STATE OF ILLINOIS

OFFICE OF THE AUDITOR GENERAL

SERVICE ORGANIZATION CONTROL REPORT

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
BUREAU OF COMMUNICATIONS &
COMPUTER SERVICES

For the Year Ended June 30, 2016

FRANK J. MAUTINO

AUDITOR GENERAL

SERVICE ORGANIZATION CONTROL REPORT

Department of Central Management Services
Bureau of Communications and
Computer Services

TABLE OF CONTENTS

Illinois Department of
Innovation & Technology

Bruce Rauner, Governor
Hardik Bhatt
Secretary Designate Department of Innovation & Technology
State CIO

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 Throughout the Period July 1, 2015 to June 30, 2016

July 29, 2016

The Honorable Frank J. Mautino
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, 2015 to June 30, 2016" (the description), based on the criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)* (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 TSP section 100, *Trust Service Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that:

a. the description does not fairly presents the system throughout the period July 1, 2015 through June 30, 2016, 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 structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunication 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, entity users, vendor personnel, and managers).
        - *Procedures.* The automated and manual procedures.
        - *Data.* Transaction streams, files, databases, tables, and output used or processed by the system.

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

(4) For information provided to, or received from, subservice organizations or other parties.

- How such information is provided or received and the role of the subservice organization and other parties.
- The procedures the Department of Central Management Services performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

- Complementary user entity controls contemplated in the design of the Department of Central Management Services' system.

(6) For subservice organizations presented using the carve-out method

- the nature of the services provided by the subservice organization
- each of the applicable trust criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the Department of Central Management Services, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

(7) 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 subservice organization and the reasons therefore.

(8) In the case of a type 2 report, relevant details of changes to 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 presented 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. Because of the matters described in the following paragraph, the controls stated in the description were not suitably designed throughout July 1, 2015 to June 30, 2016, to meet the applicable trust service criteria.

iii. In the event an Active Directory ID needs to be modified, an email or an Enterprise Service Request is to be received indicating the necessary modifications. However, the Department was unable to provide the auditors a universe of Active Directory ID modifications.

iv. 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, the password resets were completed via direct phone call or without an email to the Department's Security Software Coordinator, the Security Software Administrator or the Help Desk.

v. In the event a mainframe security software ID needs to be modified, users are required to submit an approved Mainframe Application Access Request Form or an Enterprise Service Request. However, the Department was unable to provide the auditors a universe of mainframe security software ID modifications.

vi. The Department's Compliance Officer is responsible for monitoring and ensuring compliance with policies and procedures. However, monitoring for compliance has not been conducted.

vii. Controls related to "the Department is notified of failed backups, failed backups are recorded on the Shift Report, the Department takes remedial action on failed backups, and a Remedy ticket is opened in the event of an issue did not occur during the period covered by the Report, because the circumstances that warrant the operation of those controls did not occur during the period.

viii. Controls related to "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, a Remedy ticket will be opened, and if necessary the Technical Safeguards team will be alerted" did not occur during the period covered by the Report, because the circumstances that warrant the operation of those controls did not occur during the period.

e. Any subsequent events to the period covered by management's Description of the Department's system up to the date of the service auditor's report that could have a significant effect on management's assertion or the fact that no such subsequent events have occurred.

Sincerely,

SIGNED ORIGINAL ON FILE

Hardik Bhatt
Secretary Designated
Department of Innovation & Technology

SPRINGFIELD OFFICE:
ILES PARK PLAZA
740 EAST ASH • 62703-3154
PHONE: 217/782-6046
FAX: 217/785-8222 • TTY: 888/261-2887
FRAUD HOTLINE: 1-855-217-1895

CHICAGO OFFICE:
MICHAEL A. BILANDIC BLDG. • SUITE S-900
160 NORTH LASALLE • 60601-3103
PHONE: 312/814-4000
FAX: 312/814-4006
FRAUD HOTLINE: 1-855-217-1895

OFFICE OF THE AUDITOR GENERAL
FRANK J. MAUTINO

INDEPENDENT SERVICE AUDITOR'S REPORT

The Honorable Frank J. Mautino
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, 2015 to June 30, 2016" (description) based on the criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (*SOC 2) (description criteria) 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 TSP Section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, or Privacy* (AICPA, *Trust Services Principles and Criteria*) (applicable trust services criteria), throughout the period July 1, 2015 to June 30, 2016. 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' (Department) controls are suitably designed and operating effectively, along with related controls at the Department. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-agency controls.

As indicated in the description, the Department utilizes a service organization (subservice 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 certain types of controls that management expects to be implemented at the subservice organization are suitably designed and operating effectively. The description presents the Department's 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 controls expected to be implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization, and we have not evaluated whether the controls management expects to be implemented at the subservice organization have been implemented or whether such controls were suitability designed and operating effectively throughout the period July 1, 2015 to June 30, 2016.

The information included in the section 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” is presented by management of the Department to provide additional information and is not a part of the description. Information related to the Department’s corrective action plan, staffing trends, user agency listings, information regarding the establishment of the Department of Innovation and Technology, and the Statewide financial solution (ERP) has not been subjected to procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria.

Service organization’s responsibilities
The Department has provided its assertion titled "Assertion of the Management of the Department of Central Management Services, Bureau of Communications and Computer Services,” (assertion) about the fairness of the presentation of the description based on the description criteria and the suitability of design and operating effectiveness of the controls described therein to meet the applicable trust service criteria. The Department is responsible for preparing the description and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting the controls to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the description.

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 and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted 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 and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period July 1, 2015 to June 30, 2016.

An examination of the description of a service organization system and the suitability of the design and operating effectiveness of those controls to meet the applicable trust service criteria involves:

- Evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively, to meet the applicable trust services criteria throughout the period July 1, 2015 to June 30, 2016.
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively.
- Testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- Evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in its assertion.

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 service 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 risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion
The accompanying description states that the Department had not conducted periodic risk assessments, in order to identify threats and vulnerabilities, and assess the impact. Because controls were not operating for those controls related to risk assessments, testing of operating effectiveness could not be conducted.

The Department states in the description that, in the event a user requires their Active Directory password to be reset, they contact the Help Desk via email, submit a problem report or utilize one the Department’s two Self-Service Solutions. However, as noted on pages 60, 65, and 76 of the “Description of Tests of Controls and Results Thereof”, the Department did not require an email or problem report to be submitted for Active Directory password resets. Thus, the control over the reset of Active Directory passwords was not operating effectively throughout the period July 1, 2015 to June 30, 2016. This control deficiency resulted in the Department not meeting the criteria “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. 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. 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 Department states in the description that, in the event an Active Directory ID needs to be modified, an email or an Enterprise Service Request is to be received indicating the necessary modifications. However, as noted on pages 59 and 64 of the "Description of Test of Controls and Results Thereof", the Department was unable to provide the auditors a universe of Active Directory ID modifications; therefore, detailed testing was unable to be conducted. Thus, the control over the modification of Active Directory IDs was not operating effectively throughout the period July 1, 2015 to June 30, 2016. This control deficiency resulted in the Department not meeting the criteria "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. 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."

The Department also 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 pages 60, 65, and 75 of the "Description of Tests of Controls and Results Thereof", the password resets were completed without an 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, 2015 to June 30, 2016. This control deficiency resulted in the Department not meeting the criteria "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. 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. 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 Department states in the description that, in the event a mainframe security software ID needs to be modified, users are required to submit an approved Mainframe Application Access Request Form or an Enterprise Service Request. However, as noted on pages 59 and 64, of the "Description of Test of Controls and Results Thereof", the Department was unable to provide the auditors a universe of mainframe security software ID modifications; therefore, detailed testing was unable to be conducted. Thus, the control over the modification of mainframe security software IDs was not operating effectively throughout the period July 1, 2015 to June 30, 2016. This control deficiency resulted in the Department not meeting the criteria "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. 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."

The Department states in the description that the Department's Compliance Officer is responsible for monitoring and ensuring compliance with policies and procedures. However, as noted on page 41 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 policies and procedures was not operating effectively throughout the period July 1, 2015 to June 30, 2016. This control deficiency resulted in the Department 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."

In our opinion, in all material respects because of the matters referred to in the preceding paragraphs, based on the criteria identified in the Department of Central Management Services, Bureau of Communications and Computer Services' assertion:

a. the description does not fairly present the system that was designed and implemented throughout the period July 1, 2015 to June 30, 2016.

b. the controls stated in the description were not 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, 2015 to June 30, 2016, user entities applied the complementary user entity control contemplated in the design of the Department's controls throughout the period July 1, 2015 to June 30, 2016, and the subservice organization applied the types of controls expected to be implemented at the subservice organization throughout the period July 1, 2015 to June 30, 2016.

c. the controls tested, which were those necessary to provide reasonable assurance that the applicable trust services criteria were met, did not operate effectively throughout the period July 1, 2015 to June 30, 2016, if the user entities applied the complementary user entity control contemplated in the design of the Department's controls throughout the period July 1, 2015 to June 30, 2016, and if the controls expected to be implemented at the subservice organization were also operating effectively throughout the period July 1, 2015 to June 30, 2016.

Description of tests of controls

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

Controls Did Not Operate During the Period Covered by the Report

As indicated on pages 78, 81, 94, 95, 101, 102, and 103 of the "Description of Test of Controls and Results Thereof", the Department did not encounter any failed backups during the period July 1, 2015 to June 30, 2016; therefore, we did not perform any tests of the design or operating effectiveness of controls related to "the Department is notified of failed backups, failed backups are recorded on the Shift Report, the Department takes remedial action on failed backups, and a Remedy ticket is opened in the event of an issue."

As indicated on page 53 of the "Description of Test of Controls and Results Thereof", the Department did not encounter any security breaches during the period July 1, 2015 to June 30, 2016; therefore, we did not perform any tests of the design or operating effectiveness of controls related to "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."

