SERVICE ORGANIZATION CONTROL REPORT

Department of Central Management Services
Bureau of Communications and Computer Services

July 2014

TABLE OF CONTENTS

CMS
ILLINOIS Pat Quinn, Governor
DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
Simone McNeil, Acting Director

July 15, 2014

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

RE: Management of the Department of Central Management Services, Bureau of Communications and Computer Services' Assertion Regarding the State of Illinois Mainframe Information Technology Environment System for the Period July 1, 2013 to June 30, 2014

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

We have prepared the attached description titled "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' State of Illinois Mainframe Information Technology Environment System Throughout the Period July 1, 2013 to June 30, 2014" (the description), based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraphs 1.34–.35 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the State of Illinois Mainframe Information Technology Environment, particularly system controls intended to meet the criteria for the security, availability, and processing integrity principles set forth in the 2014 version of TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the State of Illinois Mainframe Information Technology Environment System throughout the period July 1, 2013 to June 30, 2014 based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided

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

- *Infrastructure.* The physical, IT and other hardware components of a system (facilities, equipment, and networks).

- *Software*. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
- *People*. The personnel involved in the governance, operation and use of a system (developers, operators, users, vendor personnel and managers).
- *Procedures*. The automated and manual procedures involved in the operation of a system.
- *Data*. The information used and supported by a system (transaction streams, files, databases, and tables).

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

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

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

(6) If information is provided to, or received from, subservice organization or other parties, how such information is provided or received; the role of the subservice organization or other parties; and the procedures performed to determine that such information and its maintenance, and storage are subject to appropriate controls

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

(8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria

(9) Any applicable trust services criteria that are not addressed by a control at the Department of Central Management Services, Bureau of Communications and Computer Services or a subservice organization and the reasons therefore

(10) Other aspects of the Department of Central Management Services, Bureau of Communications and Computer Services control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria

(11) Relevant details of changes to the Department of Central Management Services, Bureau of Communications and Computer Services, State of Illinois

Mainframe Information Technology Environment System during the period covered by the description

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

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

c. the controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.

Sincerely,

Greg Wass, Deputy Director
Illinois Department of Central Management Services
Bureau of Communication and Computer Services

CC: Simone McNeil, Acting Director
Illinois Department of Central Management Services

This page intentionally left blank

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

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

Office Of The Auditor General
William G. Holland

INDEPENDENT SERVICE AUDITOR'S REPORT

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

Scope
We have examined the attached Description titled "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' State of Illinois Mainframe Information Technology Environment System Throughout the Period July 1, 2013 to June 30, 2014" (the Description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the security, availability, and processing integrity principles set forth in the 2014 version of TSP Section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), throughout the period July 1, 2013 to June 30, 2014. The Description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-agency controls contemplated in the design of the Department of Central Management Services, Bureau of Communications and Computer Services' controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-agency controls.

The Department utilizes a service organization to provide an alternate data center for off-site storage of backups and disaster recovery services. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The Description presents the Department of Central Management Services, Bureau of Communications and Computer Services' State of Illinois Mainframe Information Technology Environment System; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet certain applicable trust services criteria. The Description does not include any of the control implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization.

The Description indicates that certain applicable trust services criteria specified in the Description can be achieved only if complementary user-agency controls contemplated in the design of the Department of Central Management Services, Bureau of Communications and Computer Services' controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-agency controls.

Service organization's responsibilities

The Department of Central Management Services, Bureau of Communications and Computer Services has provided the attached assertion titled "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' Assertion Regarding the State of Illinois Mainframe Information Technology Environment System Throughout the Period July 1, 2013 to June 30, 2014", which is based on the criteria identified in management's assertion. The Department of Central Management Services, Bureau of Communications and Computer Services is responsible for (1) preparing the Description and assertion; (2) the completeness, accuracy, and method of presentation of both the Description and assertion; (3) providing the services covered by the Description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the Description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description based on the Description criteria set forth in the Department of Central Management Services, Bureau of Communications and Computer Services' assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants and the standards applicable to attestation engagements contained in Government Auditing Standards issued by the Comptroller General. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is fairly presented based on the Description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period July 1, 2013 to June 30, 2014.

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

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

Opinion
The Department of Central Management Services, Bureau of Communications and Computer Services states in the Description that in order for mainframe password resets for Department and proxy agency user profiles to be completed, an email request to the Help Desk is to be submitted or the Department's Identity Management website is to be accessed. However, as noted on page 59 of the Description of Tests of Controls and Results Thereof, the password resets were completed via direct phone call or email to the Department's Security Software Coordinator, the Security Software Administrator or the Help Desk. Thus, the control over the reset of mainframe passwords was not operating effectively throughout the period July 1, 2013 to June 30, 2014. This control deficiency resulted in not meeting the criterion "Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them."

In addition, the Department of Central Management Services, Bureau of Communications and Computer Services states in the Description that the Department's Compliance Officer is responsible for monitoring and ensuring compliance with security policies. However, as noted on page 42 of the Description of Tests of Controls and Results Thereof, monitoring for compliance had not been conducted. Thus, the control over the monitoring of compliance with security policies was not operating effectively throughout the period July 1, 2013 to June 30, 2014. This control deficiency resulted in not meeting the criterion "The Department has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security, availability, and processing integrity."

The Department of Central Management Services, Bureau of Communications and Computer Services also states in the Description that risk assessments are to be performed periodically and, as security threats are identified, they are to be assessed. However, as noted on pages 48, 49, and 50 of the Description of Tests of Controls and Results Thereof, the Department had not conducted risk assessments to identify threats, vulnerabilities and assessed their impact. Thus, the control over risk assessments was not operating effectively throughout the period July 1, 2013 to June 30, 2014. This control deficiency resulted in not meeting the criterion "The Department (1) identifies potential threats that would impair system security, availability, and processing integrity commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines migration strategies for those risks."

In our opinion, except for the matters referred to in the three preceding paragraphs, based on the Description criteria identified in the Department of Central Management Services, Bureau of

Communications and Computer Services' assertion and the applicable trust services criteria, in all material respects

a. the Description fairly presents the system that was designed and implemented throughout the period July 1, 2013 to June 30, 2014.

b. the controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period July 1, 2013 to June 30, 2014, the subservice organization applied, the types of controls expected to be implemented at the subservice organization and incorporated in the design of the system, and user-agencies applied the complementary user-agency controls contemplated in the design of the Department of Central Management Services, Bureau of Communications and Computer Services' controls throughout the period July 1, 2013 to June 30, 2014.

c. the controls tested, which together with the types of controls expected to be implemented at the subservice organization and incorporated in the design of the system, and the complementary user-agency controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period July 1, 2013 to June 30, 2014.

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

Other Information Provided by the Department of Central Management Service, Bureau of Communications and Computer Services That is Not Covered by the Service Auditor's Report
The information attached to the Description titled "Other Information Provided by the Department of Central Management Services, Bureau of Communications and Computer Services That Is Not Covered by the Service Auditor's Report" describes staffing trends, user agency listings, and the Department's Corrective Action Plan. It is presented by the management of the Department of Central Management Services, Bureau of Communications and Computer Services to provide additional information and is not a part of the Department of Central Management Services, Bureau of Communications and Computer Services' Description of the State of Illinois Mainframe Information Technology Environment System made available to user-agencies during the period from July 1, 2013 to June 30, 2014. Information about the Department of Central Management Services, Bureau of Communications and Computer Services' staffing issues, user listings, and Department's Corrective Action Plan have not been subjected to the procedures applied in the examination of the Description of the State of Illinois Mainframe Information Technology Environment System and the suitability of the design and operating effectiveness of controls to meet the related criteria stated in the Description of the State of Illinois Mainframe Information Technology Environment System, and, accordingly, we express no opinion on it.

Intended use

This report and the Description of Tests of Controls and Results Thereof are intended solely for the information and use of the Department of Central Management Services, Bureau of Communications and Computer Services' user-agencies of the "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' Assertion Regarding the State of Illinois Mainframe Information Technology Environment System" during some or all of the period July 1, 2013 to June 30, 2014, the Auditor General, the General Assembly, the Legislative Audit Commission, the Governor, and independent auditors and practitioners providing services to such user-agencies, and regulators who have sufficient knowledge and understanding of the following:

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

This report is a matter of public record and the distribution is not limited; however, the endorsed use of the Report is outlined in the Intended Use Section.

William J. Sampias, CISA
Director, Information Systems Audits

Mary Kathryn Lovejoy, CPA, CISA
Audit Manager

July 15, 2014
Springfield, Illinois

This page intentionally left blank

DESCRIPTION OF THE
DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
BUREAU OF COMMUNICATIONS AND COMPUTER SERVICES'
STATE OF ILLINOIS MAINFRAME INFORMATION TECHNOLOGY
ENVIRONMENT SYSTEM
THROUGHOUT THE PERIOD JULY 1, 2013 TO JUNE 30, 2014

Background

The Department of Central Management Services Bureau of Communications and Computer Services carries out statutory responsibilities relating to data processing and telecommunication services (20 ILCS 405/405-10; 20 ILCS 405/405-20; 20 ILCS 405/405-250; 20 ILCS 405/405-255; 20 ILCS 405/405-260; 20 ILCS 405/405-270; and 20 ILCS 405/405-410).

The Bureau of Communications and Computer Services:

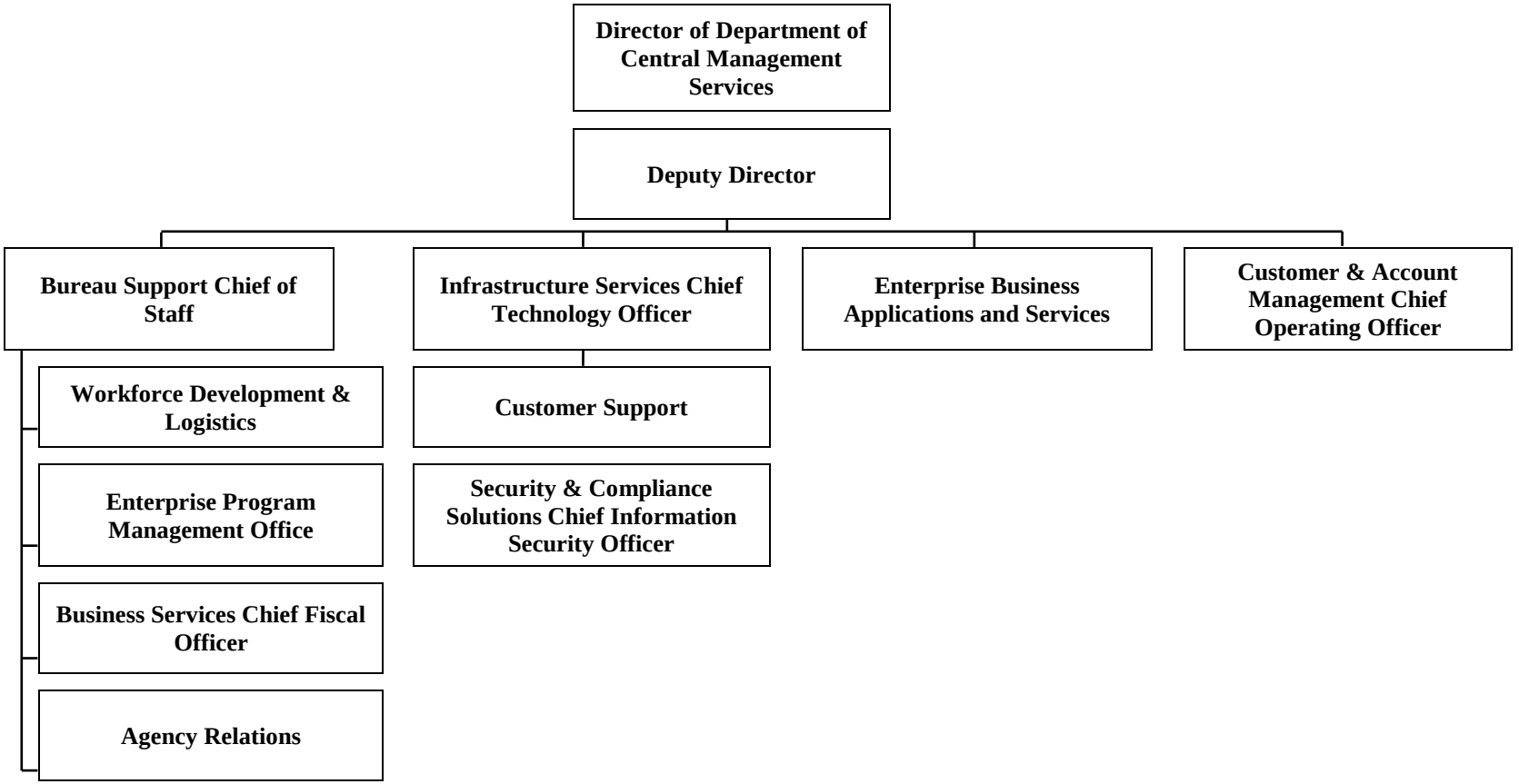
- Manages the planning, procurement, maintenance, and delivery of voice, data, wireless, video, Internet, and telecommunications services to all state government agencies, boards, commissions, and state supported institutions of higher education in Illinois, as well as other governmental and some non-governmental entities.
- Operates the Central Computer Facility, as well as other facilities, which provides mainframe processing systems and support for most state agencies, boards, and commissions.
- Maintains applications that state government agencies, boards, and commissions may utilize to meet their financial requirements.

Management Philosophy

The Department of Central Management Services, Bureau of Communications and Computer Services' control environment reflects the values of the Department regarding the importance of security over the infrastructure, users' data and information. The Bureau of Communications and Computer Services' management ensures the importance of security is adequately communicated to all levels within the Department and agency users.

Organization and Management

The Department of Central Management Services, Bureau of Communications and Computer Services is divided into several divisions in order to provide services to its users.



Deputy Director

The Deputy Director of the Bureau of Communications and Computer services is responsible for the overall management of all Information Technology and Telecommunication functions, which include services provided to all state agencies as well as other Illinois government entities. The Deputy Director works with Department senior management, the Governor's Office and the State's Chief Information Officer to develop policies, priorities and plans for statewide Information Technology and Telecommunication programs. The Deputy Director is responsible for the follow teams:

Chief Operating Officer

The Chief Operating Officer serves as a policy formulating administrator in planning, directing, implementing and administering the Customer and Account Management group. The Customer and Account Management group is the single point of contact for user service requests, service provisioning, and incident management.

- Customer Service Center (CSC)
  The CSC serves as the central point of contact for telecommunications and information technology users. The CSC serves as a Help Desk to handle, process, and manage incidents and requests for services.

- Communications Management Center (CMC)
  The CMC is responsible for all network trouble resolutions, surveillance, and ongoing technical support. The CMC is operational 24x7, and handles after hours calls of the Customer Service Center (CSC).

- Field Operations / Regional Technology Centers (RTC)
  Field Operations is responsible for maintaining nine Regional Technology Centers located throughout the State and assisting Network Services in maintaining Illinois Century Network Point-of-Presence (POP) sites throughout the State.

- Network Services
  Network Services is responsible for management and oversight of the Illinois Century Network (ICN), the Illinois Wireless Information Network, and all engineering responsibilities related to State of Illinois telecommunications services.

    - 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 III network support to other staff within Network Services.

    - Enterprise Network Support is responsible for design and support of State agencies network access. Responsibilities include installation and support of access routers, Wide Area Network (WAN) switches, Voice Over Internet Protocol (VOIP), video conferencing, fiber, Domain Name Service (DNS), and

Internet. Network Integration also performs tier III technical support for the Customer Management Service (CMC) and directly to state agencies.

- LAN Services
  LAN Services is responsible for entering rules into the firewalls and monitoring security violations. Additionally, this group is responsible for consolidated and managed agencies LAN networks, which includes: firewalls, routers, switches, hubs, Intrusion Detection System (IDS) and wireless switches.

Chief of Staff

The Chief of Staff serves as advisor to the Deputy Director on strategic, operational and problem resolution issues, serves as the primary resource between the Deputy Director and senior management, and performs special projects related to Bureau operations.

- Workforce Development and Logistics
  The Workforce Development and Logistics coordinates and facilitates internal personnel paperwork, workforce training, development and implementation, and workforce logistics for the Bureau.

