AIS. Assignment and authorization of access rights are the responsibility of each agency's security administrator.

There have been no significant changes to AIS in the past year.

AIS is automatically backed up daily, weekly, and monthly. The daily backups are maintained locally, while the weekly and monthly backups are rotated to the off-site location.

During our testing of AIS data, we did not identify any significant weaknesses. In addition, no significant weaknesses were identified in our overall review of AIS.

To ensure that controls are fully implemented and functional at the agency level, staff, internal auditors, and external auditors of agencies using AIS should:

- Verify that only accurate and authorized data are entered into AIS. It is the agency's responsibility to ensure that 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 user profiles and defined user groups with access to AIS to ensure access authorized is appropriate.

- Establish policies and procedures for the administration of user IDs.

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

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 Military Affairs
10. Department of Natural Resources
11. Department of Public Health
12. Department of Veterans' Affairs
13. Department on Aging
14. Environmental Protection Agency
15. General Assembly Retirement System
16. Guardianship and Advocacy Commission
17. Historic Preservation Agency
18. Human Rights Commission
19. Illinois Arts Council
20. Illinois Commerce Commission
21. Illinois Community College Board
22. Illinois Council on Developmental Disabilities
23. Illinois Criminal Justice Information Authority
24. Illinois Deaf and Hard of Hearing Commission
25. Illinois Educational Labor Relations Board
26. Illinois Labor Relations Board
27. Illinois Law Enforcement Training and Standards Board
28. Illinois Office of the State's Attorneys Appellate Prosecutor
29. Illinois Prisoner Review Board
30. Illinois Procurement Policy Board
31. Illinois Student Assistance Commission
32. Illinois Violence Prevention Authority
33. Illinois Workers' Compensation Commission
34. Judges' Retirement System
35. Judicial Inquiry Board
36. Office of Management and Budget
37. Office of the Attorney General
38. Office of the Auditor General
39. Office of the Executive Inspector General
40. Office of the Governor
41. Office of the Lieutenant Governor
42. Office of the State Appellate Defender
43. Office of the State Fire Marshal
44. Property Tax Appeal Board
45. State Board of Elections
46. State Employees' Retirement System
47. State Police Merit Board
48. State Universities Civil Service System
49. Supreme Court of Illinois

This Page Intentionally Left Blank

CENTRAL PAYROLL SYSTEM

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 Comptroller for the production of the agencies' payroll warrants.

CPS was implemented in July 1972 and is currently utilized by 75 entities (see page 75 for the list of user agencies).

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.

Tests Performed - Our review of CPS included reviewing input controls, logical access and security controls, security of output documents, retention practices, backup and recovery procedures, change management procedures, and modifications to CPS during the fiscal year. In addition, we performed data integrity testing on two agencies' CPS data.

Results - CPS transactions are entered online in a real-time environment, with the ability to batch transactions for processing at a later date. Most CPS user agencies enter their data online; however, Department personnel perform data entry for three agencies.

Data entered into the system is the responsibility of the user agency. The CPS has online edit checks to help prevent a user from entering a transaction with invalid data. If an error occurs during data entry, users are not allowed to continue until the error has been corrected.

Access to CPS is controlled through security software, in addition to CPS' internal security. Users must have a properly authorized user ID and password to gain access to the operating environment. Assignment and authorization of access rights are the responsibility of agency security administrators. Once access to the operating environment has been allowed, users must have a separate application user ID and password to gain access to CPS.

There have been no major changes to CPS in the past year.

CPS is automatically backed up daily and weekly. The daily backups are maintained locally, while weekly backups are rotated to an off-site storage location.

During our testing of CPS data, we did not identify any significant weaknesses. In addition, no significant weaknesses were identified in our overall review of CPS.

To ensure that controls are fully implemented and functional at the agency level, staff, internal auditors, and external auditors of agencies using CPS should:

- Verify that only accurate and authorized data are entered into CPS. It is the agency's responsibility to ensure that 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 security software profiles and defined user groups with access to CPS to ensure access authorized is appropriate.

- Establish policies and procedures for the administration of user IDs.

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

- Retain hardcopy payroll vouchers for at least the three most current pay periods, as specified by the CPS User Manual.

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.

This Page Intentionally Left Blank

CENTRAL INVENTORY SYSTEM

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 surplused, and updates of existing inventory items) are primarily entered into the CIS online real-time; meaning users' inventory data is updated immediately to reflect the transactions entered.

CIS was implemented in 1998 and is currently utilized by 26 entities (see page 79 for the list of user agencies).

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.

Tests Performed - Our review of CIS included reviewing input controls, logical access and security controls, security of output documents, retention practices, backup and recovery procedures, change management procedures, and modifications to CIS during the fiscal year. In addition, we performed data integrity testing on two agencies' CIS data.

Results - Data entered into the system is entered by the user agency, and is the responsibility of the agency. To help ensure the accuracy of the data, CIS is equipped with online edit checks that provide the user with immediate notification if errors are encountered during data entry, and processing edit checks that report processing errors online.