Emphasis-of-Matter

As described in the section 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," subsequent to the period covered by the service auditor's report, effective July 1, 2016, the Department's and State agencies' information technology functions were transferred to the Department of Innovation and Technology.

Intended use

This report and the section titled "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 State of Illinois Mainframe Information Technology Environment System during some or all of the period July 1, 2015 to June 30, 2016, 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 its distribution is not limited; however, the endorsed use of the Report is outlined in the Intended Use Section.

SIGNED ORIGINAL ON FILE

William J. Sampias, CISA
Director, Information Systems Audits

SIGNED ORIGINAL ON FILE

Mary Kathryn Lovejoy, CPA, CISA
Audit Manager

July 29, 2016
Springfield, Illinois

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, 2015 TO JUNE 30, 2016

Background

The Department of Central Management Services Bureau of Communications and Computer Services (Department) 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 is forward looking and innovative. Management values customer and employee input, not only to be aware of issues, but to enhance services and improve support. Security is also valuable to management, including security over the infrastructure as well as customer's data and information. Providing fast, reliable and secure Information Technology services that are easy to obtain are the primary objectives.

Organization and Management

The Department is organized within functional areas and organizational and reporting hierarchies have been established.

Deputy Director

The Deputy Director is the State Chief Information Officer (CIO) with Information Technology (IT) oversight of agencies under the Governor. The Deputy Director is also responsible for the overall management of Information Technology and Telecommunication functions, which includes services provided to agencies as well as other Illinois government entities. The Deputy Director works with senior management, agency directors and the Governor's Office to develop policies, priorities and plans for Statewide Information Technology and Telecommunication programs. The Deputy Director is responsible for the following teams:

Chief of Staff

The Chief of Staff provides functional oversight of operations and integration of activities, oversees and provides direction to Human Resources, Fiscal Office, IT/Telecommunication Procurement and Agency Relations. 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 operations.

Workforce Development and Logistics/Human Resources

Workforce Development and Logistics coordinates and facilitates internal personnel paperwork, workforce training, development and implementation, and workforce logistics.

Chief Fiscal Officer

The Chief Fiscal Officer oversees the fiscal operations and manages the Communications Revolving Fund and the Statistical Services Revolving Fund.

Chief of Enterprise Infrastructure

The Infrastructure Services Division is responsible for the operational management of the data centers, operational management of production control and input services, print operations, personal identity management, customer administration, software distribution, mainframe and mid-range systems, and data storage components. The Infrastructure Services Division is divided into several teams:

Data Center Operations

- Mainframe Services is responsible for the mainframe operating systems, database systems, software installation, maintenance, and support functions/services.
- Enterprise Storage and Backup is responsible for the oversight and management of the storage and backup systems across hosted and supported platforms.
- Storage Management Services is responsible for configuration, installation, and maintenance activities for the enterprise data storage infrastructure. This group performs heath/performance management and problem resolution activities. This group is also responsible for and performs data backup and restoration services.

Enterprise Production

- Library Services is responsible for the change management process for migration of mainframe application programs to the production environment for specific agencies. It is also responsible for the restoration and synchronization of program libraries for business continuity management.
- Production Control is responsible for the setup and maintenance of the mainframe automated scheduling system(s) for batch processing.
- Command Center Operations is responsible for providing continuous monitoring and operation of the computing resources to ensure availability, performance, and support response necessary to sustain user business demands.

- Input Services is responsible for monitoring and error resolution for the nightly and weekend mainframe batch processing.
- Mainframe Backup and Monitoring is responsible for the control and scheduling of backups on a routine daily and weekly basis consisting of system and program files needed to restore the infrastructure in the event of a disaster, including: (1) weekly for full system and subsystem volume backups; (2) daily for incremental system and subsystem volume backups. They are also responsible for control and monitoring of available storage levels.

Customer Administration

Customer Administration is responsible for Active Directory content related but not limited to accounts, groups, organizational units (OU), folders, printers, and PCs. This group performs approved Active Directory access and rights management services for user agencies.

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)

S&CS is responsible for:

- 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 IT 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.
- Developing and maintaining the statewide disaster recovery services for the State's Information Technology infrastructure.

Enterprise Applications and Architecture

The Enterprise Business Applications and Services 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.

Customer Service Center (CSC)
The CSC serves as the central point of contact for IT and telecommunications users. The CSC processes and manages IT, telecommunications and networking service requests and incidents, procures and manages IT and telecommunications technologies, and manages IT/telecommunications vendor performance.

Communications Management Center (CMC)
The CMC is responsible for all Wide Area Network (WAN) trouble resolutions, surveillance, and ongoing technical support. The CMC is operational 24x7, and handles after hours calls of the Customer Service Center and IT Service Desk.

Network Services
Network Services is responsible for management and oversight of the Illinois Century Network (ICN) and all design and engineering responsibilities related to State of Illinois telecommunications services as well as Tier 3/4 support for data/WAN issues.

Network Operations is responsible for installing, maintaining and managing the ICN Backbone, including the State's owned and leased fiber optic infrastructure and DWDM optical equipment, as well as the MPLS network, including the routers, firewalls, switches, WAN monitoring tools and data/WAN and Lite Services. Network Operations is also responsible for Point-of-Presence (POP) Sites, and In Line Amplification (ILA) Sites.

People

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) in order to request to fill a vacancy. Once the PAR is approved by the Department's Chief Financial Officer and the Department's Director, Administrative and Regulatory Shared Services Center will begin the hiring process by posting the vacant position. Upon employment, the Administrative and Regulatory Shared Services Center provides new employee orientation. During orientation, new employees complete various forms and training.

Personnel work with the section managers to develop position descriptions. Each position is to have a position description which outlines the duties and qualifications.

Upon separation from the Department, Personnel completes a PAR, which notifies the Department's Chief Fiscal Officer of the departure. In addition, Personnel sends the individual'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 individuals for training, and tracks all training in a database.

New Department staff are 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.

Information and Communication

The Department understands the value of maintaining communications with internal staff and external customers. Information is shared through various means, including the bccs.illinois.gov website for customer notifications, service catalog listings, policy publications, etc. The bccs.portal.illinois.gov is a website that is maintained for internal information distribution. The Department conducts staff meetings, CIO council meetings, and various working groups where staff from agencies participate, collaborate and work towards solutions together.

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

- Identity Protection Policy;
- 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; and
- Statewide CMS/BCCS Facility Access 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.

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

A formalized Risk Assessment program has not been fully implemented; however, the Department has completed some risk assessment work on the following projects:

- Neon interface to mainframe applications;
- Encryption of data in transit;
- PCI-DSS assessments for agencies that process credit cards; and
- Printer configuration changes as a result of vulnerability scans.

Additionally, on August 16, 2015, a dedicated Chief Information Security Officer (CISO) was appointed with responsibilities for all state agencies under the Executive Branch.

The development of a comprehensive Risk Management Framework is in progress, along with the establishment of a common cybersecurity framework as the standard for the State.

On January 6, 2016, a comprehensive cybersecurity strategy was adopted with sponsorship and ongoing support from the Governor.

In April 2016, the Department contracted with a third party to conduct a NIST Cybersecurity Maturity Assessment which identified baseline maturity levels for the State's security operations in areas of the NIST Cybersecurity Framework. In May 2016, a project was initiated to build a risk assessment program for the State based upon the NIST Cybersecurity Framework.

Projects and initiatives are in progress to improve the information and cyber security posture of the State’s Risk Management program. Key areas include identification activities to augment risk assessment, application rationalization, and data classification.

Three additional security staff have been assigned and requested to perform risk management activities and continue to mature the program. Intergovernmental Agreements were signed with the following agencies:

- Illinois Department of Healthcare and Family Services - May 9, 2016; and
- Office of the Illinois State Fire Marshal – April 29, 2016.

These agencies are providing personnel resources to assist in the development of specific security programs, which align with the needs of the agencies.

In January 2016, the Department initiated a project in which user agencies were to inventory systems which contained Personally Identifiable Information and a plan to secure the information. The information was to be provided to the Department by February 29, 2016. Completion of the project is targeted for October 2016.

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, any open items are passed on to the next shift, and to identify any changes which need to be made. The Checklists are reviewed by the Operations Center supervisor.

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

Staff and users may contact the Help Desk via phone, email or the Bureau’s website 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. In addition, EUC and the S&CS group are notified via email. EUC should determine if the equipment had encryption installed and if confidential information was retained on the equipment.

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. The Department did not encounter any breaches; therefore, the control related to breaches did not operate during the period covered by the Report.

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 staff including system programmers and security software staff.

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 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' security software IDs, creation, modification, revocation, and monitoring.

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

The 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 a security software ID for agencies in which the Department is the security software administrator, 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 security software ID, the Compliance 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 security software ID and temporary password. The password being temporary requires the individual to change it upon initial login.

In the event a security software ID needs to be modified, an email or ESR is to be submitted. The necessary modifications are made and the requestor is phoned indicating such action has taken place.

In the event a user requires their security software password to be reset, the user contacts the Help Desk via email, submits a problem report or utilizes the Department's Identity Management (BIM) Solution.

In the event the user does not utilize the Department's BIM to reset their security software password, the user is required to email or submit a problem report via the Department's website to the Help Desk requesting a password reset. The request is to include the user's name, security software ID, and a phone number to be contacted. The Help Desk staff will contact the user at the number given, reset the security software password and call the individual with the new password. In the event the individual is unable to be reached, a message is left instructing the individual to contact the Help Desk.

If the Help Desk staff is unable to reset the security software password, the help desk ticket will be assigned to the Security Software Coordinator or the Security Software Administrator for CMS/BCCS/S&CS in order to reset the security software password. Upon receipt, the Security Software Coordinator or the Security Software Administrator for CMS/BCCS/S&CS will reset the security software password with a temporary password and phone the individual.

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

On an annual basis, 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, Regional Technology Offices, and Enterprise Network Support are primarily responsible for networking equipment at the core, distribution, and access levels, while Local Area Network (LAN) Services is primarily responsible for networking equipment at the Data Centers and LAN infrastructure at supported agencies.