- Enterprise Program Management Office
  The Enterprise Program Management Office (EPMO) develops and implements enterprise project management policies, processes, and services, as well as other related project management support activities. The EPMO directly manages large, complex (Tier 3) projects, and oversees all other projects that meet the criteria for IT Governance (Tier 2).

- Chief Fiscal Officer
  The Chief Fiscal Officer oversees the management of the fiscal operations for the Bureau. This position administers the Communications Revolving Fund (CRF), the Statistical Services Revolving Fund (SSRF), and the General Revenue Fund (GRF) for educational technology (Illinois Century Network).

Chief Technology Officer

The Chief Technology Officer oversees the Infrastructure Services Division in order to provide continuous oversight, operation, and support of the State's Information Technology infrastructure. The Infrastructure Services Division is divided into several teams:

- Data Center Operations
  Mainframe Services is responsible for the mainframe operating systems, database systems, and software installation, maintenance, and support function/services.

  Enterprise Storage and Backup is responsible for the oversight and management of the storage and backup systems across all platforms.

- Enterprise Production/Operations
  Library Services is responsible for media initiation, inventory, tracking, lifecycle management, and business continuity media management.

Production Control is responsible for computer job scheduling and monitoring.

Command Center Operations is responsible for providing continuous monitoring and operation of the Department's computing resources to ensure availability, performance, and support response necessary to sustain user business demands.

- Customer Support
  The Customer Support Division is responsible for the End-User Computer Unit, which installs and supports PC's and laptops for all consolidated agencies, and the IT Help Desk, which supports users for all IT functions.

- Chief Information Security Officer
  The Chief Information Security Officer serves as a policy making official responsible for policy development, planning, implementation, and administration of the Security and Compliance Solutions division. The Chief Information Security Officer is responsible for overseeing and implementing the sensitive and confidential Information Technology security program for agencies, boards and commissions under the jurisdiction of the Governor.
    - Security and Compliance Solutions (S&CS)
      Security and Compliance Solutions has the following responsibilities:
        - Providing the IT security program statewide to agencies;
        - Communicating security principles through issuance of policies and hosting education opportunities;
        - Alerting users to known occurrences or potential imminent threats that could cause risk to cyber resources;
        - Notifying the applicable management of non-compliance/violations of the systems security;
        - Developing and assessing risk associated with specific business information systems and developing appropriate remediation plans;
        - Conducting security testing of the infrastructure; and
        - Developing and maintaining the statewide disaster recovery services for the State's Information Technology infrastructure.

Enterprise Business Applications and Services

The Enterprise Business Applications and Services (EBAS) Division is responsible for the development and maintenance of the applications, which are available for use by user agencies. The Division is responsible for the maintenance and support of the applications used by agencies, including Accounting Information System (AIS), Central Payroll System (CPS), Central Inventory System (CIS), Central Time and Attendance System (CTAS), and eTime.

Department management reviews the organizational structures and staffing vacancies at their weekly management meetings. Weekly, Department management reports to the Governor's office the critical structural and staffing needs.

The Department adheres to the State's hiring procedures; Personnel Code, Union Contracts and Rutan decisions, for the hiring of staff. Once a job description is in place Personnel initiates a

Personnel Action Request (PAR) and then an Electronic Personnel Action Request (ePAR) in order to request to fill a vacancy. Once the ePAR is approved by Administrative and Regulatory Shared Services, Department's Chief Financial Officer, Department's Director and the Governor's Office of Management and Budget; Administrative and Regulatory Shared Services will begin the hiring process by posting the vacant position. Upon employment, the Administrative and Regulatory Shared Services provides new employee orientation. During orientation, new employees complete various forms and training.

Personnel work with the section managers to develop position descriptions. Once completed, the position description is sent to the Administrative and Regulatory Shared Services and to the Department's Technical Services in order for the position to be created. Each position is to have a position description which outlines the duties and qualifications

Upon separation from the Department, Personnel complete a PAR, which notifies the Department's Chief Fiscal Officer of the departure. In addition, Personnel send the employee's supervisor an Exit Form which outlines the items to be retrieved and deactivation of access.

The training office works with managers to identify training needs, registers employees for training, and tracks all training in a database.

New Department staff is required to sign a statement signifying that they will comply with the security policies. Additionally, Department staff reconfirms their compliance with the security policies through annual security awareness training. Contractors are also required to take the annual security awareness training and signify they will comply with security policies.

Communication

The Department has published on their website the Service Catalog which agencies may utilize in determining their required services. The Service Catalog provides information related to the services provided, what the service includes, and rates charge.

The Department has implemented several policies to address an array of security issues; physical and logical. The policies are applicable not only to the Department, but to user agencies. The Department's Compliance Officer is responsible for monitoring and ensuring compliance with policies and procedures.

The Department has posted the following policies on their website.

Information Technology Policies

- Data Classification Policy;
- Enterprise Desktop/Laptop Policy;
- General Security for Statewide IT Resources Policy;
- General Security for Statewide Network Resources Policy;
- IT (Information Technology) Recovery Policy;
- Recovery Methodology;

- IT Resource Access Policy;
- Laptop Data Encryption Policy;
- Backup Retention Policy;
- Statewide CMS/BCCS Facility Access Policy; and
- IT (Information Technology) Risk Assessment Policy.

General Policies

- Change Management Policy;
- Data Breach Notification Policy;
- Action Plan for Notification of a Security Breach;
- Electronically Stored Information Retention Policy;
- IT Governance Policy;
- Mobile Device Security Policy; and
- Wireless Communication Device Policy.

In addition, to the security policies, the security obligations of Department staff are communicated via mandatory annual security awareness training.

The policies, along with the application user manuals, document the reporting process of system problems, security issues, and user assistance to the Help Desk. In addition, the Department has developed procedures for the identification and escalation of security breaches to Department management.

Risk Management

The Department has developed the IT Risk Assessment Policy to guide the Department's risk process. The Department is to conduct periodic risk assessments, which identify threats and vulnerabilities, and assess the impact. In addition, the Department is to remediate any risks which are identified.

As part of the planning process, the Department considers technological developments and laws and regulations.

Monitoring

Mainframe system performance and capacity is monitored by System Software programming personnel. Remote Monitoring Facility (RMF) reports are run weekly and monthly. Performance and capacity monitoring is documented via internal memorandum distributed to management.

The Operation Center continuously monitors the operation of the computing resources to ensure availability, performance, and response necessary to sustain user business demands. The Operation Center operates 24 hours a day, 7 days a week, 365 days a year.

The Operations Center utilizes software and the Automated Operations Console in order to continuously monitor the environment. Problems, issues, and incidents are recorded via the Daily Shift Reports and a Remedy Ticket is created. In the event the Operations Center cannot resolve the issue, the Remedy Ticket is assigned to the applicable division for resolution.

The Daily Shift Report documents the activity conducted on all mainframe production systems and incident calls received at the Operations Center. The Report contains the date, time, system involved in the incident, along with a narrative providing any necessary information regarding the incident.

In the event division staff or management needs to be notified, contact information is maintained within the FOCAL database.

The Operator Shift Change Checklist is completed at the beginning of each shift to ensure the production systems are operating appropriately and any open items are passed on to the next shift. The Checklists are reviewed by the supervisor.

The Shift Change Checklist and the Daily Shift Report issues are reviewed each morning at the 8:45 meeting. Staff from various divisions and user agency staff are in attendance.

The Department has developed the Data Processing Guide in order to provide staff with instruction related to their various tasks.

Department staff and users are instructed to contact the Help Desk or their supervisor to report any and all security, availability and processing issues. Staff and users may contact the Help Desk via phone or email to report an incident. When a report is received, the Help Desk staff open a ticket in Remedy and record the incident, as well as the user name, agency, contact information and a detailed incident description. The ticket is tracked through Remedy until resolution.

The Mobile Device Security Policy and the Enterprise Desktop/Laptop Policy requires users to report to the Help Desk any lost or stolen equipment. Upon notification, the Help Desk creates a Help Desk Ticket within Remedy, attaches the police report, if reported, and assigns the Ticket to the Asset Management staff. Upon assignment to the Asset Management staff, the Help Desk staff responsibility is completed. In addition, EUC is to be notified in order to determine if the equipment had encryption installed and if confidential information was retained on the equipment. In the event the determination is made confidential information was retained, then the S&CS Group is to be notified.

In the event a breach was identified, the Department will utilize the Data Breach Notification Policy and the Action Plan for Notification of a Security Breach. In addition, a Remedy ticket will be opened and if necessary the Technical Safeguards team will be alerted.

Logical and Physical Environment

The Department's mainframe configuration consists of several CMOS processors located in the Department's Central Computer Facility (CCF). The mainframe is partitioned into logical partitions consisting of production, test, and continuous service. Several partitions are configured in a SYSPLEX (coupling facility). The mainframe operating system software includes:

- The primary operating systems:
    - 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.
    - z/Virtual Machine (z/VM) is a time-sharing, interactive, multi-programming operating system.

- The primary subsystems:
    - 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.
    - DataBase 2 (DB2) is a relational database management system for z/OS environments.
    - Information Management System (IMS), which is an online database software subsystem, is used as the control architecture under which online database system applications process. An IMS system is capable of running many different applications within a single definition of one or more "Message Processing Region" and one "Control Region".

Access to operating system configurations is limited to system support personnel including system programmers and security software personnel.

The Department utilizes security software as its primary method for controlling and monitoring access to the Department's mainframe resources. The security software is designed to control access and for monitoring of secured computing resources. The security software operates as an extension of, and an enhancement to the operating system.

There are two individuals with primarily responsible for the security, administration and support; Security Software Administrator for CMS/BCCS/S&CS and the Security Software Coordinator. In addition, several of the larger agencies have in-house security software coordinators, who are responsible for the administration and support of their agencies' security software IDs.

The Security Software Coordinator is responsible for supporting the security software, in addition to supporting specific Departmental IDs; creation, modification, revocation and monitoring. The Security Software Administrator for CMS/BCCS/S&CS is responsible for

Departmental and proxy agencies' IDs; creation, modification, revocation, and monitoring.

The Department has developed several procedures which address ID management, handling forgotten passwords, privileged attributes, security options, and monitoring.

The mainframe security software requires users to have an established ID and password in order to verify the individual's identity. The primary means of defining a user's access to resources is the security software resource profile, which defines the level of access a user may have. There are three privileged attributes which can be assigned to user IDs at both a system-wide and group level.

The Department has restricted access with powerful privileges, high-level access, and access to sensitive system functions to authorized personnel.

Mainframe security software password standards have been established. In addition, passwords are maintained in an encrypted database.

In order for the Security Software Coordinator or the Security Software Administrator for CMS/BCCS/S&CS to create an ID, an Enterprise Service Request (ESR) with an approved Mainframe Security Request Form is to be completed. The Mainframe Security Request Form is to indicate the access required and be approved. In the event the request is for a non-expiring ID, the Chief Information Security Officer is required to approve the Mainframe Security Request Form.

Upon creation, the Security Software Coordinator or the Security Software Administrator for CMS/BCCS/S&CS will contact the individual's supervisor with the ID and temporary password. The password being temporary requires the individual to change it upon initial login.

In the event an ID needs to be modified, an email or ESR is received, with the Mainframe Application Request Form attached. The necessary modifications are made and the requestor is phoned indicating such action has taken place.

The Security Software Coordinator or the Security Software Administrator for CMS/BCCS/S&CS will reset a password upon assignment of an ESR from the Help Desk. Upon receipt, the Security Software Coordinator or the Security Software Administrator for CMS/BCCS/S&CS will reset the password with a temporary password and phone the individual.

In addition, a user may contact the Help Desk via email or submit a problem report via the Department's website for assistance in resetting their password or utilize the Department's Identity Management Website. The Help Desk has developed Methods and Procedures for resetting mainframe passwords.

The Help Desk staff have access to specific security software groups which allows them to reset security software passwords.

When an individual terminates or no longer requires access; an Exit Form is received, the Security Software Coordinator or the Security Software Administrator for CMS/BCCS/S&CS will deactivate the ID.

Twice a year, the Security Software Administrator for CMS/BCCS/S&CS will send out to the agencies the Security Reconciliation Reports for review. Once returned, the appropriate corrections are made.

The Department also maintains the State of Illinois Statewide Network, which consists of firewalls, routers and switches. Network Operations and Enterprise Network support are primarily responsible for networking equipment at the core, distribution, and access levels; while LAN Services is primarily responsible for networking equipment at the CCF and State agency level.

Network diagrams are maintained by Network Services depicting the network infrastructure and placement of firewalls, routers and switches.

Networking devices are configured to utilize authentication servers, logging servers, and contained banners prohibiting unauthorized access and warning of prosecution. In addition, devices contain Access Control Lists (ACLs) to deny and permit specific types of network traffic.

Authentication servers are utilized to provide authorized access to the firewalls, routers, and switches. The authentication servers utilize an administrative architecture in which groups are established with specific levels of administrative privileges for the individual's needs. Individual users (and IDs) are then assigned to appropriate groups. Password parameters have been established for users in each of these groups.

Network Services is notified by Personnel when a new individual begins employment, or changes occur in an existing individual's employment. Once notified, the Network Services Management will decide the appropriate access privileges to be granted to the individual.

In order to ensure proper access is assigned to the LAN Services technicians, LAN Services utilizes the LAN Equipment Access Rights Standard. The Standard requires supervisors to complete the LAN Services Access Rights Authorization (Form) for new individuals to obtain access. In addition, the Form is to be completed for changes to existing employee rights.

Authentication servers utilized by Network Operations and Enterprise Network Support are configured to log failed access attempts. Logs are maintained locally on the authentication servers; as well as, to two external logging servers.

Authentication servers utilized by LAN Services are configured to log failed access attempts. The authentication services provide alerts to staff. Logs are maintained locally on the authentication server.

Network Services also utilizes a product which monitors the syslogs for repeated failed access authorization attempts to networking devices from the same IP addresses. When the product recognized such attempts it places temporary commands in the configurations, and the administrators are notified.

Network Operations and Enterprise Network Support have configured servers to function as the primary logging servers for the firewalls, routers, and switches it maintains. LAN Services has configured servers to function as the primary logging servers for the firewalls, routers, and switches it maintains.

Network Operations and Enterprise Support maintain a SolarWinds server and software for the devices managed and maintained. LAN Services maintains a separate server and software for the devices managed and maintained.

SolarWinds Network Performance Manager (NPM) is utilized to monitor performance related issues such as up/down devices, bandwidth utilization, CPU utilization, etc., and will alert administrators as necessary.

To assist in the configuration and deployment of network infrastructure managed and maintained by Network Services, various standards and templates are maintained. Standards and templates maintained by Network Operations and Enterprise Network Support address routers at the core, distribution, and access levels. LAN Services maintain the CMS/BCCS LAN Services Standards for Hardware Configuration and Deployment to assist in configuring network devices maintained for agencies.

SolarWinds Network Configuration Manager (NCM) is utilized for configuration backups, making configuration changes to multiple devices at a time, and policy reporting purposes. Additionally, NCM is capable of sending alerts to administrators as deemed appropriate.

Network Services has implemented procedures to routinely backup configurations for firewalls, routers and switches they manage and maintain. Network Operations and Enterprise Network Support firewall, router, and switch configurations are backed-up.

To ensure continuous availability of the network, the Department has configured the network in a redundant manner. Where operationally feasible, the Department has configured redundancy between pop-sites; thus, ensuring redundancy and availability throughout the backbone (core level) of the network. However, redundancy between individual agency sites is ultimately the responsibility of each individual agency to determine their needs and ensure the Department is aware of those needs. Network Services offers services to agencies which configure redundancy into the network for the requesting agency at the distribution and access layers of the network.

Equipment availability is maintained by either a SMARTnet Next Business Day (NBD) coverage. The Department maintains SMARTnet agreements which provided maintenance and support services for Cisco brand hardware and software, as well as product replacement, for devices maintained by Network Services. SMARTnet does not cover equipment which has reached End-of-Support.

Network Services maintains an Enterprise Virtual Private Network (VPN) solution utilized by the Department and other state agencies to connect remotely into resources managed and maintained by the Department. A pair of firewalls and four routers, managed and maintained by Network Services, are utilized by the VPN solution.