Error reports are available to CIS staff and to user agencies. The Department generates a Location Balance Report nightly to determine whether transactions were processed correctly. Additional reports are also available to users for reconciliation purposes. The accuracy and reconciliation of data is the responsibility of the user agency.

Access to CIS is controlled through security software, in addition to CIS' internal security. Users must have a properly authorized user ID and password to gain access to the operating environment. Once access to the operating environment has been allowed, users must have a separate application user ID and password to gain access to CIS. Assignment and authorization of access rights are the responsibility of agency security administrators.

There have been no significant changes to CIS in the past year.

CIS is automatically backed up daily. The daily backups are maintained locally, while monthly backups are rotated to an off-site storage location.

During our testing of CIS data, we did not identify any significant weaknesses. In addition, no significant weaknesses were identified in our overall review of CIS.

To ensure that controls are fully implemented and functional at the agency level, staff, internal auditors, and external auditors of agencies using CIS should:

- Verify that only accurate and authorized data are entered into CIS. It is the agency's responsibility to ensure that 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 user profiles and defined user groups with access to CIS to ensure access authorized is appropriate.

- Establish policies and procedures for the administration of user IDs.

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

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 Financial and Professional Regulation
6. Department of Human Rights
7. Department of Military Affairs
8. Department of Natural Resources
9. Department of Public Health
10. Department of Transportation
11. Department of Veterans' Affairs
12. Department on Aging
13. Environmental Protection Agency
14. Historic Preservation Agency
15. Illinois Deaf and Hard of Hearing Commission
16. Illinois Educational Labor Relations Board
17. Illinois Law Enforcement Training and Standards Board
18. Illinois Office of the State's Attorneys Appellate Prosecutor
19. Illinois Procurement Policy Board
20. Illinois Student Assistance Commission
21. Illinois Violence Prevention Authority
22. Illinois Workers' Compensation Commission
23. Office of Management and Budget
24. Office of the Attorney General
25. Office of the Governor
26. Office of the Lieutenant Governor

This Page Intentionally Left Blank

CENTRAL TIME AND ATTENDANCE SYSTEM

The Central Time and Attendance System (CTAS) is an online system that provides a comprehensive system for recording and managing employee benefit time.

CTAS was implemented in 1992 and is currently utilized by 31 entities (see page 83 for the list of user agencies).

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.

Tests Performed - Our review of CTAS included reviewing input controls, logical access and security controls, security of output documents, retention practices, backup procedures, change management procedures, and modifications to CTAS during the fiscal year. In addition, we performed data integrity testing on two agencies' CTAS data.

Results - 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 timekeeper to enter or confirm an employee's general attendance information. The exception method assumes that an employee's scheduled work time is the correct attendance unless the timekeeper enters something different.

Data entered into the system is the responsibility of the user agency. CTAS has hundreds of edit checks built into the system to notify the user of any exceptions.

Access to CTAS is controlled through security software, in addition to CTAS' internal security. Users must have a properly authorized user ID and password to gain access to the operating environment. Assignment and authorization of access rights are the responsibility of each agency's security administrator. Once access to the operating environment has been allowed, users must have a separate application user ID and password to gain access to CTAS.

The interface between CTAS and CPS to reduce duplicative entry between the two applications has been completed. In addition, the system was updated to incorporate the new Equivalent Earned Time Policy.

CTAS is automatically backed up daily and weekly. The daily backups are maintained locally, while weekly backups are rotated to an off-site storage location.

During our testing of CTAS data, we did not identify any significant weaknesses. In addition, no significant weaknesses were identified in our overall review of CTAS.

To ensure that controls are fully implemented and functional at the agency level, staff, internal auditors, and external auditors of agencies using CTAS should:

- Verify that only accurate and authorized data are entered into CTAS. It is the agency's responsibility to ensure that 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 user profiles and defined 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.

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 Council on Developmental Disabilities
18. Illinois Criminal Justice Information Authority
19. Illinois Deaf and Hard of Hearing Commission
20. Illinois Educational Labor Relations Board
21. Illinois Law Enforcement Training and Standards Board
22. Illinois 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.
User agency security coordinators should effectively utilize security software features and perform periodic reviews of existing profiles to ensure access rights are appropriate. In addition, user agency security coordinators should:

- Formally encourage users to include both alphabetic and non-alphabetic characters in their passwords to protect the security of their account.
- Examine inactive or revoked IDs, and delete IDs that are no longer necessary.
- When users are required to have the ability to reset passwords, utilize the Department's password reset utilities; powerful attributes should only be assigned to users who need administrative capabilities.

Security over Local Area Network (LAN) resources should be reviewed.
To enhance LAN security, agencies should:

- Develop and implement a Security Awareness Program to keep employees aware of security issues.
- Perform a risk assessment to evaluate the strength of their internal LAN security.
- Update all servers to the current vendor recommended patch level.
- Install and continuously update virus detection software.