Network Topology diagrams are maintained by Network Services depicting the network infrastructure and placement of firewalls, routers and switches. Specific network diagrams for all network infrastructure are not maintained due to the redundancy of network design across multiple agencies.

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

Authentication servers are utilized to provide authorized access to the firewalls, routers, and switches maintained by Network Services. Network Operations and Enterprise Network Support utilize two authentication servers. LAN Services utilizes two authentication servers, which are independent of the ones utilized by Network Operations and Enterprise Network Support. Multi-Factor Authentication is also utilized for administrative access to network devices.

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.

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, two external logging servers.

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

The Advance Computer Solutions server used by Network Services generates alerts for repeated failed access authorization attempts to networking devices from the same IP addresses. Once a repeated number (based on a predefined number) of failed access attempts occurred, the administrators are notified.

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

Network Operations and Enterprise Network Support maintain a SolarWinds server and software (Network Performance Manager (NPM) and Network Configuration Manager (NCM)) for the devices they manage and maintain. LAN Services maintains two additional SolarWinds NCM and NPM servers and software for the devices they manage and maintain. One system contains Data Center LAN devices and the other System contains LAN devices at remote agency locations that are supported by the Department.

SolarWinds NPM is utilized to monitor performance related issues such as up/down devices, bandwidth utilization, CPU utilization, etc. and alert administrators as necessary. Most Network Services devices are connected to NPM.

In the event a breach is identified, Network Services utilizes the Data Breach Notification Policy and the Action Plan for Notification of a Security Breach which are posted on the Department's website. In addition, a Remedy ticket is opened and if necessary the Technical Safeguards team is alerted.

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; however, templates to address Network Operation's and Enterprise Network Support's other routers and firewalls are not maintained. LAN Services maintains the CMS/BCCS LAN Services Standards for Hardware Configuration and Deployment to assist in configuring network devices maintained for supported agencies.

SolarWinds NCM is utilized for configuration backups, and making configuration changes to multiple devices at a time. Additionally, NCM is capable of sending alerts to administrators as deemed appropriate. Most Network Services devices are connected to NCM.

Periodic reviews of configurations are performed by Network Services staff; however, documentation of these reviews is not maintained.

LAN Services also places reliance on vulnerability assessment work performed by the Technical Safeguards Unit. As the Technical Safeguards Unit performs assessments for the various agencies supported by the Department, they identify weaknesses such as open ports, open Simple Network Management Protocol (SNMP) strings, weak passwords, etc. Once notified by Technical Safeguards, LAN Services then takes action as necessary.

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 via two independent processes.

The first method of backing-up device configurations is a backup server maintained by Network Operations and Enterprise Network Support. The server utilizes an automated process to routinely retrieve configurations from devices. Files are then stored on the server for the Department's Enterprise Storage and Backup team to backup and rotate off-site according to their defined methods and procedures.

The second method of backing-up device configurations utilizes SolarWinds NCM. SolarWinds NCM is configured to routinely backup configurations for all firewalls, routers, and switches managed and maintained by Network Operations and Enterprise Network Support. NCM pulls the device configurations and places them on a database server. Once configurations are backed-up, NCM emails reports to administrators notifying them of the devices that are both successfully and unsuccessfully backed-up during the cycle.

LAN Services' firewall, router, and switch configurations are backed-up via SolarWinds NCM. SolarWinds NCM is configured to routinely backup configurations for most firewall, routers, and switches managed and maintained by LAN Services. NCM pulls the device configurations and places them on a database server for the Department's Enterprise Storage and Backup team to backup and rotate off-site according to their defined methods and procedures. Once configurations are backed-up, NCM emails reports to administrators notifying them of the devices that are both successfully and unsuccessfully backed-up during the cycle. Some systems such as IPS, F5 Firewall, and Infoblox DNS/DHCP appliances are not backed up by NCM as they have built in configuration backup capabilities or other backup processes are used.

To ensure continuous availability of the network, the Department has configured select components of 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 ICN 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 or sparing. 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.

Failed equipment, which is covered by the agreements, is called into Cisco for replacement via their Return Material Authorization (RMA) process. Cisco will then ship the replacement part to the location specified in the RMA. The failed part must then be returned to Cisco within a particular timeframe after receipt of the new/replacement part.

Equipment not covered by the SMARTnet agreement is typically covered by sparing. Spared equipment for WAN is typically kept at the Regional Technology Center (RTC) locations. Sparing equipment for LAN is typically kept at two Springfield centralized locations. Spared equipment that is too large (chassis, etc.) or too costly are typically kept at a central location.

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, is utilized by the VPN solution.

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

Network Services (specifically Enterprise Network Support) does offer a solution which encrypts an agency's data while it is in transit across the public ICN 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 ICN network. Traffic is encrypted at the agency's access router level and decrypted at the agency head-end router level. Presently, only Secretary of State, Illinois Gaming Board, and the Department of Revenue utilize the service.

The Department's Data Classification and Protection Policy documents the data classification schemas used to value and classify information generated, accessed, transmitted or stored. 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 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.

The managed enterprise computing equipment is running Windows XP, Windows 7, and Windows 8. 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 Department utilizes Microsoft's System Center Configuration Manager to push and monitor Windows patches.

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.

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 rights may disable the encryption software. However, EUC checks BitLocker against the Active Directory to determine if it is active. If encryption is not active, the user will be unable to access the network.

In order to access the Department's environment, the user is required to have an Active Directory user ID and password. To obtain an Active Directory ID, the agencies' IT Coordinator submits a completed and approved ESR indicating the access required.

In the event an Active Directory ID needs to be modified, an email or ESR is received indicating the necessary modifications which need to be made.

In the event a user requires their Active Directory password to be reset, the user contacts the Help Desk via email, submits a problem report or utilizes one of the Department's two Self-Service Solutions: BCCS Identity Management (BIM) Solution or the Forefront Identity Manager (FIM) Solution.

When an individual terminates or no longer requires access, an Exit Form is received by the Help Desk and the Active Directory ID is deactivated.

The Department utilizes the CCF and the Communications 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 notifies 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, the Exit Form is sent to the individual's supervisor to ensure the collection of equipment and termination of access. Once the Physical Security Coordinator is notified, the individual's access rights are deactivated.

Visitors, along with contractors and staff 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, and
- The uninterrupted power supply (UPS) at the facilities includes a battery farm and diesel turbine generators.

Department staff monitors the environmental factors and notifies 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.

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

The Department of Revenue's 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.

Each agency is responsible for the scheduling of their respective print jobs.

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

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.

On April 7, 2016, the Department updated the impact criteria to include a risk classification. 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 affect 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.

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 changes that cause an outage or is an emergency change. The review is conducted by the change supervisor or an Enterprise Change Management Team member.

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

Changes to applications determined to be routine or minor are to be managed via Remedy and follow the EAA Change Management Procedures. Changes that alter the design basis are managed via the EPM Portal and the Application Life Cycle Management Methodology.

The Library Services Group is responsible for moving mainframe application changes into production for Department of Human Services (DHS), Department of Central Management Services (DCMS), Department of Healthcare and Family Services (DHFS), and Department of Transportation (DOT). 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 Department of Public Health (DPH), the agencies submit an email from an authorized staff to Library Services indicating the date, time and libraries to be moved.

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.

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, with the mainframe security software controlling who has access to schedule a move.

Backup and Restoration

The Department utilizes Virtual Tape Technology (Disk Library Management (DLM)) between the CCF and the Alternate Data Center (ADC). This solution provides replication between two DLMs 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 Mainframe Storage team uses CA-Scheduler to control and schedule backups. Systems are backed up on a routine daily and weekly basis. Once scheduled, the backups run automatically utilizing a utility within CA-Scheduler to perform the backup dumps. User agencies are responsible for backing up, scheduling and the number of copies of online databases.

The Department maintains and reviews the CA-Scheduler Verify Backups document, which is used to assist with the verification that backups are successful. The Storage staff is notified of any failed backups.

- For severe problems the staff are notified by a phone call.
- When backup jobs continue, and a problem is discovered during a daily review, the failed backup jobs are scheduled on the following first business day.
- Many of the minor backup issues occur with reading individual datasets due to problems with the dataset that only the agency / programmer can solve.

The Department did not encounter any failed backups; therefore, these controls did not operate during the period covered by the Report.

Additionally, replication is to occur every 10 minutes between the CCF and ADC DLM. The monitoring software sends the software and staff an alert if the data is out of sync for more than 8 hours. The error is usually due to timing of the replication; however, if there is a true issue a Remedy Ticket would be opened. The software vendor and the staff hold weekly meetings to discuss any “issues” which have occurred the week prior. The vendor project manager maintains weekly notes and distributes the plan to the team.

The DLM Replicated Status log keeps a log of replications for the DLM between the CCF and the ADC. The logs tracks library replication outcomes for DLM replicated activity. The DLM Replicated Status logs documents the status of the replicated libraries, and the time of the last sync. The logs are maintained for 7 days. In the event an agency requires a restore, the requests are made via a Remedy Ticket.

The system automation tool controls and monitors available storage levels. The system automation tool notifies or alerts staff through email, when storage falls below the pre-determined threshold. The objective is to keep the availability threshold at 10%. Once the threshold reaches 5% availability, action is taken to identify and remove information that appears to be no longer needed. Also, staff monitors Private Pool storage resources and will notify the agency once the threshold has reached 5%, so that necessary action can be taken to free up space. In some situations the agency can request the threshold to be lowered or raised depending on the amount of space needed for the agency data. The agencies may request to have unwanted data removed in order to increase availability of space. A Remedy Ticket is created if an agency requires additional storage.

In order to gain access to storage and backup data, an authorized ESR is submitted indicating the applicable access. Only authorized staff are to have access to storage and backup data.

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, explain the problem, and request the agency to rectify the problem, if applicable. The Department did not encounter any failed backups; therefore, the control did not operate during the period covered by the Report.