To assist in managing and maintaining the Enterprise VPN solution, Network Services has developed the CMS Enterprise VPN Standard and Individual Remote Access Standard.

The CMS Enterprise VPN Standard defines the four types of VPNs available (individual remote access, LAN-to-LAN, DMVPN, and Private Net VPN), as well as the type of encryption supported for the VPNs.

The Individual Remote Access Standard defines the process to request VPN access, the network infrastructure used by the VPN, the process to connect to the VPN, and the user's requirements to ensure devices connecting to resources via the VPN are current on security and antivirus patches.

Network Services offers a solution which encrypts an agency's data while it is in transit across the public network. The encryption is not considered a true end-to-end encryption solution as it does not encrypt data PC-to-PC or throughout the local networks, but it does encrypt data as it traverses from one agency site to another over the network. Traffic is encrypted at the agency's access router level and decrypted at the agency head-end router level.

The Department's Data Classification and Protection Policy documents the data classification schemas used to value and classify information generated, accessed, transmitted or stored. The Business Reference Model collects and stores information related to application and data processing services provided based on the Data Classification and Protection Policy. The user agencies are responsible for the population of the Business Reference Model and its periodic updates.

In addition, the Data Classification and Protection Policy and the General Security For Statewide IT Resources Policy document requirements for the sharing of information with third parties.

End User Computing (EUC) is responsible for purchasing, installing, configuring, removing, and maintaining enterprise computing equipment (laptops and desktops) for managed agencies.

Agencies are responsible for submitting an ESR to for the installation/removal of equipment. Once the ESR is received by EUC, the equipment is imaged then shipped or picked up by the agency.

Managed enterprise computing equipment is running Windows XP and Windows 7. Additionally, encryption software has been installed on laptops which have been deployed after December 1, 2007. The Department utilizes Microsoft and PointSec for full disk encryption.

Individuals with administrative right may make changes to the encryption software. In addition, depending on the domain policy in which the equipment or user are assigned to, they may have the ability to install software.

The Department receives Microsoft Windows patches monthly. The patches are first tested with the technical staff, then a pilot group, and then pushed out to the general population. The patch process follows the Department's change management process.

The AntiVirus Group is responsible for pushing daily definitions and other antivirus software updates out. The definitions are delayed six hours before being pushed to users. This allows the staff to review and ensure no issues are encountered. The pushes follow the Department's change management process. The AntiVirus Group has tools available to monitor the enterprise computing equipment that are out compliance regarding antivirus definitions.

In order to access the Department's environment, the user must be assigned a user ID and password. To obtain an ID, the agency must submit an authorized ESR indicating the required access.

The Department utilizes the CCF and the Communication Building to house the State of Illinois Mainframe Information Technology Infrastructure. The facilities are monitored 24 hours a day, 7 days a week, by security guards, surveillance cameras, proximity badge readers, and security alarms.

The Department has contracted with a security company to provide security guards at the facilities. The contract requires security guards at each facility 24 hours a day, seven days a week.

Video surveillance cameras are located on the exterior and interior of the facilities. The security guards and the Physical Security Coordinator monitor the video feeds.

The Department utilizes the Hirsch Velocity system (card key) to control access to and within the facilities. In addition, the Department has created preventive measures at the CCF in order to prevent unauthorized access.

Additionally, security alarms have been placed throughout the facilities. If an alarm is triggered an alert notified the Hirsch Velocity System.

In order to obtain access to the facilities, an individual must obtain a card key badge. The individual is required to complete the ID Badge Request Form; have it approved by an authorized approver, submit it to the Physical Security Coordinator, and present a valid ID. Access rights are based on the individual's job duties. In addition, prior to receiving access, the individual is required to submit to a background check.

Upon termination of employment, the Physical Security Coordinator is notified by the individual's supervisor and Personnel. Once the Physical Security Coordinator is notified, the individual's access rights are deactivated.

Visitors, along with contractors and employees who forget their badge, are required to sign-in and register with security guards to gain access to the facilities. The security guard on duty receives the individual's driver's license for authorization with the Hirsch Velocity System. Once reviewed, the security guard provides a badge based on the individual's access rights. Visitors are provided a visitor badge, which will not allow access, and must be escorted by an authorized individual.

The Department has installed preventive environmental measures at the facilities:

- Fire extinguishers are located throughout both facilities,
- A fire suppression and detection system are located in specific areas of the facilities,
- Water detection system is located within raised floor areas of the CCF,
- Sprinkler systems are installed within specific areas,
- Cooling/heating systems are installed within the both facilities,
- The uninterrupted power supply (UPS) at the facilities include a battery farm and diesel turbine generators.

Department staff monitor the environmental factors and notify the applicable vendor for any issues.

The Department has entered into contracts/agreements with vendors for the maintenance/repairs of preventive environmental equipment. The Physical Security Coordinator monitors the contracts/agreements.

In addition, the Department utilizes two off-site storage facilities: Regional Vault and Alternate Data Center. Each facility has security controls present; card key scanners, identification requirements, and escorted access.

As of July 1, 2014, the Department will no longer utilize the Regional Vault for off-site storage. The Department will use the Alternate Data Center for off-site storage of backups.

The Department also maintains a print shop at the Department of Revenue's facility.

The Department of Revenue physical security controls include security guards, card key system, and security cameras. In order to access the print shop, an individual's ID Badge must have applicable access or the individual must sign in as a visitor and be escorted.

The Department's employees and contractors are provided with ID badges that allows them access to specific sections of the buildings. Access is assigned based on job duties.

Each agency is responsible for the scheduling of their respective print jobs. Approximately 86 agencies utilize the printing services.

Upon notification from the agency, their applicable print jobs are delivered by the print shop staff to the authorized agency personnel at the guard's desk or the loading dock. At that time, the agency personnel must provide appropriate identification. The print shop staff then verifies their

authorization via the Focal system. Upon verification, the agency personnel sign the Report Distribution Checklist.

In order to be authorized, agencies are required to submit a CMS Media Transmittal/Services Authorization Request to the security administration division. The individual is then entered into the Focal system as authorized.

In addition to print jobs, agencies have the option to view reports via Mobius. In order to obtain access to view on-line reports, the individual must have a Security Software ID with appropriate access. Each agency's Security Software Coordinator is responsible for authorizing their staff's Security Software access rights.

Change Control

The Department has developed the Remedy Change Management Guide and the Change Management Policy in which all changes to the network services infrastructure, data storage devices, and mainframe infrastructure are to follow. In addition, the Department has established the Change Advisory Committee to oversee the change process.

Each change is required to be entered into Remedy, via a Request For Change (RFC), categorized, prioritized, and approved. Additionally, specific fields within the RFC are to be completed as required by the Remedy Change Management Guide.

The level of approval is dependent upon the impact of the change. Transparent changes are low impact changes which have little to no impact and are required to be approved by Group Managers. Medium and high impact changes are changes which may have an impact on the environment or effect more than one agency. Medium and high impact changes are required to be approved by Group Mangers, Enterprise Change Management Team, and the Change Advisory Committee (CAC).

All high impact changes are required to have a testing, back out and implementation plan attached to the RFC. The detail of testing and the documentation requirements for testing, backout, and implementation plans have been established by each division.

All approvals, plans and information associated with the change are to be attached or included within the specific RFC for record purposes.

In the event of an emergency change, the Enterprise Change Management Team and the applicable manager is to be notified, in order to obtain verbal approval. Upon implementation, the change is to follow the standard process, which requires approval from the Group Managers, Enterprise Change Management Team and the CAC.

A post implementation review is required for change which causes an outage or is an emergency change. The review is conducted by the change supervisor or an Enterprise Change Management Team member.

Changes, including emergency changes are communicated each week at the CAC meetings, with the meeting minutes posted to the SharePoint site. All agencies have access to the SharePoint site in order to track the status of RFCs.

Application changes are to follow the Application Lifecycle Management Manual, which requires a request to be entered into Remedy and follow the Department's change management process. In addition, each request is to have a completed mainframe checklist.

The Operations Center staff is responsible for moving mainframe system changes into production. Each shift will review Remedy; determine if any changes are to be completed. If there are, the Remedy Ticket and the IPL screen are printed to ensure accuracy of the information. Once the change has been completed, the staff will update the Remedy Ticket indicating the move had occurred.

The Library Services Group is responsible for moving mainframe application changes into production for DHS, DCMS, DHFS, DOT and DPH. The Department and the agencies have developed the Library Standards to control the moves to production.

For moves completed by Library Services staff for DHS, DHFS and DPH, the agencies submit an email from an authorized staff to Library Services indicating the date, time and libraries to be moved. Upon completion of the move, Library Services staff notify the applicable agency.

For moves related to DCMS, once the application change has been tested and approved, the developer is to submit a move sheet to a secure mailbox. The move sheet is then forwarded to a Library Services mailbox by authorized staff. The Library Services Group moves the application change into production and notifies the sender that the change has been successfully completed.

Planned application changes are conducted during the regular scheduled maintenance window. Changes are communicated to users via email or phone.

Access to the application's production libraries is controlled by each agencies security software coordinator. The agencies' security software coordinator is responsible for maintenance of access rights to the agencies production libraries and data.

In order to complete the moves for agencies, specific Library Services staff have access, based on security software groups, to the agencies' production libraries.

In addition, agencies utilize Pan Apt to schedule a move. If the move is scheduled via Pan Apt, an authorization email is not required. Security software controls who has access to schedule.

In order to achieve the acquisition and management of systems and technology, the Department developed and implemented the IT Governance Policy, IT Guiding Principles, and the IT Governance Gates, which are published on the Department's website.

The IT Governance process applies to business-sponsored IT projects that satisfy at least one of the following criteria:

a. new business functionality is being added
b. a move to a new or updated platform is being made
c. an old system is being replaced (lifecycle)
d. a system is being in-sourced or outsourced either partially or completely
e. the work has enterprise implications.

Upon determining if the system or technology satisfies one of the above criteria, the agency is required to submit a Project Charter, Business Requirements, and Technical Requirements. The documents solicit information related to the design, acquisition, implementation, configuration, system availability/recovery requirements, and security requirements.

The IT Governance staff assess and approve the project documentation. IT Governance documentation and approvals are maintained in the EPM Portal.

Backup and Restoration

The Department utilizes Virtual Tape Disk library for the mainframe between the CCF and the Alternate Data Center (ADC). This solution provides replication between two DLM's at the CCF and one residing at the ADC. The solution supports the system software and program operating environment, Tivoli Storage Manager (TSM), Hierarchical Storage Management (HSM), Daily & Weekly Backup Job processing and Scratch Pool processing.

The Department utilizes CA-Scheduler to control and schedule backups. All systems are scheduled within CA-Scheduler to be backed up on a routine daily and weekly basis. Once scheduled, the backups run automatically utilizing a utility within CA-Scheduler to perform the backups.

To document backup jobs scheduled in CA-Scheduler and assist with the verification that backups are successful; the Department maintains and reviews the CA-Scheduler Verify Backups document.

In the event of a failed backup, the staff is notified and the incident is recorded in the Shift Report. Upon notification, the staff will research and rectify the problem, then manually run cleanup jobs until all issues are resolved. Additionally, staff notify the user agency, explained the problem, and requested the agency to rectify the problem, if applicable.

Additionally, replication is to occur every ten minutes between the CCF and ADC Data Lifecycle Management (DLM). The monitoring software sends an alert if the data is out of sync for more than two hours. In the event of an issue, a Remedy ticket will be opened and tracked until the issue is resolved.

The logs are maintained which document the library being replicated, the status of the replication, and the time of the last sync.

Only authorized staff have access to storage and backup data.

Although agencies are responsible for the scheduling of backups, via CA-Scheduler, Library Services monitors the backup process to ensure the process completed; however, they are not responsible for the accuracy of the backups. In the event of a failure of a backup, Library Services is notified, via email, who then notifies the applicable agency. Library Services maintains a listing of the backup which are scheduled to be ran, daily, weekly and monthly on their SharePoint site. The next day after the backup is scheduled, a report is run to determine the success/failure of the jobs.

If an abend occurs, the Operations staff will be notified and take the appropriate action. Additionally, Operations staff will note such in the Shift Checklist. If the file is corrupt, Operations are notified and will contact the applicable on call staff. Failed backups are rescheduled to run the next day.

Library Services is responsible for the tracking and movement of physical backup tapes. The Department has developed the Library Guide to provide guidance related to the tracking and movement of tapes.

The Department utilizes the Tape Management System (TMS) to track the location of the backups. In addition, each year the Department conducts an inventory of all physical tape media located at the CCF and the off-site vault. Any noted discrepancies are immediately resolved.

Agencies are to submit an email from an authorized individual indicating the tapes that need to be pulled and sent to the off-site vault or to be picked up by the agency. Once Library Services receives an authorized email, Library Services staff will pull the applicable tapes and box for the off-site vault currier to pick up. If an agency staff is to pick up the tapes, the individual must present the driver's license, be on the Tape Media Authorization Listing, and sign the security log.

The agencies are responsible for informing the Department's Security Administrator who is authorized to pick up tape media. The Department's Security Administrator is responsible for maintaining the Tape Media Authorization Listing.

The Department is responsible for the recovery of the State of Illinois network service and mainframe infrastructure, operating systems and the data storage infrastructure. The individual agencies are responsible for the recovery of their applications and data.

The Department has contracted with a third party vendor for an ADC. The Department has installed equipment at the ADC in order to categorize it as a "warm site".

In addition, the Department has entered into an Interagency Agreement with the Department of Agriculture to utilize the Emerson Building on the State Fair Grounds as a cold site. The Emerson Building is available to agencies upon request.

The Department had developed three recovery plans to assist in the recovery of the environment:

- The DCMS/BCCS Infrastructure Services Recovery Activation Plan,
- The IT Recovery Policy, and

- The Recovery Methodology.

The agencies are responsible for determining the recovery time objective and recording their categorization of applications/data within the Business Reference Model (BRM).

The Department conducts a comprehensive test of the Category One, Stage Zero applications/data on an annual basis. In addition, the Department tests the DCMS/BCCS Infrastructure Services Recovery Activation Plan during the annual test. The agencies are to submit to the Department, the goals and outcomes of their testing for review and updating of Plans and recovery documentation.

In the event the agencies require additional testing, they may arrange testing time with the Department.

Applications

The Department provides and maintains applications which agency may utilize for accounting, inventory and payroll functions. All data entered into and the balancing of is the responsibility of the agencies.

The Accounting Information System (AIS) is an online, menu-driven, mainframe application that provides an automated expenditure control and invoice/voucher processing system. AIS was officially implemented in March 1995.

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, which processes approximately 1.85 million transactions per month, is online from 7 a.m. to 7 p.m. Monday through Thursday, 7 a.m. to 5 p.m. on Friday, and 7 a.m. to 7 p.m. on Saturday. The system is not available on Sundays.

The Central Inventory System (CIS), developed in 1985 and updated in 1998, 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, 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, which processes approximately 50,000 transactions per month, is online from 7 a.m. to 7 p.m. Monday through Thursday, 7 a.m. to 5 p.m. on Friday, and 7 a.m. to 4 p.m. on Saturday. The system is not available on Sundays or holidays.

The Central Payroll System (CPS) enables State agencies to maintain automated pay records and provides a file which is submitted to the Comptroller's Office for the production of payroll

warrants. CPS transactions are entered online in a real-time environment, with the ability to batch transactions for processing at a later date.

CPS processes approximately 160,000 transactions per month. CPS users have access to the system each weekday during the pay cycle, except for down days, from 7 a.m. until 8 p.m., and from 8 a.m. to 4 p.m. on Saturdays. A down day is a day where no entry to CPS will be allowed, and each pay schedule (except supplemental) will have at least one down day per pay cycle. In addition, CPS is down every Sunday for weekly maintenance.

The Central Time and Attendance System (CTAS), developed in 1992, is an online system that provides a comprehensive system for recording and managing employee benefit time. 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.

CTAS, which processes approximately 450,000 transactions each month, is online from 6 a.m. to 8:30 p.m. seven days per week including holidays.

eTime is a web-based, real-time application which allows management and employee to manage and account for their time and attendance. eTime interfaces with CTAS in order to transfer attendance records.

eTime is online from 6 a.m. to 8:30 p.m. seven days per week including holidays.

Access to AIS, CIS, CTAS and CPS is controlled through system software security, in addition to the application's 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. The Security Module defines the parameters and staff authorization; access, approve transactions, modify and delete transactions.