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 over Networks 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 Customer Information Control System (CICS) should be reviewed.
User agencies should:

- Coordinate with the Department to assure the 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 powerful CICS commands are adequately restricted.

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, staff, internal auditors, and external auditors of agencies using AIS should:

- Verify only accurate and authorized data are entered into AIS. It is the agency's responsibility to ensure that 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 user profiles and defined user groups with access to AIS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up AIS reports, and inform appropriate AIS personnel of changes timely.

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 controls are functional at the agency level, agencies should:

- Verify only accurate and authorized data are entered into CPS. It is the agency's responsibility to ensure that only properly authorized transactions are entered into the system.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the users and user groups with access to CPS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up payroll reports, and inform appropriate CPS personnel of changes timely.
- Retain hardcopy payroll vouchers for at least the three most current pay periods, as specified by the CPS User Manual.

Central Inventory System (CIS) use should be reviewed.
We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, staff, internal auditors, and external auditors of agencies using CIS should:

- Verify only accurate and authorized data are entered into CIS. It is the agency's responsibility to ensure that 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 user profiles and defined user groups with access to CIS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up inventory reports, and inform appropriate CIS personnel of changes timely.

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 controls are functional at the agency level, agencies should:

- Verify only accurate and authorized data are entered into CTAS. It is the agency's responsibility to ensure that 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 user profiles and defined 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. Please feel free to contact the Office at 217-782-6046 or auditor@mail.state.il.us.

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 Labor
17. Department of Military Affairs
18. Department of Natural Resources
19. Department of Public Health
20. Department of Revenue
21. Department of Transportation
22. Department of Veterans' Affairs
23. Department on Aging
24. East St. Louis Financial Advisory Authority
25. Eastern Illinois University
26. Emergency Management Agency
27. Environmental Protection Agency
28. Executive Ethics Commission
29. General Assembly (Senate Operations)
30. General Assembly Retirement System
31. Governors State University
32. Guardianship and Advocacy Commission
33. Historic Preservation Agency
34. House of Representatives
35. House Republican Staff
36. Human Rights Commission
37. Illinois Arts Council
38. Illinois Civil Service Commission
39. Illinois Commerce Commission
40. Illinois Community College Board
41. Illinois Council on Developmental Disabilities
42. Illinois Criminal Justice Information Authority
43. Illinois Deaf and Hard of Hearing Commission
44. Illinois Educational Labor Relations Board
45. Illinois Finance Authority
46. Illinois Housing Development Authority
47. Illinois Labor Relations Board
48. Illinois Law Enforcement Training and Standards Board

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

APPENDIX C

ACRONYM GLOSSARY

ACL – Access Control List

AIS - Accounting Information System

AIX – Advanced Interactive eXecutive

ARB – Architecture Rationalization Board

ARCM - Accounts Receivable Credit Memorandum

ARPS – Accounts Receivable Posting System

BAS – Billing Allocation System

BCCS - Bureau of Communication and Computer Services

Bureau - Bureau of Communication and Computer Services

CAF - Credit Adjustment Form

CCF - Central Computer Facility

CDPD - Cellular Digital Packet Data

CHRI - Criminal History Record Information

CICS - Customer Information Control System

CIS - Central Inventory System

CMC – Customer Management Center

CMS - Central Management Services

CPU – Central Processing Unit

CPS - Central Payroll System

CRF - Communication Revolving Fund

CSD - CICS System Definition File

CTAS - Central Time and Attendance System

DB2 - DataBase 2

DCMS - Department of Central Management Services

Department - Department of Central Management Services

DP Guide – Data Processing Guide

EA&S – Enterprise Architecture and Strategy

EPMO – Executive Program Management Office

FCIAA – Fiscal Control and Internal Auditing Act

FY – Fiscal Year

HIPAA – Health Insurance Portability and Accountability Act

IBiS – Internet Billing System

ICN – Illinois Century Network

ILCS – Illinois Compiled Statutes

IMS – Information Management System

IOIA – Illinois Office of Internal Audit

ISD – Information Services Division

IT - Information Technology

IWIN - Illinois Wireless Information Network

LAN - Local Area Network

LEADS - Law Enforcement Agencies Data System

MDC - Mobile Data Computer

MONIES - Management of Network Income Expense Services System

NCC - Network Control Center

NCIC - National Crime Information Center

NLETS - National Law Enforcement Telecommunications System

OA - Office Automation

PKI - Public Key Infrastructure

QA – Quality Assurance

SAMS - Statewide Accounting Management System

SLA – Service Level Agreement

SNA - Systems Network Architecture

SOS – Secretary of State

SR- Service Request

SRRS - Service Request Registration System

SSRF - Statistical Services Revolving Fund

TCP/IP - Transmission Control Protocol/Internet Protocol

TDR - Telecommunications Data/Intercity Service Request

TGR - Terminal Generation Request

TSR - Telecommunications Service Request

UPS - Uninterruptible Power Supply

VM - Virtual Machine

WAN - Wide Area Network

z/OS - Zero Downtime Operating System