Although agencies are responsible for the scheduling of backups, via CA-Scheduler, Library Services monitors the backup process for DHS, DCMS, DHFS, and DOT to ensure the process completed; however, they are not responsible for the accuracy of the backups. 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.

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 space at an alternate data center. The Department has installed equipment at the alternate data center in order to categorize it as a “cold and warm site”.

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

The Department has 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 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 to the extent possible without disrupting production services. 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 agencies 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, which include access, approve transactions, modify and delete transactions.

Access to eTime is controlled through the user's Active Directory account. The employee's access is based on their duties, which include 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.

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 'System' 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 communicated to the Department's Help Desk any lost or stolen equipment.
- 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 within the Business Reference Model;
- User agencies have submitted to the Department an authorized ESR requesting agencies' users access to applicable resources;
- User agencies utilize the Identity Management Solution to reset their passwords or contact the Help Desk.
- User agencies have reviewed, updated, approved, and returned to the Department on a annual basis their security listings;
- User agencies have submitted an authorized ESR for the installation/removal of equipment;
- User agencies have reviewed and approved individuals with access to the agencies production libraries and data.
- Agencies have scheduled and reviewed their backups of applications and data.
- Agencies have submitted to the Department their continuous service goals and outcomes of their testing.
- 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, recovery exercise procedures and schedules, and ongoing communications with the Department.

BOUNDARIES OF THE SYSTEM

The Department of Central Management Services provides 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 vendor's 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, and Processing Integrity Criteria, 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.

TESTS OF OPERATING EFFECTIVENESS

Our tests of the operating effectiveness of controls were designed to cover a representative number of processes throughout the period of July 1, 2015 through June 30, 2016, for each of the controls, which are designed to achieve the applicable trust services criteria. In selecting particular tests of the operating effectiveness of controls, we considered (a) the nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the applicable trust services criteria to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

The basis for all tests of operating effectiveness included inquiry of the individual(s) responsible for the control. As part of our testing of each control we inquired of the individual(s) to determine the fairness of the description of the controls and to evaluate the design and implementation of the control. As part of inquiries, the auditor also gained an understanding of the knowledge and experience of the personnel managing the control(s) and corroborated evidence obtained as part of other testing procedures. While inquiries were performed for every control, this test was not listed individually for every control activity shown in the matrices in Description of Test of Controls and Results Thereof.

The additional testing methods described below were used to test operating effectiveness.

Type	Description
Interviewed	Inquiry of appropriate personnel.
Observation	Observed the application or existence of the specific control(s) as represented by management.
Inspection/Reviewed	Inspected/Reviewed documents and records indicating performance of the control. This includes examples such as: • Inspection of audit evidence that demonstrate the performance of the control. • Inspection of systems documentation, for example operations manuals, flow charts and job descriptions. • Reading of documents such as policies and meeting minutes to determine appropriate information is included.
Reperformance	Reperformed the control or processing application to ensure the accuracy of its operation. This includes processing test transactions through application programs in a test environment to ensure edits are properly functioning.

DESCRIPTION OF TESTS OF CONTROLS AND RESULTS THEREOF

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

	Criteria	Department’s Control	Testing Performed	Results
CC1.1	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 has a position description which outlines the duties and qualifications.	Reviewed a selection of positions to determine if a position description had been completed.	No deviation noted.
			Reviewed the position descriptions to determine if they outlined the duties and qualifications.	No deviation noted.
		The Department is organized within functional areas and organizational and report hierarchies have been established.	Reviewed Organizational Chart to determine if functional areas and reporting hierarchies had been established.	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 with the Department’s authority to ensure policies and other system requirements are effectively promulgated and placed in operation.	Each position has a position description which outlines the duties and qualifications.	Reviewed a selection of positions to determine if a position description had been completed.	No deviation noted.

TRUST SERVICES - CRITERIA, 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 position descriptions to determine if they outlined the duties and qualifications.	No deviation noted.
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 to determine the hiring process.	No deviation noted.
			Reviewed a selection of new hires to determine if they were filled in accordance with the hiring procedures.	No deviation noted.
		Personnel initiates a Personal Acton Request in order to fill the vacancy. The Department’s Director and the Chief Fiscal Officer approve the Personal Action Request.	Reviewed a selection of new hires to determine if the Personal Action Request was properly completed and approved.	No deviation noted.
		Upon employment, the Administrative and Regulatory Shared Services Center provides new employee orientation. During orientation, new employees are provided training.	Reviewed the training to determine the training provided to new employees.	No deviation noted.
			Reviewed a selection of new employees to determine if they had been provided training.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		The Department's training office works with managers to identify training needs, registers employees for training, and tracks training.	Reviewed the training report to determine if employees had received training.	No deviation noted.
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 and contractors are communicated via the mandatory annual security awareness training.	Reviewed a selection of employees and contractors to determine if they had completed the Security Awareness Training.	1 employee and 1 contractor of 80 employees/ contractors selected had not completed security awareness training.
		New Department staff are required to sign a statement signifying that they will comply with the security policies.	Reviewed the security awareness training report and signed compliance statements to determine if new Department staff signified compliance with security policies.	No deviation noted.
			Reviewed a selection of new employees to determine if they had completed the Security Awareness Training.	No deviation noted.
		Department staff reconfirm their compliance with the security policies through the annual security training.	Reviewed the security awareness training report and signed compliance statements to determine if staff reconfirmed their compliance with security policies.	No deviation noted.
			Reviewed a selection of employees to determine if they had completed the Security Awareness Training.	1 of 40 employees selected had not completed security awareness training.

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

	Criteria	Department's Control	Testing Performed	Results
		Contractors confirm their compliance with security policies through security training.	Reviewed the security awareness training report and signed compliance statements to determine if contractors confirmed their compliance with security policies.	No deviation noted.
			Reviewed a selection of contractors to determine if they had completed the Security Awareness Training.	1 of 40 contractors selected had not completed security awareness training.
		New employees and contractors are required to have background checks.	Reviewed a selection of new employees and contractors to determine if a background check had been completed.	No deviation noted.
		The Department's Compliance Officer is assigned responsibility for monitoring and ensuring compliance with policies and procedures.	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 during the period covered by the report.

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

	Criteria	Department's Control	Testing Performed	Results
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system 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 which agencies may utilize in determining their required services.	Reviewed the Service Catalog to determine if the services and/or products offered were communicated to the user agencies.	No deviation noted.
CC2.2	The Department's security, availability, and processing integrity commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.	New Department staff are required to sign a statement signifying that they will comply with the security policies.	Reviewed the security awareness training report and signed compliance statements to determine if new Department staff signified compliance with security policies.	No deviation noted.
			Reviewed a selection of new employees to determine if they had completed the Security Awareness Training.	No deviation noted.
		Department staff reconfirm their compliance with the security policies through the annual security training.	Reviewed the security awareness training report and signed compliance statements to determine if staff reconfirmed their compliance with security policies.	No deviation noted.
			Reviewed a selection of employees to determine if they had completed the Security Awareness Training.	1 of 40 employees selected had not completed security awareness training.

	Criteria	Department's Control	Testing Performed	Results
		Contractors confirm their compliance with security policies through security training.	Reviewed the security awareness training report and signed compliance statements to determine if contract confirmed their compliance with security policies.	No deviation noted.
			Reviewed a selection of contractors to determine if they had completed the Security Awareness Training.	1 of 40 contractors selected had not completed security awareness training.
		The Department has published on their website the Service Catalog which agencies may utilize in determining their required services.	Reviewed the Service Catalog to determine if the services and/or products offered were communicated to the user agencies.	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 rights (documentation, tracking, approvals), -periodic review of access rights, -revocation of access rights, and -the actions supervisors were to take when notified

	Criteria	Department’s Control	Testing Performed	Results
				of security issues, and -procedures related to the administration of mainframe security software did not address the proper authorization of Mainframe Security Request Forms.
CC2.3	The Department communicates the responsibilities of internal and external users and others whose roles affect system operations.	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 rights (documentation, tracking, approvals), -periodic review of access rights, -revocation of access rights, and -the actions supervisors were to take when notified of security issues, and -procedures related to the administration of mainframe

	Criteria	Department's Control	Testing Performed	Results
				security software did not address the proper authorization of Mainframe Security Request Forms.
		New Department staff are required to sign a statement signifying that they will comply with the security policies.	Reviewed the security awareness training report and signed compliance statements to determine if new Department staff signified compliance with security policies.	No deviation noted.
			Reviewed a selection of new employees to determine if they had completed the Security Awareness Training.	No deviation noted.
		Department staff reconfirm their compliance with the security policies through the annual security training.	Reviewed the security awareness training report and signed compliance statements to determine if staff reconfirmed their compliance with security policies	No deviation noted.
			Reviewed a selection of employees to determine if they had completed the Security Awareness Training.	1 of 40 employees selected had not completed security awareness training.
		Contractors confirm their compliance with security policies through security training.	Reviewed the security awareness training report and signed compliance statements to determine if contractors confirmed their compliance with security policies.	No deviation noted.

TRUST SERVICES - CRITERIA, 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 a selection of contractors to determine if they had completed the Security Awareness Training.	1 of 40 contractors selected had not completed security awareness training.
CC2.4	Internal and external personnel with responsibilities for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, availability, 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, approvals), -periodic review of access rights, -revocation of access rights, -the actions supervisors were to take when notified of security issues, and -procedures related to the administration of mainframe security software did not address the proper authorization of Mainframe Security Request Forms.