Access to eTime is controlled through the users Active Directory account. The employee's access is based on their duties; access, approve, modify or delete transactions. Employee's access is limited to their specific information, whereas, supervisors and managers have access to the employee's accounts in which they are responsible.

The assignment, authorization, and maintenance of access rights are the responsibility of each agency's security administrator. In the event Department staff require access, an authorized ESR is to be completed, indicating the applicable access required.

The Department has developed user manuals and reference guide for each application, which provides guidance to the user when utilizing the various functions of the applications. Data entered into the application is the responsibility of the user agency.

To ensure the accuracy of the data, the applications have numerous edit checks and range checks to alert the user of errors. Error handling procedures are followed during data origination to ensure that errors and irregularities are detected, reported, and corrected. Each transaction is assigned an identifying number.

The applications provide various on-line and batch reports to assist in the balance of transactions. A complete listing of the various reports is maintained in the user manual.

The Department has developed the disaster recovery plans or procedures for the restoration of the applications. The applications are backed up daily, weekly, and monthly. A history of data is maintained.

BOUNDARIES OF THE SYSTEM

The Department of Central Management Services provides all state government agencies, boards, and commissions a mainframe Information Technology infrastructure in which to host their applications. The system description herein only relates to the mainframe computing environment and excludes the midrange server computing environment. The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures and data necessary to provide such services. The boundaries of the Department's system include the mainframe environment, networking components (firewalls, routers, switches), data storage devices, and end user computing. The Department maintains and provides applications which are utilized by multiple agencies: Accounting Information System, Central Inventory System, Central Time and Attendance System, Central Payroll System, and eTime. However, the input and integrity of the data is the responsibility of the user and, therefore, is not within the boundaries of the system.

In addition, the Department has contracted with a vendor for the utilization of an alternate data center for off-site storage of backups and disaster recovery services. The controls over the alternate data center are the responsibility of the vendor and reported upon within the vendors Service Organization Controls Report. Therefore, the controls are not within the boundaries of the system.

TRUST SERVICES CRITERIA AND RELATED CONTROLS

Although the trust services criteria and related controls are presented in Trust Services Criteria Common to All, Availability Principle, and Processing Integrity Principal Criterias, along with the Related Controls, and Test of Controls, they are an integral part of the State of Illinois Mainframe Information Technology Environment System's description.

COMPLEMENTARY USER-AGENCY CONTROLS

The Department of Central Management Services' services were designed with the assumption that certain controls would be implemented by the user agency. The user agency controls subsequently presented should not be regarded as a comprehensive list of all controls that should be employed by the user agency.

User agencies of the Department of Central Management Services, Bureau of Communications and Computer Services, State of Illinois Mainframe Information Technology Environment should maintain controls to provide reasonable assurance that:

- User agencies have reviewed and adhere to the security polices located on the Department's website;
- User agencies have communicated to the Department their specific security requirements;
- User agencies have informed the Department's Help Desk in a timely manner of any security, availability, or processing issues;
- User agencies have classified their applicable applications and data based on criticality and sensitivity;
- User agencies have reviewed, updated, approved, and returned to the Department on a bi-annual basis their applicable user listings;
- User agencies are effectively utilizing security software features and perform periodic reviews of existing profiles to ensure that access rights are appropriate;
- User agencies have reviewed the effectiveness of critical manual controls over the applications, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions;
- User agencies enter only accurate and authorized data into the applications;
- User agencies regularly review the users and user groups with access to the applications to ensure access authorized is appropriate;
- User agencies regularly review those authorized to pick up payroll reports, and inform appropriate Department staff of changes timely;
- User agencies retain hardcopy payroll vouchers for at least the three most current pay periods, as specified by the CPS User Manual; and
- User agencies develop and maintain appropriate and viable business continuity plans, application recovery scripts, designated application information updates to the Business Reference Model, recovery exercise procedures and schedules, and ongoing communications with the Department.

This page intentionally left blank

Description of Test of Controls and Results Thereof

This page intentionally left blank

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria Common to All (Security, Availability, and Processing Integrity)

	Criteria	Department's Control	Testing Performed	Results
CC1.0	**Common Criteria Related to Organization and Management**			
CC1.1	The Department has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they relate to security, availability, and processing integrity.	Each position is to have a position description which outlines the duties and qualifications.	Reviewed a sample of positions to determine if position descriptions had been completed.	No deviation noted.
			Reviewed the position descriptions to determine if they outlined the duties and qualifications.	No deviation noted.
		The Organization Chart is reviewed weekly at the management meetings, with weekly reports to the Governor's Office on critical vacancies.	Reviewed a sample of weekly management meeting agendas and weekly reports to the Governor's Office to determine if critical vacancies were reviewed and reported.	No deviation noted.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the Department's system controls are assigned to individuals within the Department with authority to ensure policies and other system requirements are effectively promulgated and placed in operation.	Each position is to have a position description which outlines the duties and qualifications.	Reviewed a sample of positions to determine if position descriptions had been completed.	No deviation noted.
			Reviewed the position descriptions to determine if they outlined the duties and qualifications.	No deviation noted.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria Common to All (Security, Availability, and Processing Integrity)

	Criteria	Department's Control	Testing Performed	Results
CC1.3	Personnel responsible for designing, developing, implementing, operating, maintaining and monitoring the system affecting security, availability, and processing integrity have the qualifications and resources to fulfill their responsibilities.	The Department adheres to the State's hiring procedures; Personnel Code, Union Contracts and Rutan decisions, for the hiring of staff.	Reviewed the hiring procedures; Personnel Code, Union Contract, and Rutan decisions.	No deviation noted.
			Reviewed a sample of new hires to determine if they were filled in accordance with the hiring procedures.	No deviation noted.
		Once a job description is in place the Personnel initiates a Personnel Action Request (PAR) and then an Electronic Personnel Action Request (ePAR) in order to request to fill a vacancy. Once the ePar is approved by the Administrative and Regulatory Shared Services, Department's CFO, Department's Director and the Governor's Office of Management and Budget, the hiring process begins.	Reviewed a sample of new hires and ensured the PAR and ePAR were properly completed and approved.	No deviation noted.
		Upon employment, the Administrative and Regulatory Shared Services provides new employees orientation. New employees complete various forms and training at the orientation.	Reviewed the training provided to new employees.	No deviation noted.
			Reviewed a sample of new employees to determine if they had been provided training.	No deviation noted.
		The Department's training office works with managers to identify training needs, registers employees for training, and tracks all training in a database.	Reviewed the training report to determine if employees had received training.	No deviation noted.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria Common to All (Security, Availability, and Processing Integrity)

	Criteria	Department's Control	Testing Performed	Results
CC1.4	The Department has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security, availability, and processing integrity.	The security obligations of Department staff are communicated via the mandatory annual security awareness training.	Reviewed the Security Awareness Training Report to determine if employees and contractors completed training.	No deviation noted.
		New Department staff confirm their compliance with the security policies through security training.	Reviewed security awareness training to determine if confirmation of compliance with policies is required.	No deviation noted.
			Reviewed the security awareness training report to determine if new employees had confirmed compliance with policies.	No deviation noted.
		Department staff reconfirm their compliance with the security policies through the annual security training.	Reviewed security awareness training to determine if confirmation of compliance with policies was required.	No deviation noted.
			Reviewed the security awareness training report to determine if employees had confirmed compliance with policies.	No deviation noted.
		Contractors confirm their compliance with the security policies through security training.	Reviewed security awareness training to determine if confirmation of compliance with policies was required.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
			Reviewed the security awareness training report to determine if contractors had confirmed compliance with policies.	No deviation noted.
		The Department's Compliance Officer is assigned responsibility for monitoring and ensuring compliance.	Reviewed the Compliance Manager's job description to determine if the responsibilities of monitoring and compliance were outlined.	No deviation noted.
			Reviewed the Compliance Manager's monitoring of compliance.	Monitoring for compliance had not been conducted.
		New employees and contractors are required to have background checks.	Reviewed a sample of new employees and contractors to determine if a background check had been completed.	No deviation noted.
CC2.0	**Common Criteria Related to Communications**			
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.	The Department has published on their website the Service Catalog for which agencies may utilize in determining their required services.	Reviewed the Service Catalog to determine the services and/or products offered.	No deviation noted.
CC2.2	The Department's security, availability, and processing integrity commitments are communicated to external users, as appropriate, and those commitments	New Department staff confirm their compliance with the security policies through security training.	Reviewed security awareness training to determine if confirmation of compliance with policies was required.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
	and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.		Reviewed the security awareness training report to determine if new employees had confirmed compliance with policies.	No deviation noted.
		Department staff reconfirm their compliance with the security policies through the annual security training.	Reviewed security awareness training to determine if confirmation of compliance with policies was required.	No deviation noted.
			Reviewed the security awareness training report to determine if employees had confirmed compliance with policies.	No deviation noted.
		Contractors confirm their compliance with the security policies through security training.	Reviewed security awareness training to determine if confirmation of compliance with policies was required.	No deviation noted.
			Reviewed the security awareness training report to determine if contractors had confirmed compliance with policies.	No deviation noted.
		The Department has published on their website the Service Catalog for which agencies may utilize in determining their required services.	Reviewed the Service Catalog to determine the services and/or products offered.	No deviation noted.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria Common to All (Security, Availability, and Processing Integrity)

	Criteria	Department's Control	Testing Performed	Results
		The Department has implemented several policies to address an array of security issues; physical and logical.	Reviewed security policies to determine if they addressed physical and logical security issues.	The policies did not address: - the requirements for requesting, obtaining, and modifying access (documentation, tracking and approvals), -the periodic review of access rights, -the revocation of access rights, -the actions supervisors were to take when notified of a security issue.
CC2.3	The Department communicates the responsibilities of internal and external users and others whose roles affect system operation.	New Department staff confirm their compliance with the security policies through security training.	Reviewed security awareness training to determine if confirmation of compliance with policies was required.	No deviation noted.
			Reviewed the security awareness training report to determine if new employees had confirmed compliance with policies.	No deviation noted.
		Department staff reconfirm their compliance with the security policies through the annual security training.	Reviewed security awareness training to determine if confirmation of compliance with policies was required.	No deviation noted.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria Common to All (Security, Availability, and Processing Integrity)

	Criteria	Department's Control	Testing Performed	Results
			Reviewed the security awareness training report to determine if employees had confirmed compliance with policies.	No deviation noted.
		Contractors confirm their compliance with the security policies through security training.	Reviewed security awareness training to determine if confirmation of compliance with policies was required.	No deviation noted.
			Reviewed the security awareness training report to determine if contractors had confirmed compliance with policies.	No deviation noted.
		The Department has implemented several policies to address an array of security issues; physical and logical.	Reviewed security policies to determine if they addressed physical and logical security issues.	The policies did not address: - the requirements for requesting, obtaining, and modifying access (documentation, tracking and approvals), -the periodic review of access rights, -the revocation of access rights, -the actions supervisors were to take when notified of a security issue.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria Common to All (Security, Availability, and Processing Integrity)

	Criteria	Department's Control	Testing Performed	Results
CC2.4	Internal and external personnel with responsibility for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, availability, and processing integrity of the system, have the information necessary to carry out those responsibilities.	The Department has implemented several policies to address an array of security issues; physical and logical.	Reviewed security policies to determine if they addressed physical and logical security issues.	The policies did not address: - the requirements for requesting, obtaining, and modifying access (documentation, tracking and approvals), -the periodic review of access rights, -the revocation of access rights, -the actions supervisors were to take when notified of a security issue.
CC2.5	Internal and external system users have been provided with information on how to report security, availability, and processing integrity failures, incidents, concerns, and other complaints to appropriate personnel.	Policies and procedures, which are published on the website, document the reporting process of system problems, security issues, and user assistance.	Reviewed the website to determine if the policies were posted.	No deviation noted.
			Reviewed security policies to determine if they documented the reporting process of system problems, security issues and user assistance.	The security policies did not address the actions supervisors were to take when notified of a security issue.

	Criteria	Department's Control	Testing Performed	Results
		The Department has developed procedures for the identification and escalation of security breaches to Department management.	Reviewed the Security Incident Process, Critical Incident Response Procedure, and the Major Outage Response Team Process to determine the process for identification and escalation of security breaches.	The Security Incident Process was in draft form and had not been implemented.
			Reviewed a sample of security issues to determine compliance with procedures.	1 of 6 security incidents was not in compliance with procedures.
		The user manuals for applications provide instructions for users to contact the Help Desk to report issues.	Reviewed the user manuals to determine if they provide instruction to report issues to the Help Desk.	No deviation noted.
		The Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provided guidance to users for the reporting of lost or stolen assets.	Reviewed the Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy to determine if they provided guidance to users for the reporting of lost or stolen assets.	No deviation noted.
			Reviewed a sample of lost or stolen assets to determine compliance with the policies.	No deviation noted.
CC2.6	System changes that affect internal and external system user responsibilities or the Department's commitments and	Infrastructure changes are communicated to users and management via the CAC meetings;	Reviewed a listing of agencies with access to the SharePoint site.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
	requirements relevant to security, availability, and processing integrity are communicated to those users in a timely manner.	which the meeting minutes are posted on the ECM SharePoint site. Agencies have access to the ECM SharePoint site.	Reviewed a sample of CAC Meeting minutes to ensure they were posted on the SharePoint site.	No deviation noted.
			Reviewed a sample of Request For Changes (RFC) to determine if they were included in CAC meeting minutes on the SharePoint Site.	5 of 32 RFCs were not included in CAC meeting minutes.
		Emergency changes are communicated to users post implementation via the CAC meeting.	Reviewed a sample of emergency changes to determine if they were included in the CAC meeting minutes on the SharePoint Site.	No deviation noted.
		Changes to applications are communicated to users via email or phone.	Reviewed a sample of changes to determine if they had been communicated.	4 of 13 changes to the applications did not have documentation of communication with users.
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**			
CC3.1	The Department (1) identifies potential threats that would impair system security, availability, and processing integrity commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies).	The Department is to conduct periodic risk assessments which identify threats and vulnerabilities, and assesses their impact.	Interviewed Acting Chief Information Security Officer.	The Department had not conducted risk assessments to identify threats, vulnerabilities and assessed their impact.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria Common to All (Security, Availability, and Processing Integrity)

	Criteria	Department's Control	Testing Performed	Results
		The Department is to remediate any risk identified.	Interviewed Acting Chief Information Security Officer.	The Department had not conducted risk assessments.
CC3.2	The Department designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.	The Department is to conduct periodic risk assessments which identify threats and vulnerabilities, and assesses their impact.	Interviewed Acting Chief Information Security Officer.	The Department had not conducted risk assessments to identify threats, vulnerabilities and assessed their impact.
		The Department is to remediate any risk identified.	Interviewed Acting Chief Information Security Officer.	The Department had not conducted risk assessments.
		As part of the annual comprehensive test of Category One, Stage Zero applications/data, the DCMS/BCCS Infrastructure Services Recovery Activation Plan is tested.	Reviewed the DCMS/BCCS Infrastructure Services Recovery Activation Plan (Plan) and testing documentation to determine if the Plan had been tested.	No deviation noted.
CC3.3	The Department (1) identifies and assesses changes (for example, environmental, regulatory, and technological changes) that could significantly affect the system of internal control for security, availability, and processing integrity and reassesses risks and mitigation strategies based on the changes and (2) reassesses the suitability of the design and deployment of control activities based on the operation and monitoring of those activities, and updates them as necessary.	The Department is to conduct periodic risk assessments which identify threats and vulnerabilities, and assess the impact	Interviewed Acting Chief Information Security Officer.	The Department had not conducted risk assessments to identify threats, vulnerabilities and assessed their impact.