	Criteria	Department's Control	Testing Performed	Results
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 website to determine if 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.
		The Enterprise Desktop/Laptop Policy, the Mobile Device Security Policy, and the Missing IT Equipment Procedures provided guidance to users for the reporting of lost or stolen assets.	Reviewed policies and procedures to determine if they provided adequate guidance for reporting lost or stolen assets.	The Missing IT Equipment Procedure did not address the process in the event encryption was not installed on missing equipment.
		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 selection of lost/stolen devices to determine if a Remedy Ticket had been created and a police report was attached to the Remedy 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.	Reviewed a selection of lost/stolen devices to determine if EUC had conducted an analysis to determine if encryption was installed.	2 of 5 lost/stolen laptops selected did not have an analysis completed to determine if encryption had been installed.
		The user manuals for applications provide instructions for users to contact the Help Desk to report issues.	Reviewed user manuals to determine if they provided instruction to report issues to the Help Desk.	No deviation noted.
		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 (MORT) Process to determine the process for identification and escalation of security breaches.	No deviation noted.
			Reviewed a selection of security issues to determine compliance with procedures.	1 of 3 MORTs selected did not have the required escalation notification. 2 of 3 MORTs selected did not have the required email attached to the Remedy ticket.

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

	Criteria	Department’s Control	Testing Performed	Results
CC2.6	System changes that affect internal and external user responsibilities or the Department’s commitments and requirements relevant to security, availability, and processing integrity are communicated to those users in a timely manner.	Infrastructure changes are communicated to users and management via the Change Advisory Committee (CAC) meetings and the meeting minutes are posted on the ECM SharePoint site.	Reviewed SharePoint site to determine if CAC meeting minutes were posted.	No deviation noted.
			Reviewed a selection of changes (RFCs) to determine if those required to be posted were included in the CAC meeting minutes posted on the SharePoint site.	2 of 60 changes (RFCs) selected were not included in the CAC meeting minutes.
		Emergency changes are communicated to users post implementation via the CAC meeting.	Reviewed a selection of emergency changes to determine if they were included in the CAC meeting minutes posted on the SharePoint site.	No deviation noted.
		Agencies have access to the ECM SharePoint site.	Reviewed access to determine if agencies had access to the Sharepoint site.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
CC3.1	The Department (1) identifies potential threats that could 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 had not implemented controls to identify, analyze, and mitigate potential threats.	The Department had not implemented controls to identify, analyze, and mitigate potential threats.	Based on an interview with staff, the Department had not implemented controls to identify, analyze, and mitigate potential threats. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
CC3.2	The Department designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.	The Department had not implemented controls related to the assessment and mitigation of risk.	The Department had not implemented controls related to the assessment and mitigation of risk.	Based on an interview with staff, the Department had not implemented controls related to risk mitigation strategies. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
		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 Plan and testing documentation to determine if the Plan had been tested.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
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 had not implemented controls related to the assessment and mitigation of risk.	The Department had not implemented controls related to the assessment and mitigation of risk.	Based on an interview with staff, the Department had not implemented controls related to the assessment and mitigation of risk. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
CC4.1	The design and operating effectiveness of controls are periodically evaluated against security, availability, 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 is continuously monitored.	No deviation noted.
		Problems, issues, and incidents are recorded via the Daily Shift Report and a Remedy Ticket is created.	Reviewed a selection of Daily Shift Reports to determine if problems, issues, and incidents were reported.	No deviation noted.
		For any incident the Operations Center cannot resolve, the Remedy ticket is assigned to the applicable division for resolution.	Reviewed a selection of Daily Shift Reports to determine if a Remedy ticket had been created and assigned for resolution.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		The Daily Shift Report documents the activity conducted on all mainframe production systems and incident calls received at the Operations Center.	Review a selection of Daily Shift Reports to determine if the activity on production systems was recorded and incident calls were recorded.	No deviation noted.
		The Operator Shift Change Checklist is completed at the beginning of each shift to ensure the production systems are operating appropriately, that 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 selection of Operator Shift Change Checklists to determine if they were completed and reviewed.	No deviation noted.
		In the event division staff or management needs to be notified, contact information is maintained with the FOCAL database.	Observed the FOCAL database to determine management contact information was maintained.	No deviation noted.
		The Department has developed the Data Processing Guide in order to provide staff with instructions related to their various tasks.	Reviewed the Data Processing Guide to determine the instructions provided.	No deviation noted.
		System performance is monitored via software tools.	Reviewed a selection of software tool reports to determine if system performance was monitored.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		Performance monitoring is documented via internal memorandum distributed to management.	Reviewed a selection of memorandums to management regarding system performance and capacity to determine if issues were documented.	No deviation noted.
		Remote Monitoring Facility (RMF) reports are run weekly and monthly.	Reviewed a selection of RMF reports to determine the frequency.	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 Unit will be alerted.	Reviewed the Data Breach Notification Policy and the Action Plan for Notification of a Security Breach to determine the process for notification in the event of a security breach.	No deviation noted.
			The Department did not encounter any breaches during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not encounter any breaches during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

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

	Criteria	Department’s Control	Testing Performed	Results
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of 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.	In order to access the Department’s environment, the user must be assigned an Active Directory (AD) ID and password.	Observed that an Active Directory ID and password was required to access the Department’s environment.	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 mainframe security software.	No deviation noted.
		The mainframe security software requires users to have an established ID and password in order to verify the individual’s identity.	Reviewed system options and password requirements memo to determine password standards.	No deviation noted.
			Observed a user sign-on to determine if a security software ID and password were required to verify identity.	No deviation noted.
		Passwords are maintained in an encrypted database.	Determined if passwords were maintained in an encrypted database.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		In order to access an application, a user must have a separate application ID and password in order to gain access.	Observed users log into applications to determine if a separate ID and password to gain access was required.	No deviation noted.
		Logical mainframe security controls are in place to restrict access to operating system configurations.	Reviewed security reports to determine if logical security controls were in place.	No deviation noted.
			Reviewed security software profiles for primary systems programming groups and support staff to determine if access to system resources was adequate.	2 of 9 system groups did not have appropriate access. 1 of 18 system programmers no longer required access. 2 of 27 administrative users no longer required access.
			Reviewed security software options to determine if established security parameters were adequate.	No deviation noted.
			Reviewed access to system level libraries to determine if access was appropriately restricted.	No deviation noted.

TRUST SERVICES - CRITERIA, 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 access rights to sensitive system functions and authorizations to determine if access was appropriately restricted to system programming personnel.	1 of 18 system programmers no longer required access. 2 of 27 administrative users no longer required access.
			Reviewed a selection of security software IDs exempt from having a change interval to determine reasonableness.	No deviation noted.
		Mainframe operating systems have been configured to promote security.	Reviewed security reports to determine if mainframe operating systems were configured.	No deviation noted.
			Reviewed operator commands to determine if access was restricted.	No deviation noted.
			Reviewed physical and logical controls over operator consoles to determine security controls.	No deviation noted.
			Reviewed supervisory calls to determine if access was restricted.	No deviation noted.
			Reviewed access to SMF records to determine if access was restricted.	No deviation noted.
			Reviewed exits to determine if access was restricted.	No deviation noted.
			Reviewed subsystems to determine if access was restricted.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
			Reviewed DB2 agency listings, job installation streams, and system coupling to determine if access was restricted.	No deviation noted.
			Reviewed intruder alerts to determine if management maintained reports for investigating access violations.	No deviation noted.
		Weekly mainframe security software violation reports are reviewed for invalid and unauthorized access attempts. Violations are investigated.	Reviewed a selection of weekly violation reports to determine if violations were investigated.	No deviation noted.
		The Department has restricted mainframe access with powerful privileges, high-level access, and access to sensitive system functions to authorized staff.	Reviewed security software reports to determine if powerful, high-level access to sensitive system functions were limited to authorized staff.	No deviation noted.
		Network Services maintains an Enterprise Virtual Private Network (VPN) solution utilized by the Department and other state agencies to allow for a secure remote connection into resources managed and maintained by the Department.	Reviewed VPN configurations to determine if the security settings were configured to allow for a secure remote connection into resources managed and maintained by the Department.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		Firewalls, routers, and switches 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 selection of configuration files to determine if firewalls, routers, and switches were configured to utilize authentication servers, logging servers, banners warning prohibiting unauthorized access and warning of prosecution and ACLs to deny and permit specific traffic.	1 of 60 devices selected did not have a banner placed in the configuration file.
		Access to storage and backup data is limited to authorized staff.	Reviewed a selection of staff with access to storage and backup data to determine if limited to appropriate staff.	No deviation noted.
		Authorized staff has access to specific security software groups which allows them to reset security software passwords.	Reviewed a selection of authorized staff to determine if their access rights were appropriate.	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.	In order to obtain an AD ID to access the Department's environment, the agency is to submit an authorized Enterprise Service Request (ESR) indicating the required access.	Reviewed a selection of staff to determine if an authorized ESR indicating required access was submitted.	1 of 23staff's ESR selected did not have the approval date completed.
		In order to obtain a mainframe security software ID, users are required to submit an approved Mainframe Application Access Request Form or an ESR.	Reviewed a selection of new requests to determine if a Mainframe Application Access Request Form or an ESR had been submitted.	No deviation noted.

	Criteria	Department’s Control	Testing Performed	Results
		In the event an AD ID needs to be modified, an email or an ESR is to be received indicating the necessary modifications.	The Department was unable to provide a universe of AD ID modifications. Therefore, the Service Auditor did not test the operating effectiveness of the control.	The Department was unable to provide a universe of AD ID modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
		In the event a mainframe security software ID needs to be modified, users are required to submit an approved Mainframe Application Access Request Form or an Enterprise Service Request.	The Department was unable to provide a universe of mainframe ID modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department was unable to provide a universe of mainframe ID modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
		The user may utilize one of the two Self-Service Solutions, BCCS Identity Management Solution or the Forefront Identity Manager Solution, to reset their passwords.	Reviewed the Department’s Identity Management Website to determine solutions to reset passwords.	No deviation noted.