	Criteria	Department's Control	Testing Performed	Results
		The Department is to remediate any risk identified.	Interviewed Acting Chief Information Security Officer.	The Department had not conducted risk assessments.
		Department management considers technological developments, and laws and regulations during the planning process.	Reviewed the planning process to determine if the Department considered technological developments, and laws and regulations.	No deviation noted.
CC4.0	**Common Criteria Related to Monitoring of Controls**			
CC4.1	The design and operating effectiveness of controls are periodically evaluated against security, availability, and processing integrity commitments and requirements, corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	The Operations Center utilizes software and the Automated Operations Console in order to continuously monitor the environment.	Observed the software utilized and the Automated Operations Console to determine if the environment was monitored.	No deviation noted.
		Problems, issues, and incidents are recorded via the Daily Shift Report and a Remedy Ticket is created.	Reviewed a sample of Daily Shift Reports to determine if problems, issues, and incidents were reported.	No deviation noted.
		For any incident in which the Operations Center cannot resolve, the Remedy Ticket is assigned to the applicable division for resolution	Reviewed a sample of Daily Shift Reports to determine if a Remedy Ticket had been created and assigned for resolution.	No deviation noted.
		The Daily Shift Report records the activity conducted on all production systems and incident calls received at the Operations Center.	Reviewed a sample of Daily Shift Reports to determine if the activity on production systems was recorded and if incident calls were recorded.	No deviation noted.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria Common to All (Security, Availability, and Processing Integrity)

	Criteria	Department's Control	Testing Performed	Results
		The Operator Shift Change Checklist is completed at the beginning of each shift to ensure the production systems are operation appropriately, any open items are passed on, and to identify any changes which need to occur. The Checklists are reviewed by the Operations Center Supervisor.	Reviewed a sample of the Operator Shift Change Checklists to determine if they were completed and reviewed.	No deviation noted.
		In the event management needs to be contacted immediately, contact information is maintained with the FOCAL database.	Reviewed the FOCAL database to determine if management contact information was maintained.	No deviation noted.
		The DP Guide provides Command Center staff with guidance.	Reviewed the Data Processing Guide.	No deviation noted.
		System performance is monitored via software tools.	Reviewed software tool reports to determine if system performance was monitored.	No deviation noted.
		In the event a breach was identified, the Department will utilize the Data Breach Notification Policy and the Action Plan for Notification of a Security Breach. In addition, a Remedy ticket will be opened and if necessary the Technical Safeguards team will be alerted.	Reviewed the Data Breach Notification Policy and the Action Plan for Notification of a Security Breach to determine the process of notification in the event of a security breach.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
			Reviewed a sample of breaches to determine if a Remedy ticket was created, the Technical Safeguards team was alerted, and the affected users were notified in accordance with the Policy and Action Plan.	No deviation noted.
CC5.0	***Common Criteria Related to Logical and Physical Access Controls***			
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.	Logical security controls are in place to restrict access to operating system configurations.	Reviewed system options, security reports, security software, exits, and access rights to sensitive system functions to determine if logical security controls were in place to restrict access to operating system configurations.	Three active IDs with access to operating system configurations were not specifically assigned.
		Operating systems have been configured to promote security.	Reviewed system options, security reports, security software, exits, and libraries to determine if operating systems were configured and controlled to promote security.	No deviation noted.
		Logical access to mainframe information is protected through system security software.	Reviewed system options and security software reports to determine if information was protected by security software.	No deviation noted.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria Common to All (Security, Availability, and Processing Integrity)

	Criteria	Department's Control	Testing Performed	Results
		The mainframe security software requires users to have an established ID and password in order to verify the individual's identity.	Observed a user sign-on process to determine if an ID and password were required to verify identity.	No deviation noted.
			Reviewed system options and password requirements memo to determine password standards.	No deviation noted.
		The primary means of defining a user's access to resources is the system security software resource profile, which defines the level of access a user may have.	Reviewed user profiles to determine if the users' level of access was defined.	No deviation noted.
		The Department has restricted mainframe access with powerful privileges, high-level access, and access to sensitive system functions to authorized personnel.	Reviewed security software report to determine if powerful privileges, high-level access, and access to sensitive system functions were limited to authorized personnel.	No deviation noted.
		In order to access an application, a user must have a separate application ID and password in order to gain access.	Observed the applications required a separate ID and password to gain access.	No deviation noted.
		Staff has access to specific RACF groups which allows them to reset passwords.	Reviewed a sample of Help Desk staff to determine if their access rights were appropriate.	No deviation noted.
		Access to storage and backup data is limited to authorized staff.	Reviewed a sample of staff with access to storage and backup data to determine appropriateness.	2 of 18 individuals had inappropriate access to storage and backup data.

	Criteria	Department's Control	Testing Performed	Results
		In order to access the Department environment, the user must be assigned a user ID and password.	Observed that an ID and password was required in order to gain access to the Department's environment.	No deviation noted.
		The Department maintained an Enterprise Virtual Private Network solution to connect remotely into resources managed and maintained by the Department.	Reviewed the VPN standards to ensure resources were managed and maintained by the Department.	No deviation noted.
		Firewalls and routers are used and configured to prevent unauthorized access via authentication servers, logging servers, banners prohibiting unauthorized access and warning of prosecution and ACLs to deny and permit specific types of network traffic.	Reviewed a sample of firewalls, routers, and switch configurations to determine if they were configured to utilize authentication servers, logging servers, banner warnings, and ACLs to deny and permit specific traffic.	No deviation noted.
		Network Services required manager review and approval of new access rights.	Reviewed a sample of new staff to determine if a manager reviewed and approved access.	No deviation noted.
		LAN Services utilized the LAN Services Access Authorization Form in order for staff to obtain access rights.	Reviewed a sample of new staff to determine if the LAN Services Access Authorization Form had been completed.	No deviation noted.
CC5.2	New internal and external system users are registered and authorized prior to being issued system credentials, and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.	Upon notification of an employee's termination, Personnel will complete a PAR and an Exit Form.	Reviewed a sample of terminated employees to determine if a PAR and Exit Form had been completed.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		The Exit Form is sent to the employee's supervisor indicting the items to be retrieved and the deactivation of access.	Reviewed a sample of separated employees to determine if their access had been deactivated in a timely manner.	1 of 9 separated employee's access was not deactivated in a timely manner.
		In order to obtain an ID to access the Department's environment, the user's supervisor must submit an authorized ESR indicating the required access.	Reviewed a sample of staff to determine if an authorized ESR was submitted.	4 of 13 staff did not have an authorized ESR. An ESR was not provided for 2 of 13 individuals.
		The Mainframe Application Access Request Form indicates the access required and proper approval.	Reviewed a sample of Mainframe Application Access Request Forms to determine if the required access and proper approval was obtained.	5 of 5 Mainframe Application Access Request Forms were not properly approved.
		Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form for new and modification requests and submit via a Remedy Enterprise Service Request or email.	Reviewed a sample of new and modified requests to determine if a Mainframe Application Access Request Form had been submitted via an Enterprise Service Request or email.	No deviation noted.
		In the event the Mainframe Application Access Request Form is for a non-expiring ID, the CISO must approve.	Reviewed a sample of non-expiring IDs to determine if a Mainframe Application Access Request Form was approved by the CISO.	No deviation noted.
		The mainframe security software requires user to have an established mainframe ID and password in order to verify the individual's identity.	Observed a user sign-on process to determine if an ID and password were required to verify identity.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
			Reviewed system options and password requirements memo to determine password standards.	No deviation noted.
		The primary means of defining a user's access to mainframe resources is the security software resource profile, which defines the level of access a user may have.	Reviewed user profiles to determine if the users' level of access was defined.	No deviation noted.
		Network Services required manager review and approval of new access rights.	Reviewed a sample of new staff to determine if a manager reviewed and approved access.	No deviation noted.
		LAN Services utilized the LAN Services Access Authorization Form in order for staff to obtain access rights.	Reviewed a sample of new staff to determine if a manager reviewed and approved access.	No deviation noted.
CC5.3	Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data).	Mainframe security software password standards have been established.	Reviewed system options and password requirements memo to determine password standards.	No deviation noted.
		The mainframe security software requires users to have an established ID and password in order to verify the individual's identity.	Observed a user sign-on process to determine if an ID and password were required to verify identity and the user profile contained a name field.	No deviation noted.
			Reviewed system options and password requirements memo to determine password standards.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		The primary means of defining a user's access to resources is the security software resource profile, which defines the level of access a user may have.	Reviewed user profiles to determine if the level of access was defined.	No deviation noted.
		In order to access an application, a user must have a separate application ID and password in order to gain access.	Observed that the applications required a separate ID and password in order to gain access.	No deviation noted.
		The Department maintained an Enterprise Virtual Private Network solution to connect remotely into resources managed and maintained by the Department.	Reviewed the VPN standards to ensure resources were managed and maintained by the Department.	No deviation noted.
		Users establish their identity and authentication to systems and applications through the use of user IDs and passwords.	Reviewed the administrative architecture deployed on the authentication services.	No deviation noted.
			Reviewed a sample of user accounts to determine if they were assigned a user ID and password.	No deviation noted.
			Reviewed a sample of users with powerful access rights to determine if the rights were appropriate.	No deviation noted.
		Password parameters have been established on authentication servers.	Reviewed the password configurations.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
			Reviewed a sample of user accounts to determine if the password configurations had been enforced.	The main administrator account password configuration did not meet the established standard.
		Firewalls and routers are used and configured to prevent unauthorized access via authentication servers, logging servers, banners prohibiting unauthorized access and warning of prosecution and ACLs to deny and permit specific types of network traffic.	Reviewed a sample of firewalls, routers, and switch configurations to determine if they were configured to utilize authentication servers, logging servers, banner warnings, and ACLs to deny and permit specific traffic.	No deviation noted.
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them.	Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form for new and modification requests and submit via a Remedy Enterprise Service Request or email.	Reviewed a sample of new and modified requests to determine if a Mainframe Application Access Request Form had been submitted via an Enterprise Service Request or email.	No deviation noted.
		The Mainframe Application Access Request Form indicates the access required and proper approval.	Reviewed a sample of Mainframe Application Access Request Forms to determine if the required access and proper approval was obtained.	5 of 5 Mainframe Application Access Request Forms were not properly approved.
		In the event the Mainframe Application Access Request Form is for a non-expiring ID, the CISO must approve.	Reviewed a sample of non-expiring IDs to determine if a Mainframe Application Access Request Form was approved by the CISO.	No deviation noted.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria Common to All (Security, Availability, and Processing Integrity)

	Criteria	Department's Control	Testing Performed	Results
		Upon notification of termination, via an Exit Form, ESR or email, an individual's security software ID is deactivated.	Reviewed a sample of separated employees to determine if their access had been deactivated in a timely manner.	1 of 9 separated employees did not have their access deactivated in a timely manner.
		Password resets to Department and proxy agency user profiles are completed by submitting an email request to the Help Desk, or by accessing the Department's Identity Management website.	Reviewed a sample of password resets to determine if an email request had been submitted.	31 of 95 password resets did not have an email request submitted.
			Reviewed the Department's Identity Management Website.	No deviation noted.
		Bi-annually, the Department's RACF Coordinator will send all agencies a listing of their users on the security authorization listing, requesting the agency to review for accuracy, note any modifications, and return to the Department.	Reviewed the bi-annual communication to agencies indicting the review of their listing of their users.	No deviation noted.
		An ESR is created in order for Help Desk staff to receive the appropriate access.	Reviewed a sample of new Help Desk staff to determine if an ESR had been completed.	1 of 3 ESRs could not be provided.
		LAN Services utilized the LAN Services Access Authorization Form in order for staff to obtain access rights.	Reviewed a sample of individuals whose employment status had changed to determine if the individual's access rights were adjusted accordingly.	1 of 1 separated staff did not have their access rights removed in a timely manner.

	Criteria	Department's Control	Testing Performed	Results
		Network Services is notified by Personnel of changes in an individual's employment status and makes changes to user's access rights accordingly.	Reviewed a sample of individuals whose employment status had changed to determine if the individual's access rights were adjusted accordingly.	No deviation noted.
		The Department maintained an Enterprise Virtual Private Network solution to connect remotely into resources managed and maintained by the Department.	Reviewed the VPN standards to ensure resources were managed and maintained by the Department.	No deviation noted.
		Users establish their identity and authentication to systems and applications through the use of user IDs and passwords.	Reviewed the administrative architecture deployed on the authentication services.	No deviation noted.
			Reviewed a sample of user accounts to determine if they were assigned a user ID and password.	No deviation noted.
			Reviewed a sample of users with powerful access rights to determine if the rights were appropriate.	No deviation noted.
		Password parameters have been established on authentication servers.	Reviewed the password configurations.	No deviation noted.
			Reviewed a sample of user accounts to determine if the password configurations had been enforced.	The main administrator account password configuration did not meet the established standard.

	Criteria	Department's Control	Testing Performed	Results
		Firewalls and routers are used and configured to prevent unauthorized access via authentication servers, logging servers, banners prohibiting unauthorized access and warning of prosecution and ACLs to deny and permit specific types of network traffic.	Reviewed a sample of firewalls, routers, and switch configurations to determine if they were configured to utilize authentication servers, logging servers, banner warnings, and ACLs to deny and permit specific traffic.	No deviation noted.
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel.	The CCF and Communication Building are monitored 24 hours a day, 7 days a week by security guards.	Reviewed duties outlined in the security guard contract.	No deviation noted.
			Observed the security guards and performance of duties.	No deviation noted.
		Video surveillance cameras are located on the interior and exterior of the CCF and Communication Building.	Observed the location of the video surveillance cameras.	No deviation noted.
		The security guards and the Physical Security Coordinator monitor the video feeds.	Observed video feeds to determine if they were monitored by the security guards and Physical Security Coordinator.	No deviation noted.
		Security alarms have been placed throughout the CCF and Communications Building.	Observed the location of security alarms.	No deviation noted.
		The Department has created preventive measures at the CCF in order to prevent unauthorized access.	Observed the measures at the CCF to prevent unauthorized access.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		A cardkey system is utilized to restrict access to and within the CCF and the Communications Building.	Observed the cardkey system to determine if it was utilized to restrict access to the facilities and within.	No deviation noted.
		In order to obtain a card key, an ID Badge Request Form is to be completed; approval must be obtained from an authorized manager, presentation of a valid ID and a completed background check prior to access being granted.	Reviewed a sample of new employees and contractors ID Badge Request Forms to determine if the Forms were properly approved and if a background check had been completed prior to access being granted.	2 of 10 ID Badge Forms were not provided.
		Access to restricted areas is based on the employee and contractor's duties.	Reviewed a sample of employees and contractors with access to the CCF, Communications Building, and sensitive area to determine appropriateness.	No deviation noted.
		Visitors are required to sign in and out, provide their driver's license, and be escorted.	Reviewed a sample of visitor logs to determine if they were properly completed.	No deviation noted.
			Observed visitors being escorted.	No deviation noted.
		Employees and contractors who have forgotten their cardkey are required to sign-in, and provide their driver's license. The employee or contractor is provided a cardkey with access based on the authorization within the cardkey system.	Reviewed a sample of Admittance Registers to determine if the employee or contractor signed in and were provided the appropriate badge based on the authorization within the cardkey system.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		Visitors are provided visitor badges, which does not permit access to or within the CCF and Communications Building.	Observed the operation of visitor badges to determine that access to and within the CCF and Communications Building was not permitted.	No deviation noted.
		Upon notification of an employee's termination, Personnel will complete a PAR and an Exit Form.	Reviewed a sample of terminated employees to determine if a PAR and Exit Form had been completed.	The Department was unable to provide the Exit Form for 3 of 15 separated individuals.
		The Exit Form is sent to the employee's supervisor to ensure collection of equipment and termination of access.	Reviewed a sample of terminated employees to determine if the Exit Form had been completed and access was terminated.	1 of 9 terminated individual's ID badge was still active.
		Physical access controls are in place to restrict access to Regional Vault offsite storage location.	Reviewed access controls to determine if access was restricted.	No deviation noted.
			Reviewed a sample of individuals with access to the offsite storage location to determine if appropriate.	2 of 7 individual's access were no longer required.
CC5.6	Logical access security measures have been implemented to protect against security, availability, and processing integrity threats from sources outside the boundaries of the system.	Logical access to information is protected through system security software.	Reviewed system options and security software reports to determine if information was protected by security software.	No deviation noted.
		Laptop and desktop operating systems are updated as required by the vendor.	Reviewed the Department's compliance report to determine if the operating	7,919 of 35,332 laptops and desktops were not