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

	Criteria	Department’s Control	Testing Performed	Results
		If the user does not utilize the Self-Service Solutions to reset their mainframe security software ID reset, they are to send an email to the Help Desk requesting such.	Reviewed a selection of mainframe security software password resets to determine if an email had been received.	17 of 60 mainframe security software password resets selected did not have an email request submitted.
		If the user does not utilize the Self-Service Solutions to reset their AD password, the user is required to submit an email or problem report to the Help Desk requesting their password be reset.	Requested from Help Desk staff email and problem reports.	The Department did not follow the requirements of an email or problem report to be submitted for Active Directory password resets.
		Non-expiring mainframe security software ID are required to complete a Request for Non-Expiring RACF ID Form and be approved by the Compliance Manager.	Reviewed a selection of non-expiring mainframe security software IDs to determine if the Form was completed and approved by the Compliance Manager.	No deviation noted.
		The Exit Form is sent to the employee’s supervisor indicating the items to be retrieved and the deactivation of access.	Reviewed a selection of separations to determine if their access had been deactivated in a timely manner.	5 of 12 separated individuals selected did not have their access deactivated in a timely manner.

TRUST SERVICES - CRITERIA, 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 separation from the Department, Personnel complete a PAR, which notifies the Department’s CFO of the departure. Personnel also send the employee’s supervisor an Exit Form which outlines the items to be retrieved and deactivation of access.	Reviewed a selection of separations to determine if a PAR and Exit Form had been completed.	No deviation noted for employees. The Department had not implemented a formal exit process for contractor separations.
		Bi-monthly a report is run documenting separations from the Department and proxy agencies. The report is reviewed to ensure the applicable security software IDs are revoked.	Reviewed a selection of reports to determine if the reports had been reviewed and if security software IDs were revoked.	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).	In order to access the Department’s environment, the user must be assigned an AD ID and password.	Observed a user to determine if an AD ID and password were required to access the Department’s environment.	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 users log into applications to determine if a separate ID and password to gain access were required.	No deviation noted.
		Mainframe software password standards have been established.	Reviewed system options to determine if password standards had been established.	No deviation noted.

TRUST SERVICES - CRITERIA, 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 a mainframe security software ID and password were required to verify identity.	No deviation noted.
			Observed that user profile included a name field.	No deviation noted.
			Reviewed system options report and password requirements memo to determine password standards had been established and communicated.	No deviation noted.
		The Department maintained a VPN solution to connect remotely into resources managed and maintained by the Department.	Reviewed the VPN configurations to determine if the security settings were configured to allow for a secure remote connection into resources 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 to determine if users establish their identity and authentication to systems and applications.	No deviation noted.
			Observed a user to determine if they were assigned a user ID and password.	No deviation noted.
			Reviewed a selection of user accounts with powerful access rights to determine if rights were appropriate.	No deviation noted.

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

	Criteria	Department’s Control	Testing Performed	Results
		Authentication servers utilize an administrative architecture in which groups are established with specific levels of administrative privileges for individual’s needs.	Reviewed a selection of groups to determine if the privileges were appropriate.	No deviation noted.
		Password parameters have been established on authentication servers.	Reviewed the network password parameters to determine if the password strength, duration and history were appropriately configured.	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 selection of configuration files to determine if firewalls, routers, and switches were configured to utilize authentication servers, logging servers, banners warning prohibiting unauthorized access and warning of prosecution and ACLs to deny and permit specific traffic.	1 of 60 devices selected did not have a banner placed in the configuration file.
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.	In order to obtain an AD ID to access the Department’s environment, the agency is to submit an authorized ESR indicating the required access.	Reviewed a selection of staff to determine if an authorized ESR indicating required access was submitted.	1 of 23 staff’s ESR selected did not have the approval date completed.

	Criteria	Department's Control	Testing Performed	Results
		In order to obtain a mainframe security software ID, users are required to submit an approved Mainframe Application Access Request Form or an Enterprise Service Request.	Reviewed a selection of new requests to determine if a Mainframe Application Access Request Form or an ESR had been submitted.	No deviation noted.
		In the event a mainframe security software ID needs to be modified, users are required to submit an approved Mainframe Application Access Request Form or an Enterprise Service Request.	The Department was unable to provide a universe of mainframe ID modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department was unable to provide a universe of mainframe ID modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
		In the event an AD ID needs to be modified, an email or an ESR is to be received indicating the necessary modifications.	The Department was unable to provide a universe of AD ID modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department was unable to provide a universe of AD ID modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

	Criteria	Department's Control	Testing Performed	Results
		The user may utilize one of the two Self-Service Solutions, BCCS Identity Management Solution or the Forefront Identity Manager Solution, to reset their passwords.	Reviewed the Department's Identity Management Website to determine solutions to reset passwords.	No deviation noted.
		If the user does not utilize the Self-Service Solutions to reset their mainframe security software ID reset, they are to send an email to the Help Desk requesting such.	Reviewed a selection of mainframe security software password resets to determine if an email had been received.	17 of 60 mainframe security software password resets selected did not have an email request submitted.
		If the user does not utilize the Self-Service Solutions to reset their AD password, the user is required to submit an email or problem report to the Help Desk requesting their password be reset.	Reviewed AD resets to determine if an email or problem report was received.	The Department did not follow the requirements of an email or problem report to be submitted for AD password resets.
		The Exit Form is sent to the employee's supervisor indicating the items to be retrieved and the deactivation of access.	Reviewed a selection of separations to determine if their access had been deactivated in a timely manner.	5 of 12 separated individuals selected did not have their access deactivated in a timely manner.
		Bi-monthly, a report is run documenting separations from the Department and proxy agencies. The report is reviewed to ensure the applicable security software IDs are revoked.	Reviewed a selection of reports to determine if the reports had been reviewed and the security software IDs were revoked.	No deviation noted.

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

	Criteria	Department's Control	Testing Performed	Results
		Non-expiring mainframe security software ID are required to complete a Request for Non-Expiring RACF ID Form and be approved by the Compliance Manager.	Reviewed a selection of non-expiring mainframe security software IDs to determine if the Form was completed and approved by the Compliance Manager.	No deviation noted.
		On an annual basis, the Security Software Administrator will send out the Security Reconciliation Report to agencies.	Reviewed the Security Reconciliation Report to determine if the Security Reconciliation Reports had been sent out.	No deviation noted.
		Only authorized staff are able to create or modify a user's access.	Reviewed a selection of authorized staff to determine if access was appropriate.	No deviation noted.
		The Department maintained a VPN solution to connect remotely into resources managed and maintained by the Department.	Reviewed the VPN configurations to determine if the security settings were configured to allow for a secure remote connection into resources 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 to determine if users establish their identity and authentication to systems and applications.	No deviation noted.
			Observed a user to determine if they were assigned a user ID and password.	No deviation noted.

	Criteria	Department’s Control	Testing Performed	Results
			Reviewed a selection of user accounts with powerful access rights to determine if rights were appropriate.	No deviation noted.
		Authentication servers utilize an administrative architecture in which groups are established with specific levels of administrative privileges for individual’s needs.	Reviewed a selection of groups to determine if the privileges were appropriate.	No deviation noted.
		Password parameters have been established on authentication servers.	Reviewed the network password parameters to determine if the password strength, duration and history were configured as documented.	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 selection of configuration files to determine if firewalls, routers, and switches were configured to utilize authentication servers, logging servers, banners warning prohibiting unauthorized access and warring of prosecution and ACLs to deny and permit specific traffic.	1 of 60 devices selected did not have a banner placed in the configuration file.
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 Central Computer Facility (CCF) and Communications Building are monitored 24 hours a day, 7 days a week by security guards.	Reviewed security guard contract to determine their duties at the CCF and Communications Building.	No deviation noted.

	Criteria	Department’s Control	Testing Performed	Results
			Observed the security guards to determine their performance of duties.	No deviation noted.
		Video surveillance cameras are located on the interior and exterior of the CCF and Communications Building.	Observed the locations of the video surveillance cameras to determine the monitoring of the CCF and Communications Building.	No deviation noted.
		The security guards and the Physical Security Coordinator monitor the video feeds.	Observed the video feeds to determine if they were monitored by the security guards and the Physical Security Coordinator.	No deviation noted.
		Security alarms have been placed throughout the CCF and Communications Building.	Observed location of security alarms to determine if the CCF and Communications Building had been alarmed.	No deviation noted.
		If an alarm is triggered, an alert notifies the Velocity System.	Observed alarm notifications to determine if the Velocity Systems sent alert notifications.	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 determine the prevention of unauthorized access.	No deviation noted.
		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 and within the facilities.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		In order to obtain a card key, an ID Badge Request Form is to be completed; approval must be obtained from an authorized manager, a valid ID must be presented and a background check must be completed prior to access being granted.	Reviewed a selection of new employees and contractors' ID Badge Request Forms to determine if the Forms were properly approved.	10 of 23 Badge Request Forms selected were approved 1 to 102 days after the hire date. 2 of 23 employees selected did not have a completed Badge Request Form.
			Reviewed a selection of new employees and contractors to determine if a background check had been completed prior to access being granted.	No deviation noted.
		Access to restricted areas is based on the employee's and contractor's duties.	Reviewed a selection of employees and contractors with access to the CCF, Communications Building and sensitive area to determine appropriateness.	9 of 60 employees or contractors selected had access that was no longer required.
		Visitors are required to sign in and out, provide their driver's license, and be escorted.	Reviewed a selection of Admittance Registers to determine if visitor sign in and out was properly completed.	1 of 60 Admittance Registers selected was not properly completed.
			Observed visitors being escorted.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		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 selection 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.
		Visitors are provided visitor badges, which does not permit access to or within the CCF and Communications Building.	Observed the operation of the visitor badge to determine if access to the CCF and Communications Building was not permitted.	No deviation noted.
		Upon separation from the Department, Personnel completes a PAR, which notifies the Department's CFO of the departure. Personnel also sends the employee's supervisor an Exit Form which outlines the items to be retrieved and deactivation of access.	Reviewed a selection of separations to determine if a PAR and Exit Form had been completed.	No deviation noted for employees. The Department had not implemented a formal exit process for contractor separations.