	Criteria	Department's Control	Testing Performed	Results
			system had been updated on laptops and desktops.	running the latest version of the operating system or the latest version was unknown. 7,230 of those laptops and desktops were running Windows XP, which as of April 2014 was no longer supported by the vendor.
		Network diagrams are maintained depicting the infrastructure and placement of firewalls, routers, and switches.	Reviewed network diagrams to determine the placement of firewalls, routers, and switches.	No deviation noted.
		The Department maintained an Enterprise Virtual Private Network solution to connect remotely into resources managed and maintained by the Department.	Reviewed the VPN standards to ensure resources were managed and maintained by the Department.	No deviation noted.
CC5.7	The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the Department to meet its commitments and requirements as they relate to security, availability, and processing integrity.	The Data Classification and Protection Policy documents the data classification schema used to value and classify information generated, accessed, transmitted or stored.	Reviewed the Data Classification and Protection Policy to determine the data classification schema utilized to value and classify information generated, access, transmitted or stored.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		The Data Classification and Protection Policy and the General Security For Statewide IT Resources Policy document requirements for the sharing of information with third parties.	Reviewed the Data Classification and Protection Policy and the General Security For Statewide IT Resources Policy to determine the requirements for sharing information with third parties.	The General Security for Statewide IT Resource Policy indicated in the event of misuse, theft or abuse of information, the individual were to report the incident to their supervisor. However, the Policy did not address what the supervisor was to do once an incident was reported.
		The Business Reference Model collects and stores information related to application and data processing services provided based on the Data Classification and Protection Policy.	Reviewed the Business Reference Model to determine if it collected and stored information related to application and data process services provided based on the Data Classification and Protection Policy.	1,402 of 1,738 applications had not been categorized.
		Laptops deployed after December 1, 2007 has encryption installed.	Reviewed compliance report to determine if laptops deployed after December 1, 2007 had encryption installed.	568 of 7,672 laptops did not have encryption installed. Information regarding

	Criteria	Department's Control	Testing Performed	Results
				encryption was not available for an additional 2,471 laptops.
		The Department makes available encryption technologies and access gateways for the transmission of sensitive or confidential information.	Reviewed the VPN standards to determine the type of connectivity available, encryption supported, VPN access requests and requirements.	No deviation noted.
			Reviewed the web portal utilized to login to the VPN to determine if a banner indicated the system was only for use by authorized users, use may be monitored, and user's requirements to ensure devices connection to resources via the VPN were current on security and antivirus patches.	No deviation noted.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software.	The ability to install, modify, and replace mainframe operating systems is limited to authorized staff.	Reviewed access rights to determine if the ability to install, modify, and replace operating systems were limited to authorized staff.	No deviation noted.
		Access to sensitive system functions is restricted to authorized staff.	Reviewed security reports and access rights to determine that access to system resources was restricted to authorized staff.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		The ability to install software on laptops and desktops is restricted via the domain policy.	Reviewed the domain policy to determine the appropriateness of user's ability to install software.	No deviation noted.
		Antivirus is installed on laptops and desktops.	Reviewed compliance report to determine if antivirus software was installed on laptops and desktops.	9,866 of 42,562 laptops and desktops did not have antivirus software installed.
		Antivirus is installed on laptops and desktops at least daily.	Reviewed compliance report to determine if antivirus software was updated at least daily on the laptops and desktops.	596 of 32,696 laptops and desktops had antivirus software that had not been updated in more than 5 days.
		The Department has tools in place to monitors laptops and desktops to ensure their Antivirus is updated.	Reviewed the compliance report to determine if antivirus software was monitored on laptops and desktops.	No deviation noted.
CC6.0	***Common Criteria Related to System Operations***			
CC6.1	Vulnerabilities of system components to security, availability, and processing integrity breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities.	The Operations Center utilizes software and the Automated Operations Console in order to continuously monitor the environment.	Observed the software utilized and the Automated Operations Console to determine if the environment was monitored.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		Problems, issues, and incidents are recorded via the Daily Shift Report and a Remedy Ticket is created.	Reviewed a sample of Daily Shift Reports to determine if problems, issues, and incidents were reported.	No deviation noted.
		For any incident in which the Operations Center cannot resolve, the Remedy Ticket is assigned to the applicable division for resolution.	Reviewed a sample of Daily Shift Reports to determine if a Remedy Ticket had been created and assigned for resolution.	No deviation noted.
		Records exist for monitoring and documenting operating system actions.	Reviewed system files to determine if records exist for monitoring and documenting operating system actions.	No deviation noted.
		System performance is monitored via software tools.	Reviewed software tool reports to determine if system performance was monitored.	No deviation noted.
		In the event a user encounters a security issue, the Department's website instructs them to contact the Help Desk.	Reviewed the website to determine if instructions for contacting the Help Desk were included.	No deviation noted.
		The Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provides guidance to the user for the reporting of lost or stolen assets.	Reviewed the Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy to determine if guidance was provided to users.	No deviation noted.
		Upon notification of a lost or stolen asset, the Help Desk staff is to create a Remedy ticket, attach the police report and assign the ticket to the Asset Management group.	Reviewed a sample of lost/stolen devices to determine if a Remedy Ticket had been created and a police report was attached to the ticket.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		EUC is to be notified in order to determine if the equipment had encryption installed. If encryption was not installed, EUC was to determine if confidential information was retained and notify the S&CS Group if it was.	Reviewed a sample of lost/stolen devices to determine if EUC had conducted an analysis to determine if encryption was installed.	No deviation noted.
		CA-Scheduler is utilized to schedule and control backups.	Reviewed a sample of backup schedules to determine if mainframe systems were backed up.	No deviation noted.
		Backups are conducted routinely.	Reviewed a sample of schedules to determine if backups were conducted.	No deviation noted.
		The Department verifies the daily and weekly backups completed successfully.	Reviewed a sample of the Verify Backup Reports to determine if backups were successful.	No deviation noted.
			Reviewed a sample of EMC logs to determine the success of data replication to the ADC.	No deviation noted.
		The Department is notified of failed backups.	Reviewed a sample of alerts to determine if failed backups were followed up on.	Network Service or LAN Services were not notified of failed backups.
		Failed backups are recorded on the Shift Report.	Reviewed a sample of failed backups to determine if they were reported on the Shift Report.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		Users are required to email or a problem report via the Department's website to the Help Desk requesting a RACF mainframe password reset. The request is included the user's name, ID, and a phone number to be contacted	Reviewed a sample of password resets to determine if an email or problem report had been submitted indicating the user's name, ID and phone number.	No deviation noted.
		Authentication servers are utilized to control access, log access attempts, and alert management.	Reviewed a sample of authentication servers to determine if they were utilized to control access, log access attempts, and alert management.	No deviation noted.
		The Department has tools in place to identify and log network services security breaches.	Reviewed a sample of firewalls, routers, and switches to determine if they were configured to utilize logging servers.	No deviation noted.
			Reviewed tools to determine if monitoring of performance, bandwidth utilization, CPU utilization, and alerts to management were conducted.	Alerts to management regarding backups were not utilized.
			Reviewed a sample of devices to determine if they were connected to tools.	No deviation noted.
		Routine backups of configurations for firewalls, routers and switches are conducted.	Reviewed a sample of networking devices to determine if they were connected to backup solutions.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
			Reviewed job schedules, and configuration files located on the backup servers.	No deviation noted.
CC6.2	Security, availability, and processing integrity incidents, including logical and physical security breaches, failures, concerns, and other complaints, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures.	The Operations Center utilizes software and the Automated Operations Console in order to continuously monitor the environment.	Observed the software utilized and the Automated Operations Console to determine if the environment was monitored.	No deviation noted.
		Problems, issues, and incidents are recorded via the Daily Shift Report and a Remedy Ticket is created.	Reviewed a sample of Daily Shift Reports to determine if problems, issues, and incidents were reported.	No deviation noted.
		For any incident in which the Operations Center cannot resolve, the Remedy Ticket is assigned to the applicable division for resolution.	Reviewed a sample of Daily Shift Reports to determine if a Remedy Ticket had been created and assigned for resolution.	No deviation noted.
		The Daily Shift Report records the activity conducted on all production systems and incident calls received at the Operations Center.	Reviewed a sample of Daily Shift Reports to determine if the activity on production systems was recorded and if incident calls were recorded.	No deviation noted.
		In the event management needs to be contacted immediately, contact information is maintained with the FOCAL database.	Reviewed the FOCAL database to determine if management contact information was maintained.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		The Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provides guidance to the user for the reporting of lost or stolen assets.	Reviewed the Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy to determine if guidance was provided to users.	No deviation noted.
		Upon notification of a lost or stolen asset, the Help Desk staff is to create a Remedy ticket, attach the police report and assign the ticket to the Asset Management group.	Reviewed a sample of lost/stolen devices to determine if a Remedy Ticket had been created and a police report was attached to the ticket.	No deviation noted.
		EUC is to be notified in order to determine if the equipment had encryption installed. If encryption was not installed, EUC was to determine if confidential information was retained and notify the S&CS Group if it was.	Reviewed a sample of lost/stolen devices to determine if EUC had conducted an analysis to determine if encryption was installed.	No deviation noted.
		The Department is notified of failed backups.	Reviewed a sample of failed backups to determine if the Department was notified.	No deviation noted.
		The Department takes remedial action on failed backups.	Reviewed a sample of failed backups to determine the actions taken.	No deviation noted.
		The user manuals for applications provide instructions for users to contact the Help Desk to report issues.	Reviewed the user manuals to determine if they provided instructions to report issues to the Help Desk.	No deviation noted.
CC7.0	**Common Criteria Related to Change Management**			
CC7.1	Security, availability, and processing integrity commitments and requirements, are addressed, during the system development lifecycle including	Changes are categorized and ranked according to priority.	Reviewed a sample of changes to determine if they were properly categorized and ranked according to priority.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
	design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.			
		Transparent changes (low impact changes), which have little to no impact are required to be approved by Group Managers. Medium and high impact changes are required to be approved by Group Mangers, Change Management Team and the Change Advisory Committee (CAC).	Reviewed a sample of changes to determine if they were properly approved.	No deviation noted.
		Project Charters, Business Requirements, and Technical Requirements are required to be submitted to and approved by the Governance staff.	Reviewed a sample of IT Projects to determine if Project Charters, Technical Requirements, and Business Requirements had been submitted and approved.	No deviation noted.
		Governance staff review and assess the project scope statement.	Reviewed a sample of IT projects to determine if Governance staff reviewed and assessed the project scope statement.	No deviation noted.
		Emergency changes require verbal approval prior to implementation. Standard approvals are to be obtained post implementation.	Reviewed a sample of emergency changes to determine if verbal approval was obtained prior to implementation and if standard approvals were obtained post implementation.	No deviation noted.
		Application changes are required to follow the structured change control process outlined in the Application	Reviewed the Application Lifecycle Manual and a sample of application changes to	The Application Lifecycle Manual did not address:

	Criteria	Department's Control	Testing Performed	Results
		Lifecycle Manual, which requires changes to be entered into Remedy and follow the Department's change management process.	determine compliance with the Application Lifecycle Manual.	- -Required approvals, -Testing and Documentation Requirements, -Requirements for follow up after change is moved into production, and -Emergency change requirements. 13 of 13 changes did not have completed Backout, Implementation, and Testing Plans.
		Application changes are required to have the Mainframe Checklist completed.	Reviewed a sample of changes to determine if the Mainframe Checklist had been completed.	6 of 60 change tasks did not have the Mainframe Checklist completed. We were unable to assess the adequacy of the completeness of the Mainframe Checklist, due to the Mainframe Checklist Procedures not stating the required artifacts.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria Common to All (Security, Availability, and Processing Integrity)

	Criteria	Department's Control	Testing Performed	Results
CC7.2	Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the system commitments and requirements as they relate to security, availability, and processing integrity.	A post implementation review (PIR) is conducted on change which causes an outage or an emergency change. The review is conducted by the change supervisor or a Change Management Team member.	Reviewed a sample of emergency changes to determine if a post implement review had been conducted and properly reviewed.	2 of 17 emergency changes did not have a PIR conducted. The Department did not have a mechanism to track changes which cause an outage; therefore, detailed testing could not be conducted.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.	Each change is required to have a completed Request For Change (RFC) within Remedy. Specific fields within the RFC are to be completed as required by the Remedy Change Management Guide.	Reviewed the Guide and Policy to determine the requirements for a completed RFC.	The Guide did not provide sufficient guidance or requirements for post implementation reviews, testing levels, or back-out and implementation plans. The Policy did not provide sufficient guidance or requirements for testing, evaluating and authorizing changes prior to implementation.

	Criteria	Department's Control	Testing Performed	Results
			Reviewed a sample of changes determine if a RFC was properly completed.	55 of 60 RFCs did not have all of the required fields completed.
		Approvals, plans and information associated with the change are to be attached or included within the specific RFC for record purposes.	Reviewed a sample of changes to determine if they were properly approved and if plans and information were attached.	5 of 9 RFCs did not have the backout, implementation, and testing plans attached.
		A post implementation review (PIR) is conducted on change which causes an outage or an emergency change. The review is conducted by the change supervisor or a Change Management Team member.	Reviewed a sample of emergency changes to determine if a post implement review had been conducted and properly reviewed.	2 of 17 emergency changes did not have a PIR conducted. The Department did not have a mechanism to track changes which cause an outage; therefore, detailed testing could not be conducted.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with security, availability, and processing integrity.	High impact changes require backout, test, and implementation plans to be attached to the RFC for the use in the event of a disruption.	Reviewed a sample of high impact changes to determine if backout, testing and implementation plans were attached to the RFC.	5 of 9 RFCs did not have the backout, implementation, and testing plans attached.
		Transparent changes (low impact changes), which have little to no impact are required to be approved by Group Managers. Medium and	Reviewed a sample of changes to determine if they were properly approved.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		high impact changes are required to be approved by Group Mangers, Change Management Team and the Change Advisory Committee (CAC).		
		The detail of testing, and the documentation requirements for testing, backout and implementation plans are to be established by each division.	Reviewed documentation requirements.	Testing and documentation requirements for backout and implementation plans had not been established.
			Reviewed a sample of changes to determine if testing, backout and implementation plans met the requirements.	5 of 9 RFCs did not have testing, backout, and implementation plans attached.
		Emergency changes require verbal approval prior to implementation. Standard approvals are to be obtained post implementation.	Reviewed a sample of emergency changes to determine if verbal approval was obtained prior to implementation and if standard approvals were obtained post implementation.	No deviation noted.
		The Operations Center staff is responsible for completing the mainframe changes. Once the change has been completed, the staff will update the Remedy Ticket indicating the move had occurred. In addition, the Remedy Ticket and	Reviewed a sample of Remedy Tickets to determine if the Operation Center staff updated and printed the Ticket, and screen printed the IPL.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		the IPL screen are printed to ensure accuracy of the information.		
		Library Services standards control the moves of changes to agency applications to production libraries.	Reviewed the Library Services Standards which controls moves to production.	No deviation noted.
		Library Services is responsible for moving agencies application changes into production. In order for a move to be completed, the agencies are required to submit an email from an authorized staff to Library Services indicating the date, time, and libraries to be moved into production.	Reviewed a sample of moves to determine if an authorized email was submitted which indicated the date, time, and libraries to be moved to production.	No deviation noted.
		Upon completion of the move, Library Services notifies the applicable agency.	Reviewed a sample of moves to determine if the agency was notified.	The Department did not maintain the notification emails to agencies indicating the move had been completed.
		For moves related to DCMS applications, the developer submits a move sheet to a secure mailbox. The move sheet is then forwarded to a Library Services mailbox by authorized staff.	Reviewed a sample of moves to determine if a move sheet and an authorized email was submitted which indicated the date, time, and libraries to be moved to production.	1 of 52 changes did not have a completed move sheet. 16 of 52 moves did not have an authorized email.

	Criteria	Department's Control	Testing Performed	Results
		Standards provide guidance on the configuration and deployment of network devices.	Reviewed the configuration templates and standards.	No deviation noted.
		Tools are in place to assist in the deployment of and reporting on configurations.	Reviewed a sample of networking devices to determine if they were connected to tools.	No deviation noted.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria for Availability

	Criteria	Department's Control	Testing Performed	Results
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements.	System capacity is monitored via software tools.	Reviewed software tool reports to determine if system capacity was monitored.	No deviation noted.
		The network is configured in a redundant manner.	Reviewed a sample of networking devices to determine if they were configured for redundancy.	10 of 60 devices were not configured for redundancy.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.	The DCMS/BCCS Infrastructure Services Recovery Activation Plan, IT Recovery Policy, and the Recovery Methodology have been developed.	Reviewed the DCMS/BCCS Infrastructure Services Recovery Activation Plan, ITS Recovery Policy, and the Recovery Methodology.	The Policy and Methodology had not been updated to reflect the change in recovery vendors and backup processes.
		The Department has entered into an Interagency Agreement with the Department of Agriculture for the utilization of space for a cold site.	Reviewed the Interagency Agreement with the Department of Agriculture.	No deviation noted.
		Application recovery plans or procedures have been developed.	Reviewed the applications' recovery plan or procedures.	The CIS Plan had not been tested as outlined in the Plan. The CPS Plan did not document testing requirements or RTO. eTime documentation did not outline

	Criteria	Department's Control	Testing Performed	Results
				responsibilities, testing, location of recovery documentation, and the RTO has not been determined.
		CA-Scheduler is utilized to schedule and control backups.	Reviewed a sample of backup schedules to determine if mainframe systems were backed up.	No deviation noted.
		Backups are conducted routinely.	Reviewed a sample of schedules to determine if backups were conducted.	No deviation noted.
		Application data is backed up daily, weekly and monthly.	Reviewed the backup schedule to determine if the applications were scheduled to be backed up daily, weekly and monthly.	No deviation noted.
			Reviewed a sample of backups to determine if the applications had been backed up.	No deviation noted.
		The Department verifies the daily and weekly backups completed successfully.	Reviewed a sample of the Verify Backup Reports to determine if backups were successful.	No deviation noted.
			Reviewed a sample of EMC logs to determine the success of data replication to the ADC.	No deviation noted.
		The Department is notified of failed backups.	Reviewed a sample of failed backups to determine if the Department was notified.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		Failed backups are recorded on the Shift Report.	Reviewed a sample of failed backups to determine if they were reported on the Shift Report.	No deviation noted.
		The Department takes remedial action on failed backups.	Reviewed a sample of failed backups to determine the actions taken.	No deviation noted.
		Library Services runs a report each morning to determine the success/failure of backup logs.	Reviewed a sample of reports to determine the success or failure of backups.	No deviation noted.
		Virtual tapes are replicated to the Alternate Data Center.	Reviewed a sample of EMC logs to determine the success of data replication to the ADC.	No deviation noted.
		The Library Guide provides guidance related to the tracking and movement of tape media.	Reviewed the Library Guide to determine if it contained guidance on the tracking and movement of tape media.	No deviation noted.
		The Tape Management System tracks the location of backups.	Reviewed a sample of tapes, to determine if the TMS accurately tracked the location of the backup.	No deviation noted.
		Agencies submit an email from an authorized staff indicating the tapes which need to be pulled and transported to the off-site vault.	Reviewed a sample of pulled tapes to determine if an authorized email had been provided.	No deviation noted.
		If an agency is to pick up the tapes, the individual is to present their driver's license, be on the Tape Media Authorization Listing and sign the security log.	Reviewed a sample of Media Transmittal Forms to determine if the individuals were on the Tape Media Authorization Listing.	No deviation noted.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria for Availability

	Criteria	Department's Control	Testing Performed	Results
		Physical backup tapes are stored offsite.	Reviewed a sample of tapes to determine if stored offsite.	No deviation noted.
		A physical inventory of tape media is conducted annually.	Obtained the annual inventory to determine if discrepancies had been rectified.	No deviation noted.
		The Department has installed preventive environmental measures at the CCF and the Communications Building. • Fire extinguishers, • Fire suppression, • Sprinkler system, • Water detection, • Cooling/heating systems, • UPS, and • Generators	Observed the measures in place to protect against environmental factors at the CCF and Communications Building.	No deviation noted.
			Reviewed the fire extinguishers and suppression system to determine if they were up to date.	No deviation noted.
			Reviewed a sample of days to determine if the cooling/heating measurements were within industry limits.	No deviation noted.
			Determined if UPS and Generators had been properly tested.	8 of 12 monthly testing reports were not provided.
		Preventive maintenance agreements and scheduled maintenance procedures are in place for environmental factors.	Reviewed scheduled procedures outlined in maintenance contracts.	After March 18, 2014, the Department did not maintain the maintenance logs for the automation and cooling systems for the CCF.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria for Availability

	Criteria	Department's Control	Testing Performed	Results
			Obtained the maintenance reports to determine if maintenance procedures were conducted in accordance with contracts.	The Department could not provide maintenance/testing reports for the heating/cooling systems, fire alarm, and generators. In addition the Department did not have a current maintenance contract for the generators.
		The Department has configured the network in a redundant manner.	Reviewed a sample of networking devices to determine if they were configured for redundancy.	10 of 60 devices were not configured for redundancy.
A1.3	Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements.	As part of the annual comprehensive test of Category One, Stage Zero applications/data, the DCMS/BCCS Infrastructure Services Recovery Activation Plan is tested.	Reviewed the DCMS/BCCS Infrastructure Services Recovery Activation Plan and testing documentation to determine if the Plan had been tested.	No deviation noted.
		The agencies are to submit to the Department, the goals and outcomes of their testing for review and updating of Plans and recovery documentation.	Reviewed testing documentation from the September 2013 comprehensive test.	Test documentation for testing conducted in September 2013 lacked detail to determine the outcome of the test.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria for Availability

	Criteria	Department's Control	Testing Performed	Results
		Application recovery plans or procedures have been developed.	Reviewed the applications' recovery plan or procedures.	The CIS Plan had not been tested as outlined in the Plan. The CPS Plan did not document testing requirements or RTO. eTime documentation did not outline responsibilities, testing, location of recovery documentation, and the RTO has not been determined.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria for Processing Integrity

	Criteria	Department's Control	Testing Performed	Results
PI1.1	Procedures exist to prevent, detect, and correct processing errors to meet processing integrity commitments and requirements.	System capacity is monitored via software tools.	Reviewed software tool reports to determine if system capacity was monitored.	No deviation noted.
		CA-Scheduler is utilized to schedule and control backups.	Reviewed a sample of backup schedules to determine if mainframe systems were backed up.	No deviation noted.
		Backups are conducted routinely.	Reviewed a sample of schedules to determine if backups were conducted.	No deviation noted.
		Application data is backed up daily, weekly and monthly.	Reviewed the backup schedule to determine if the applications had been scheduled to be backed up daily, weekly and monthly.	No deviation noted.
			Reviewed a sample of backups to determine if the applications had been backed up.	No deviation noted.
		The Department verifies the daily and weekly backups completed successfully.	Reviewed a sample of the Verify Backup Reports to determine if backups were successful.	No deviation noted.
			Reviewed a sample of EMC logs to determine the success of data replication to the ADC.	No deviation noted.
		The Department is notified of failed backups.	Reviewed a sample of failed backups to determine if the Department was notified.	No deviation noted.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria for Processing Integrity

	Criteria	Department's Control	Testing Performed	Results
		Failed backups are recorded on the Shift Report.	Reviewed a sample of failed backups to determine if they were reported on the Shift Report.	No deviation noted.
		The Department takes remedial action on failed backups.	Reviewed a sample of failed backups to determine the actions taken.	No deviation noted.
		Virtual tapes are replicated to the Alternate Data Center.	Reviewed a sample of EMC logs to determine the success of data replication to the ADC.	No deviation noted.
		The Department has installed preventive environmental measures at the CCF and the Communications Building. • Fire extinguishers, • Fire suppression, • Sprinkler system, • Water detection, • Cooling/heating systems, • UPS, and • Generators	Observed the measures in place to protect against environmental factors at the CCF and Communications Building.	No deviation noted.
			Reviewed the fire extinguishers and suppression system to determine if they were up to date.	No deviation noted.
			Reviewed a sample of days to determine if the cooling/heating measurements were within industry limits.	No deviation noted.
			Determined if UPS and Generators had been properly tested.	8 of 12 monthly reports were not provided.
		Environmental factors are monitored at the CCF and the Communication Building.	Observed the measures in place to protect against environmental factors at the CCF and Communications Building.	No deviation noted.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria for Processing Integrity

	Criteria	Department's Control	Testing Performed	Results
		Vendor agreements are in place for maintenance and support services associated with networking equipment.	Reviewed vendor agreements to determine if they were in place for maintenance and support.	No deviation noted.
			Reviewed a sample of hardware devices and software versions to determine if they were supported by the vendor.	28 of 60 hardware devices were no longer supported by the vendor. 11 of 60 software versions were no longer supported by the vendor.
PI1.2	System inputs are measured and recorded completely, accurately, and timely in accordance with processing integrity commitments and requirements.	Data entry screens contain field edits and range checks, which provide immediate notification of an error.	Reviewed a sample of field edits and range checks to determine if they were functioning appropriately and were providing error notifications.	27 of 51 States' (including Washington DC) tax rates were not included in the CPS tax table. 17 of 24 States' (including Washington DC) tax rates were incorrect. The State of Illinois tax rate was correct.
			Reviewed a sample of agencies data to determine if edits and checks were functioning appropriately.	No deviation noted.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria for Processing Integrity

	Criteria	Department's Control	Testing Performed	Results
PI1.3	Data is processed completely, accurately, and timely as authorized in accordance with processing integrity commitments and requirements.	Applications provide various balancing reports to ensure accuracy of information.	Reviewed the balancing reports to ensure the accuracy of information.	No deviation noted.
		Each transaction is assigned an identifying number.	Reviewed a sample of agencies data to determine if each transaction had an identifying number assigned.	No deviation noted.
PI1.4	Data is stored and maintained completely and accurately for its specified life span in accordance with processing integrity commitments and requirements.	Applications provide various balancing reports to ensure accuracy of information.	Reviewed the balancing reports to ensure the accuracy of information.	No deviation noted.
		The Department maintains transaction history for a defined period of time.	Reviewed the transaction history.	No deviation noted.
		Access to the application's production libraries has been restricted to authorized Department personnel.	Reviewed a sample of users with access to production libraries to determine appropriateness.	4 of 10 programmers had inappropriate access to production libraries.
		Application data is backed up daily, weekly and monthly.	Reviewed the backup schedule to determine if the applications were scheduled to be backed up daily, weekly and monthly.	No deviation noted.
			Reviewed a sample of backups to determine if the applications had been backed up.	No deviation noted.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria for Processing Integrity

	Criteria	Department's Control	Testing Performed	Results
PI1.5	System output is complete, accurate, distributed, and retained in accordance with processing integrity commitments and requirements.	Hardcopy output is printed at a secure facility with security guards, cardkey system, and security cameras.	Observed security at the facility; security guards, cardkey system, and cameras.	No deviation noted.
		In order to access the print shop, an individual's ID Badge must have applicable access or the individual must sign in as a visitor and be escorted.	Reviewed the print shop access report to determine appropriateness of access.	134 of 152 individuals no longer required access.
		Upon request for pick up, the individual must provide identification, sign the Report Distribution Checklist, and be on the authorization listing.	Reviewed a sample of Report Distribution Checklists to determine if the individuals who picked up the print job were authorized.	2 individual listed on Report Distribution Checklist for 26 days sampled were not on the authorization listing.
		Applications provide various balancing reports to ensure accuracy of information.	Reviewed the balancing reports to ensure the accuracy of information.	No deviation noted.
PI1.6	Modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.	Application level security restricts the ability to access, approve transactions, modify and delete transactions.	Reviewed the security tables to determine if the level of security restricts the ability to access, approve, modify and delete transactions.	No deviation noted.
		Access to the application's production libraries has been restricted to authorized Department personnel.	Reviewed a sample of users with access to production libraries to determine appropriateness.	4 of 10 programmers had inappropriate access to production libraries.

TRUST SERVICES-CRITERIA, RISK, RELATED CONTROLS, TEST OF CONTROLS, AND RESULTS THEREOF
Criteria for Processing Integrity

	Criteria	Department's Control	Testing Performed	Results
		Application data is backed up daily, weekly and monthly.	Reviewed the backup schedule to determine if the applications were scheduled to be backed up daily, weekly and monthly.	No deviation noted.
			Reviewed a sample of backups to determine if the applications had been backed up.	No deviation noted.

This page intentionally left blank

Other Information Provided by the Department of Central Management Services, Bureau of Communications and Computer Services that is Not Covered by the Service Auditor's Report

Department's Corrective Action Plan
(Not Examined)

The Department agrees with the deficiencies noted in the Auditor's report and will take the following actions to proactively address the noted deficiencies.

The Department will review specific policy language concerning the requirement of an email request to the Help Desk for password resets, update applicable policies and procedures and communicate the process with employees to ensure compliance.

The Department will review specific policy language regarding monitoring compliance with security policies. The language will be modified to reflect what can reasonably be accomplished given resource constraints.

The Department will review the current risk assessment framework, update it as appropriate and conduct risk assessments as resources become available. The Department has begun assessing risk for new developments as of January 1, 2014 in the Enterprise Application & Architecture area.

The Department has taken or will take the following actions:

Principle	Criteria	Corrective Action Plan
Common Criteria	C.C. 2.3	The Department will review policies, update and communicate user responsibilities as appropriate.
	C.C. 2.4	The Department will review policies, update and communicate user responsibilities as appropriate.
	C.C.2.5	The Department has an active project underway to solidify the processes for reporting and resolving user security issues.
	C.C. 2.6	The Department will ensure relevant items are discussed in change meetings and documented.
	C.C. 5.1	The Department will make every effort to comply with access and password policies and procedures.
	C.C. 5.2	The Department will develop procedures for granting/removing access to staff and will ensure documentation is completed and maintained.
	C.C. 5.3	The Department will make every possible effort to comply with password control policies and procedures.
	C.C. 5.4	The Department will develop procedures for granting/removing access to staff and will ensure documentation is completed and maintained.

	C.C. 5.5	The Department will work with its managers and the CMS Bureau of Facilities Management to ensure the ID badge request process is properly followed, building access rules are followed and access rights are revoked as necessary.
	C.C. 5.6	The Department has measures in place to remove and protect its resources from outside threats. CMS/BCCS has entered into an enterprise-wide extended support contract to address critical security updates.
	C.C. 5.7	The Department has an active project underway to solidify the processes for the handling of security issues reported by users. The Department has an active end of life cycle project in progress to ensure the protection of sensitive data.
	C.C. 5.8	The Department will work to review the devices for prevention and detection controls to ensure they are implemented.
	C.C. 6.1	The Department will review, update and implement processes to ensure monitoring and alerts are maintained.
	C.C. 7.1	Applications and Architecture Division has finalized policies and procedures documenting the change control process over application changes and will ensure they are fully implemented. The Department will ensure changes are tracked from initiation to implementation. The Application Lifecycle Manual will be revised to reflect the present accepted processes and procedures for minor application changes.
	C.C. 7.2	The Change Management Guide will be reviewed and updated as necessary and the Department will emphasize compliance and proper documentation. Library Services will update the agency approver listing.
	C.C. 7.3	The Change Management Guide will be reviewed and updated as necessary and the Department will emphasize compliance and proper documentation. The Department's Enterprise Applications and Architecture Division has finalized policies and procedures documenting the change control process over application changes and will ensure they are fully implemented.
	C.C. 7.4	The Department will emphasize the importance of completing all fields of the move sheets and Library Services will update the agency about the move.

Principle	Criteria	Corrective Action Plan
Availability	A 1.1	The Department will review network configuration to determine the operational requirement of adding capacity to help meet availability needs.
	A 1.2	The Department will review and update its policies and plans to ensure environmental protections, data backup processes, recovery infrastructure and documentation is maintained to meet processing integrity and availability requirements.
	A 1.3	The Department will review and update its policies and plans to ensure environmental protections, data backup processes, recovery infrastructure and documentation is maintained to meet processing integrity and availability requirements.
Processing	P.I. 1.1	The Department will review the Recovery plan and update as needed and emphasize proper documentation of testing in all cases. The Department will work with user agencies to provide recovery classifications for their applications.
	P.I. 1.2	The Department will review State Taxes for states where employees reside, correct them as needed, and implement a process to ensure the rates are updated.
	P.I. 1.4	The Department will review access rights and correct them as needed. The Department is aware of the problem and has started addressing this as a high priority.
	P.I. 1.5	The Department will work to ensure the report pickup procedures are followed.
	P.I. 1.6	The Department will review access rights and correct them as needed.