	Criteria	Department's Control	Testing Performed	Results
		The Exit Form is sent to the employee's supervisor to ensure collection of equipment and termination of access.	Reviewed a selection of terminated employees and contractors to determine timely deactivation of access.	1 of 12 selected terminated contractor's separation notification was not received by the Physical Security Coordinator. 4 of 12 selected terminated contractor's badge were deactivated 1 to 150 days after employment.
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 mainframe system security software.	Reviewed system options and security software reports to determine if information was protected by security software.	No deviation noted.
		Network diagrams are maintained depicting the infrastructure and placement of firewalls, routers, and switches.	Reviewed the network diagrams to determine the placement of the firewalls, routers and switches.	No deviation noted.
		The Department maintained a VPN solution to connect remotely into resources managed and maintained by the Department.	Reviewed the VPN configurations to determine if the security settings were configured to allow for a secure remote connection into resources managed and maintained by the Department.	No deviation noted.

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

	Criteria	Department’s Control	Testing Performed	Results
		Laptop and desktop operating systems are updated as required by the vendor.	Reviewed the compliance report to determine if the operating system was updated on the laptops and desktops.	Of the 40,493 laptops and desktops connected to services on May 16, 2016, 656 were not running the latest version of the operating system. Of the 44,584 laptops and desktops connected to services on May 16, 2016, 12,900 were not running the latest operating system patch.
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 if the data classification schema utilized to value and classify information generated, access, transmitted or stored was documented.	No deviation noted.
		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.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		The Department makes available encryption technologies and access gateways for the transmission of sensitive or confidential information.	Reviewed the VPN configurations to determine the security settings are configured to allow for a secure remote connection into resources managed and maintained by the Department.	No deviation noted.
			Reviewed the VPN web portal login screen to determine if a banner was displayed to indicate 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.
		Laptops deployed after December 1, 2007 have encryption installed.	Reviewed a selection of laptops deployed after December 1, 2007 to determine if encryption had been installed.	Information to determine if encryption had been installed on 6 of 40 laptops selected was not available.
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 was 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 if access to system resources was restricted to authorized staff.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		Antivirus is installed on laptops and desktops.	Reviewed the compliance report to determine if antivirus was installed on selected laptops/desktops.	Information to determine if antivirus was installed on 11 of 40 laptops and desktops selected was not available.
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.
		Problems, issues, and incidents are recorded via the Daily Shift Report and a Remedy ticket is created.	Reviewed a selection of Daily Shift Reports to determine if problems, issues, and incidents were reported.	No deviation noted.
		For any incident the Operations Center cannot resolve, the Remedy ticket is assigned to the applicable division for resolution.	Reviewed a selection 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 and access to determine if records exist for monitoring, documenting operating system actions.	No deviation noted.
		System performance is monitored via software tools.	Reviewed a selection of software tool reports to determine if system performance was monitored.	No deviation noted.

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

	Criteria	Department’s Control	Testing Performed	Results
		Performance monitoring is documented via internal memorandum distributed to management.	Reviewed a selection of memorandums to management regarding system performance and capacity to determine if issues were documented.	No deviation noted.
		Remote Monitoring Facility (RMR) reports are run weekly and monthly.	Reviewed a selection of RMF reports to determine the frequency.	No deviation noted.
		Library Services maintains a listing of backups which are scheduled to be run on SharePoint.	Reviewed a selection of schedules which were maintained on SharePoint to determine backup schedules.	No deviation noted.
		The day after the backup is scheduled to run, a report is run to determine the success/failure of the job.	Reviewed a selection of backup logs to determine the success or failure of the job.	No deviation noted.
		The user may utilize one of the two Self-Service Solutions, BCCS Identity Management Solution or the Forefront Identity Manager Solution, to reset their passwords.	Reviewed the Department’s Identity Management Website to determine solutions to reset passwords.	No deviation noted.
		If the user does not utilize the Self-Service Solutions to reset their mainframe security software password, they are to send an email to the Help Desk requesting such.	Reviewed a selection of mainframe security software password resets to determine if an email had been received.	17 of 60 mainframe security software password resets selected did not have an email request submitted.

	Criteria	Department's Control	Testing Performed	Results
		If the user does not utilize the Self-Service Solutions to reset their AD password, the user is required to submit an email or problem report to the Help Desk requesting their password be reset.	Reviewed AD resets to determine if an email or problem report was received.	The Department did not follow the requirements of an email or problem report to be submitted for Active Directory password resets.
		Authentication servers are utilized to control access, log access attempts, and alert management.	Reviewed system settings to determine if authentication servers were utilized to control access, log access attempts, and alert management based upon predetermined thresholds.	No deviation noted.
		The Department has tools in place to identify and log network services security breaches, in addition to notifying management if devices exceed predetermined thresholds.	Reviewed a selection of configuration files to determine if firewalls, routers, and switches were configured to utilize logging servers.	No deviation noted.
			Reviewed SolarWinds system settings to determine if SolarWinds monitors performance, bandwidth utilization, CPU utilization, and whether management was notified if devices exceed the predetermined threshold.	No deviation noted.

	Criteria	Department’s Control	Testing Performed	Results
			Reviewed a selection of firewalls, routers, and switches to determine if the devices were connected to SolarWinds reporting tools.	No deviation noted.
		Routine backups of configurations for firewalls, routers and switches are conducted.	Reviewed a selection of firewalls, routers, and switches to determine if the devices were connected to backup solutions.	No deviation noted.
			Reviewed system settings to determine if routine backups were configured for firewalls, routers and switches.	No deviation noted.
		The Department is notified of failed backups.	Reviewed system settings to determine if the Department was notified of failed backups.	System was not configured to notify management of failed ICN configuration backups.
		Network monitoring tools are utilized to monitor inbound and outbound network traffic.	Reviewed the tools utilized to monitor traffic to determine who was monitoring and the frequency of monitoring.	No deviation noted.
			Reviewed a selection of monthly network monitoring reports to determine who monitors inbound and outbound network traffic.	No deviation noted.
		CA-Scheduler is utilized to schedule and control mainframe backups.	Reviewed a selection of backup schedules to determine if mainframe systems were backed up.	No deviation noted.
		Backups are conducted routinely.	Reviewed a selection of schedules to determine if backups were conducted.	No deviation noted.

TRUST SERVICES - CRITERIA, 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 verifies that daily and weekly backups were completed successfully.	Reviewed a selection of the verify backup reports to determine if backups were completed successfully.	No deviation noted.
			Reviewed a selection of Disk Library for Mainframe (DLM) logs to determine if the replication was successful.	No deviation noted.
		The Department is notified of failed backups.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
		Failed backups are recorded on the Shift Report.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

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

	Criteria	Department's Control	Testing Performed	Results
		System automation tool controls and monitors available storage levels.	Reviewed system automation tool storage levels.	No deviation noted.
		System automation tool notifies staff via email when storage levels fall below the pre-determined threshold.	Requested from the Enterprise Storage and Backups staff the email notifications.	The Department did not maintain the email notifications.
		A Remedy ticket is created if an agency requires additional storage.	Reviewed a selection of requests for additional storage to determine if a Remedy ticket was created.	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 the instructions for contacting the Help Desk were included.	No deviation noted.
		The Enterprise Desktop/Laptop Policy, the Mobile Device Security Policy, and the Missing IT Equipment Procedures provide guidance to users for the reporting of lost or stolen assets.	Reviewed policies and procedures to determine if they provided adequate guidance for reporting lost or stolen assets.	The Missing IT Equipment Procedure did not address the process in the event encryption was not installed on missing equipment.
		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 selection of lost/stolen devices to determine if a Remedy ticket had been created and a police report was attached to the Remedy 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.	Reviewed a selection of lost/stolen devices to determine if EUC had conducted an analysis to determine if encryption was installed.	2 of 5 lost/stolen laptops selected did not have an analysis completed to determine if encryption had been installed.
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 selection of Daily Shift Reports to determine if problems, issues, and incidents were reported.	No deviation noted.
		For any incident the Operations Center cannot resolve, the Remedy ticket is assigned to the applicable division for resolution.	Reviewed a selection 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 selection of Daily Shift Reports to determine if the activity on production systems was recorded and incident calls were recorded.	No deviation noted.

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

	Criteria	Department’s Control	Testing Performed	Results
		In the event division staff or management needs to be notified, contact information is maintained with the FOCAL database.	Observed the FOCAL database to determine management contact information was maintained.	No deviation noted.
		The user manuals for applications provide instructions for users to contact the Help Desk to report issues.	Reviewed user manuals to determine if they provided instruction to report issues to the Help Desk.	No deviation noted.
		The Department is notified of failed backups.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
		The Department takes remedial action on failed backups.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

	Criteria	Department’s Control	Testing Performed	Results
		The Enterprise Desktop/Laptop Policy, the Mobile Device Security Policy, and the Missing IT Equipment Procedures provided guidance to users for the reporting of lost or stolen assets.	Reviewed policies and procedures to determine if they provided adequate guidance for reporting lost or stolen assets.	The Missing IT Equipment Procedure did not address the process in the event encryption was not installed on missing equipment.
		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 selection 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.	Reviewed a selection of lost/stolen devices to determine if EUC had conducted an analysis to determine if encryption was installed.	2 of 5 lost/stolen laptops selected did not have an analysis completed to determine if encryption had been installed.
CC7.1	Security, availability, and processing integrity commitments and requirements, are addressed, during the system development lifecycle including design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.	Department maintains a documented change management process.	Reviewed the Remedy Guide (Guide) and Change Management Policy (Policy) to determine the change management process.	The Guide did not provide sufficient guidance or requirements for post implementation reviews. The Policy did not provide sufficient guidance or requirements for

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

	Criteria	Department’s Control	Testing Performed	Results
				testing, evaluating, and authorizing changes prior to implementation. Prior to January 29, 2016, the Department had not provided guidance or requirements related to implementation plans, testing plans, or back-out plans.
		Changes (RFCs/changes) are categorized and ranked according to priority.	Reviewed a selection of changes to determine if they were properly categorized and ranked according to priority.	No deviation noted.
		Emergency changes require verbal approval prior to implementation. Standard approvals are to be obtained post implementation.	Reviewed a selection of emergency changes to determine if verbal approval was obtained prior and if standard approvals were obtained post implementation.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		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 selection of changes to determine if they were properly approved.	No deviation noted.
		Application changes are required to have the Mainframe Checklist completed.	Reviewed a selection of application changes to determine if the Mainframe Checklist had been completed.	4 of 30 change tasks selected did not have the Mainframe Checklist completed. 1 of 26 change tasks selected did not have the Mainframe Checklist properly completed.