Department's Analysis of Staffing Trends
(Not Examined)

The following table reflects staff losses experienced by the Bureau since FY07. As shown, the Bureau has lost a significant number of staff during this period, which has affected its ability to operate effectively, particularly in some areas. The net staff losses alone would create a challenge, but the numbers do not reflect the institutional knowledge that has been lost, as many long-term employees have reached retirement age. In addition, a recent analysis has shown a high number of staff will be eligible to retire in the next two years. These issues are compounded by difficulty hiring qualified staff, especially in areas that require knowledge and experience on older technologies. Bureau Management has been proactive in attempting to address this issue, but nevertheless, it should be considered a major risk.

Fiscal Year	**Number of Separations**	**Number of Hires**	**Net Staff Loss**
2007	57	39	18
2008	49	12	37
2009	38	23	15
2010	47	9	38
2011	49	7	42
2012	72	16	56
2013	51	37*	14
2014	48	20**	28
TOTAL	**411**	**163**	**248**

*12 of 37 hires were from consolidation.
**3 of the 20 hires were from consolidation.

Listing of User Agencies of the State of Illinois Mainframe Information Technology Environment (Not Examined)

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 Corrections-Correctional Industries
12. Department of Employment Security
13. Department of Financial and Professional Regulation
14. Department of Healthcare and Family Services
15. Department of Human Rights
16. Department of Human Services
17. Department of Insurance
18. Department of Juvenile Justice
19. Department of Labor
20. Department of Lottery
21. Department of Military Affairs
22. Department of Natural Resources
23. Department of Public Health
24. Department of Revenue
25. Department of Transportation
26. Department of Veterans' Affairs
27. Department on Aging
28. East St. Louis Financial Advisory Authority
29. Eastern Illinois University
30. Environmental Protection Agency
31. Executive Ethics Commission
32. General Assembly Retirement System
33. Governors State University
34. Guardianship and Advocacy Commission
35. House of Representatives
36. Human Rights Commission
37. Illinois Arts Council
38. Illinois Civil Service Commission
39. Illinois Commerce Commission
40. Illinois Comprehensive Health Insurance Plan
41. Illinois Community College Board
42. Illinois Council on Developmental Disabilities
43. Illinois Criminal Justice Information Authority
44. Illinois Deaf and Hard of Hearing Commission
45. Illinois Educational Labor Relations Board
46. Illinois Emergency Management Agency
47. Illinois Finance Authority
48. Illinois Gaming Board

Information provided by the Department of Central Management Services – Not Examined

49. Illinois Health Information Exchange Authority
50. Illinois Historic Preservation Agency
51. Illinois Housing Development Authority
52. Illinois Independent Tax Tribunal
53. Illinois Labor Relations Board
54. Illinois Law Enforcement Training and Standards Board
55. Illinois Math and Science Academy
56. Illinois Medical District Commission
57. Illinois Office of the State's Attorneys Appellate Prosecutor
58. Illinois Pollution Control Board
59. Illinois Power Agency
60. Illinois Prisoner Review Board
61. Illinois Procurement Policy Board
62. Illinois Racing Board
63. Illinois State Board of Investment
64. Illinois State Police
65. Illinois State Toll Highway Authority
66. Illinois State University
67. Illinois Student Assistance Commission
68. Illinois Workers' Compensation Commission
69. Joint Committee on Administrative Rules
70. Judges' Retirement System
71. Judicial Inquiry Board
72. Legislative Audit Commission
73. Legislative Ethics Commission
74. Legislative Information System
75. Legislative Printing Unit
76. Legislative Reference Bureau
77. Legislative Research Unit
78. Northeastern Illinois University
79. Northern Illinois University
80. Office of Management and Budget
81. Office of the Architect of the Capitol
82. Office of the Attorney General
83. Office of the Auditor General
84. Office of the Comptroller
85. Office of the Executive Inspector General
86. Office of the Governor
87. Office of the Legislative Inspector General
88. Office of the Lieutenant Governor
89. Office of the Secretary of State
90. Office of the State Appellate Defender
91. Office of the State Fire Marshal
92. Office of the Treasurer
93. Property Tax Appeal Board
94. Senate Operations
95. Sex Offender Management Board
96. Southern Illinois University
97. State Board of Education
98. State Board of Elections
99. State Charter School Advisory Commission
100. State Employees' Retirement System

Information provided by the Department of Central Management Services – Not Examined

101. State Police Merit Board
102. State Universities Civil Service System
103. State Universities Retirement System
104. Supreme Court of Illinois
105. Teachers' Retirement System of the State of Illinois
106. University of Illinois
107. Western Illinois University

Listing of User Agencies of the Accounting Information System (Not Examined)

1. Board of Higher Education
2. Capital Development Board
3. Department of Agriculture
4. Department of Central Management Services
5. Department of Corrections
6. Department of Financial and Professional Regulation
7. Department of Human Rights
8. Department of Insurance
9. Department of Labor
10. Department of the Lottery
11. Department of Military Affairs
12. Department of Natural Resources
13. Department of Public Health
14. Department of Revenue
15. Department on Aging
16. Department of Veterans' Affairs
17. Environmental Protection Agency
18. Guardianship and Advocacy Commission
19. Historic Preservation Commission
20. Human Rights Commission
21. Illinois Arts Council
22. Illinois Civil Service Commission
23. Illinois Commerce Commission
24. Illinois Community College Board
25. Illinois Council on Developmental Disabilities
26. Illinois Criminal Justice Information Authority
27. Illinois Deaf and Hard of Hearing Commission
28. Illinois Educational Labor Relations Board
29. Illinois Emergency Management Agency
30. Illinois Gaming Board
31. Illinois Independent Tax Tribunal
32. Illinois Labor Relations Board
33. Illinois Law Enforcement Training and Standards Board
34. Illinois Office of the State's Attorneys Appellate Prosecutor
35. Illinois Prisoner Review Board
36. Illinois Procurement Policy Board
37. Illinois Racing Board
38. Illinois Student Assistance Commission

39. Illinois Workers' Compensation Commission
40. Judges' Retirement System
41. Judicial Inquiry Board
42. Office of Management and Budget
43. Office of the Attorney General
44. Office of the Auditor General
45. Office of the Executive Inspector General
46. Office of the Governor
47. Office of the Lieutenant Governor
48. Office of the State Appellate Defender
49. Office of the State Fire Marshal
50. Property Tax Appeal Board
51. State Board of Elections
52. State Employees' Retirement System of Illinois
53. State Police Merit Board
54. State Universities Civil Service System
55. Supreme Court of Illinois

Listing of Users Agencies of the Central Inventory System
(Not Examined)

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 Regulations
6. Department of Human Rights
7. Department of Military Affairs
8. Department of Public Health
9. Department of Transportation
10. Department of Veterans' Affairs
11. Department on Aging
12. Environmental Protection Agency
13. Historic Preservation Agency
14. Illinois Arts Council
15. Illinois Deaf and Hard of Hearing Commission
16. Illinois Law Enforcement Training and Standards Board
17. Illinois Office of the State's Attorneys Appellate Prosecutor
18. Office of Management and Budget
19. Office of the Attorney General
20. Office of the Governor
21. Office of the Lieutenant Governor

Listing of User Agencies of the Central Payroll System

(Not Examined)

1. Board of Higher Education
2. Capital Development Board
3. Commission on Government Forecasting and Accountability
4. Court of Claims
5. Department of Agriculture
6. Department of Central Management Services
7. Department of Children and Family Services
8. Department of Commerce and Economic Opportunity
9. Department of Corrections
10. Department of Financial and Professional Regulation
11. Department of Human Rights
12. Department of Insurance
13. Department of Juvenile Justice
14. Department of Labor
15. Department of the Lottery
16. Department of Military Affairs
17. Department of Natural Resources
18. Department of Public Health
19. Department of Revenue
20. Department on Aging
21. East St. Louis Financial Advisory Authority
22. Emergency Management Agency
23. Environmental Protection Agency
24. Executive Ethics Commission
25. Guardianship and Advocacy Commission
26. House of Representatives
27. Human Rights Commission
28. Illinois Arts Council
29. Illinois Civil Service Commission
30. Illinois Commerce Commission
31. Illinois Community College Board
32. Illinois Council on Developmental Disabilities
33. Illinois Criminal Justice Information Authority
34. Illinois Deaf and Hard of Hearing Commission
35. Illinois Educational Labor Relations Board
36. Illinois Gaming Board
37. Illinois Health Information Exchange Authority
38. Illinois Historic Preservation Agency
39. Illinois Independent Tax Tribunal
40. Illinois Labor Relations Board
41. Illinois Law Enforcement Training and Standards Board
42. Illinois Math and Science Academy
43. Illinois Office of the State's Attorneys Appellate Prosecutor
44. Illinois Power Agency
45. Illinois Prisoner Review Board
46. Illinois Procurement Policy Board
47. Illinois Racing Board
48. Illinois State Board of Investment
49. Illinois State Police
50. Illinois Student Assistance Commission
51. Illinois Workers' Compensation Commission
52. Joint Committee on Administrative Rules
53. Judges' Retirement System
54. Judicial Inquiry Board
55. Legislative Audit Commission
56. Legislative Ethics Commission
57. Legislative Information System
58. Legislative Printing Unit
59. Legislative Reference Bureau
60. Legislative Research Unit
61. Office of Management and Budget
62. Office of the Architect of the Capitol
63. Office of the Attorney General
64. Office of the Auditor General
65. Office of the Executive Inspector General
66. Office of the Governor
67. Office of the Lieutenant Governor
68. Office of the State Appellate Defender
69. Office of the State Fire Marshal
70. Office of the Treasurer
71. Property Tax Appeal Board
72. Senate Operations
73. State Board of Education
74. State Board of Elections
75. State Employees' Retirement System of Illinois
76. State of Illinois Comprehensive Health Insurance Board
77. State Police Merit Board
78. State Universities Civil Service System
79. Teachers' Retirement System of the State of Illinois

Information provided by the Department of Central Management Services – Not Examined

Listing of User Agencies of the Central Time and Attendance System
(Not Examined)

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 Insurance
8. Department of Labor
9. Department of the Lottery
10. Department of Natural Resources
11. Department of Public Health
12. Department of Revenue
13. Department of Veterans' Affairs
14. Department on Aging
15. Environmental Protection Agency
16. Executive Ethics Commission
17. Guardianship and Advocacy Commission
18. Human Rights Commission
19. Illinois Civil Service Commission
20. Illinois Comprehensive Health Insurance Plans
21. Illinois Deaf and Hard of Hearing Commission
22. Illinois Educational Labor Relations Board
23. Illinois Gaming Board
24. Illinois Independent Tax Tribunal
25. Illinois Law Enforcement Training and Standards Board
26. Illinois Planning Council on Developmental Disabilities
27. Illinois Power Agency
28. Illinois Prisoner Review Board
29. Illinois Procurement Policy Board
30. Illinois Racing Board
31. Illinois State Police
32. Illinois Workers' Compensation Commission
33. Office of the Attorney General
34. Office of the Executive Inspector General
35. Office of the Governor
36. Office of the Lt. Governor
37. Office of the State Fire Marshal
38. Property Tax Appeal Board
39. State Board of Elections
40. State Employees' Retirement System of Illinois

Listing of User Agencies of the eTime System
(Not Examined)

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 Regulations
6. Department of Human Rights
7. Department of Insurance
8. Department of Labor
9. Department of the Lottery
10. Department of Public Health
11. Department of Revenue
12. Executive Ethics Commission
13. Guardianship and Advocacy Commission
14. Illinois Deaf and Hard of Hearing Commission
15. Illinois Health Information Exchange Authority
16. Illinois Prisoner Review Board
17. Illinois Workers' Compensation Commission
18. Office of the Lieutenant Governor
19. Property Tax Appeal Board
20. State Employees' Retirement System of Illinois

Listing of Security Software Proxy Agencies
(Not Examined)

1. Capital Development Board
2. Chicago State University
3. Commission on Government Forecasting and Accountability
4. Court of Claims
5. Department of Agriculture
6. Department of Central Management Services
7. Department of Human Rights
8. Department of Labor
9. Department of Military Affairs
10. Department of Veterans Affairs
11. Eastern Illinois University
12. Executive Ethics Commission
13. Governor's State University
14. Guardianship and Advocacy Commission
15. House of Representatives
16. Human Rights Commission
17. Illinois Arts Council
18. Illinois Civil Service Commission
19. Illinois Commerce Commission
20. Illinois Community College Board
21. Illinois Comprehensive Health Insurance Plan
22. Illinois Council on Developmental Disabilities
23. Illinois Deaf and Hard of Hearing Commission
24. Illinois Educational Labor Relations Board
25. Illinois Emergency Management Agency
    Illinois Health Information Exchange Authority
26. Illinois Historic Preservation Agency
27. Illinois Housing Development Authority
    Illinois Independent Tax Tribunal
28. Illinois Labor Relations Board
29. Illinois Law Enforcement Training and Standards Board
30. Illinois Math and Science Academy
31. Illinois Medical District Commission
32. Illinois Office of the State's Attorneys Appellate Prosecutor
33. Illinois Power Agency
34. Illinois Prisoner Review Board
35. Illinois Procurement Policy Board

36. Illinois State Board of Investment
37. Illinois State Toll Highway Authority
38. Illinois State University
39. Joint Committee on Administrative Rules
40. Judicial Inquiry Board
41. Legislative Audit Commission
42. Legislative Ethics Commission
43. Legislative Information Systems
44. Legislative Printing Unit
45. Legislative Reference Bureau
46. Legislative Research Unit
47. Northeastern Illinois University
48. Northern Illinois University
49. Office of Management and Budget
50. Office of the Architect of the Capital
51. Office of the Attorney General
52. Office of the Comptroller
53. Office of the Executive Inspector General
54. Office of the Governor
    Office of the Legislative Inspector General
55. Office of the Lieutenant Governor
56. Office of the Secretary of State
57. Office of the State Appellate Defender
58. Office of the State Fire Marshall
59. Office of the Treasurer
60. Property Tax Appeal Board
61. Senate Operations
62. Southern Illinois University
63. State Board of Education
64. State Board of Elections
65. State Police Merit Board
66. State Universities Civil Service System
67. State Universities Retirement System
68. University of Illinois
69. Western Illinois University

ACRONYM GLOSSARY

ACL – Access Control List
ADC – Alternate Data Center
AIS – Accounting Information System
BCCS – Bureau of Communication and Computer Services
Bureau – Bureau of Communication and Computer Services
BRM – Business Reference Model
CAC – Change Advisory Committee
CCF – Central Computer Facility
CICS – Customer Information Control System
CIRT – Critical Incident Response Team
CIS – Central Inventory System
CISO – Chief Information Security Officer
CMC – Customer Management Center
CMS – Central Management Services
CPS – Central Payroll System
CPU – Central Processing Unit
CTAS – Central Time and Attendance
CTO – Chief Technology Officer
DASD – Direct Access Storage Device
DB2 – Database 2
DCMS – Department of Central Management Services
Department – Department of Central Management Services
DNS – Domain Name Service
DP – Data Processing
DR – Disaster Recovery
EAA – Enterprise Application & Architecture
ECM – Enterprise Change Management
EoL – End of Life
EPMO – Enterprise Program Management Office
ESR – Enterprise Service Request
FISMA – Federal Information Security Management Act
FY – Fiscal Year
HIPAA – Health Insurance Portability and Accountability Act
HR – Human Resources
ICN – Illinois Century Network
ID – Identification
ISD – Infrastructure Services Division
ILCS – Illinois Compiled Statutes
IMS – Information Management System
IT – Information Technology
ITG – Information Technology Governance
LAN – Local Area Network
MORT – Major Outage Response Team

NCC – Network Control Center
NIST– National Institute of Standards and Technology
PKI – Public Key Infrastructure
POP – Point of Presence
RACF – Resource Access Control Facility
RFC – Request for Change
RMF – Resource Monitoring Facility
RTC – Regional Technology Center
RTO – Recovery Time Objective
SSL – Secure Socket Level
UPS – Uninterruptible Power Supply
VOIP – Voice Over Internet Protocol
VPN – Virtual Private Network
WAN – Wide Area Network
z/OS – Zero Downtime Operating System
z/VM – Zero Downtime Virtual Machine