	Criteria	Department's Control	Testing Performed	Results
		Changes to applications determined to be routine or minor are to be managed via Remedy and follow the EAA Change Management Procedures. Changes that alter the design basis will be managed via the EPM Portal and the Application Life Cycle Management Methodology.	Reviewed the EAA Change Management Procedures (Procedures) and the Application Life Cycle Management Methodology (Methodology) to determine the change management process.	The Procedures and the Methodology did not address: -Required approvals, -Testing and documentation requirements, -Requirements for followup after change is moved to production, and -Emergency change requirements.
			Reviewed a selection of application changes to determine compliance with the EAA Change Management Procedures and the Application Life Cycle Management Methodology.	5 of 5 changes selected did not have the required Impact Assessment completed, did not have the Business Owner approval, and did not have Key Communications noted within the change ticket.
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.	Post implementation reviews (PIR) are conducted on a 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 selection of emergency changes to determine if a PIR had been conducted and properly approved.	1 of 6 emergency changes selected did not have a PIR conducted.

	Criteria	Department’s Control	Testing Performed	Results
			The Department did not have a mechanism to track changes which caused an outage. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not have a mechanism to track changes which caused an outage. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
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 a selection of changes to determine if a RFC was properly completed.	55 of 60 RFCs selected did not have the requested date field completed. 1 of 60 RFCs selected did not have the impact field completed, did not have the estimated down time field completed, and did not have the DR update field completed as required by the Create Change Request Guide.

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

	Criteria	Department's Control	Testing Performed	Results
		Approvals, plans and information associated with the change are to be attached or included within the specific RFC for record purposes.	Reviewed a selection of changes to determine if they were properly approved, and plans and information were attached or included.	No deviation noted.
		A post implementation review is conducted on changes which cause an outage or an emergency change. The review is conducted by the change supervisor or a Change Management Team member.	Reviewed a selection of emergency changes to determine if a post implement review had been conducted.	1 of 6 emergency changes selected did not have a post implementation review completed.
			The Department did not have a mechanism to track changes which caused an outage. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not have a mechanism to track changes which caused an outage. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

	Criteria	Department’s Control	Testing Performed	Results
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 selection of high impact changes to determine if the RFC had backout, testing, and implementation plans attached.	Testing and documentation requirements for backout and implementation plans had not been established prior to January 29, 2016. After January 30, 2016, no deviation noted.
		Emergency changes require verbal approval prior to implementation. Standard approvals are to be obtained post implementation.	Reviewed a selection of emergency changes to determine if verbal approval was obtained prior to moving to production and standard approvals were obtained post implementation.	No deviation noted.
		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 Managers, Change Management Team and the Change Advisory Committee (CAC).	Reviewed a selection of changes to determine if they were properly approved.	No deviation noted.

TRUST SERVICES - CRITERIA, 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 detail of testing, and the documentation requirements for testing, backout and implementation plans, are to be established by each division.	Reviewed documentation requirements. Reviewed a selection of changes to determine if testing, backout and implementation plans met the requirements.	Testing and documentation requirements for backout and implementation plans had not been established prior to January 29, 2016. After January 30, 2016, no deviation noted.
		For moves related to AIS, CPS, CIS and CTAS, 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 selection of moves to determine if a move sheet and an authorized email were submitted which indicated the date, time, and libraries to be moved to production.	4 of 19 change tasks selected did not have a completed move sheet.
		For moves related to eTime, the EA&A Interactive Production Administrator Group complete the moves.	The Department did not have any changes to eTime. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not have any changes to eTime. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

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

	Criteria	Department's Control	Testing Performed	Results
		Library Services standards control the moves of changes to agency applications to production libraries.	Reviewed the Library Services Standards to determine the process over 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 selection of moves to determine if an authorized email was submitted which indicated the date, time and libraries to be moved.	1 of 60 moves selected was not authorized.
		Standards provide guidance on the configuration and deployment of network devices.	Reviewed standard and configuration templates to determine if they provided guidance on the configuration and deployment of network devices.	No deviation noted.
		Tools are in place to assist in the deployment of and reporting on configurations.	Reviewed a selection of firewalls, routers, and switches to determine if devices were connected to SolarWinds reporting tools.	No deviation noted.

TRUST SERVICES - CRITERIA, 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 a selection of software tool reports to determine if system capacity was monitored.	No deviation noted.
		Capacity monitoring is documented via internal memorandum distributed to management.	Reviewed a selection of memorandums to management regarding system performance and capacity to determine if issues were documented.	No deviation noted.
		The network is configured in a redundant manner.	Reviewed a selection of firewalls, routers, and switches to determine if devices were configured in a redundant manner for availability.	52 of 60 firewalls, routers, and switches selected were not configured in a redundant manner for availability.
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 (Plan), IT Recovery Policy (Policy), and the Recovery Methodology (Methodology) have been developed.	Reviewed the Plan, Policy, and the Methodology to determine recovery process.	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 to determine utilization of space for a cold site.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		Application recovery plans or procedures have been developed.	Reviewed the applications recovery plan or procedures to determine recovery process.	The Central Inventory System Plan had not been updated to include the Vtape and did not include information regarding testing requirements and Recovery Time Objective (RTO). The Central Payroll Plan did not include information regarding testing requirements and RTO. The Central Time and Attendance System Recovery documentation did not include information regarding testing requirements and RTO.

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

	Criteria	Department's Control	Testing Performed	Results
				The eTime System documentation did not outline responsibilities, testing requirements, location of recovery documentation, and RTO.
		Application data is backed up daily, weekly and monthly.	Reviewed the backup schedules to determine if the application was scheduled to be backed up daily, weekly and monthly.	No deviation noted.
		Upon receipt of an authorized email, Library Services will restore production libraries. The authorized email indicates the library to be restored and the date and time.	Reviewed a selection of restores to determine if an authorized email was submitted indicating the library, date and time.	No deviation noted.
		The Department has configured the network in a redundant manner.	Reviewed a selection of firewalls, routers, and switches to determine if devices were configured in a redundant manner for availability.	52 of 60 firewalls, routers, and switches selected were not configured in a redundant manner for availability.
		CA-Scheduler is utilized to schedule and control backups.	Reviewed a selection of backup schedules to determine if mainframe systems were backed up.	No deviation noted.
		Backups are conducted routinely.	Reviewed a selection of schedules to determine if backups were conducted.	No deviation noted.

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

	Criteria	Department’s Control	Testing Performed	Results
		The Department verifies that daily and weekly backups were completed successfully.	Reviewed a selection of verify backup reports to determine if backups were completed successfully.	No deviation noted.
			Reviewed a selection of DLM logs to determine if the replication was successful.	No deviation noted.
		The Department is notified of failed backups.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
		Failed backups are recorded on the Shift Report.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

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

	Criteria	Department's Control	Testing Performed	Results
		The Department takes remedial action on failed backups.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
		Data replication occurs every 10 minutes between the CCF and the Alternate Data Center (ADC).	Reviewed a selection of replication logs to determine if replication occurred every 10 minutes.	No deviation noted.
		Monitoring software sends an alert if the data is out of sync for more than 8 hours.	Reviewed the monitoring software to determine if an alert was sent if data was out of sync for more than 8 hours.	No deviation noted.
		A Remedy ticket is opened in the event of a data replication issue.	The Department did not encounter data replication issues during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not encounter data replication issues during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

	Criteria	Department's Control	Testing Performed	Results
		The software vendor and the staff hold weekly meetings to discuss any issues.	Requested from the Enterprise Storage and Backup staff the meeting minutes.	The Department did not maintain meeting minutes.
		Logs are maintained of the libraries replicated, their status, and the time of last sync.	Reviewed a selection of logs to determine if libraries were replicated, their status and the time of last sync.	No deviation noted.
		A system automation tool controls and monitors available storage levels.	Reviewed system automation tool storage levels.	No deviation noted.
		A system automation tool notifies staff via email when storage levels fall below the pre-determined threshold.	Requested from the Enterprise Storage and Backup staff the email notifications.	The Department did not maintain the email notifications.
		A Remedy ticket is created if an agency requires additional storage.	Reviewed a selection of requests for additional storage to determine if a Remedy ticket had been created.	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 various measures in place to protect against environmental factors at the CCF and Communications Building.	No deviation noted.

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

	Criteria	Department's Control	Testing Performed	Results
			Reviewed contracts and maintenance reports to determine if the UPS and Generators had been inspected.	Contractually scheduled monthly and semi-annual inspections were not conducted.
		Preventive maintenance agreements and scheduled maintenance procedures are in place for environmental factors.	Reviewed maintenance agreements to determine compliance.	A fire suppression contract for the CCF was not in place from July 1, 2015 to August 25, 2015. Chiller maintenance contract for the CCF was not in place from February 1, 2016 to April 18, 2016. A fire extinguisher contract for the CCF and Communications Building was not in place from February 29, 2016 to April 28, 2016.
			Reviewed scheduled procedures outlined in maintenance contracts to determine compliance.	Contractually scheduled monthly and semi-monthly inspections were not conducted.

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

	Criteria	Department's Control	Testing Performed	Results
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 (Plan) is tested.	Reviewed the 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 October 2015 comprehensive test to determine testing completed.	No deviation noted.
		Application recovery plans or procedures have been developed.	Reviewed the applications recovery plan or procedures to determine recovery process.	The Central Inventory System Plan had not been updated to include the Vtape and did not include information regarding testing requirements and Recovery Time Objective (RTO). The Central Payroll Plan did not include information regarding testing requirements and RTO.

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

	Criteria	Department’s Control	Testing Performed	Results
				The Central Time and Attendance System Recovery documentation did not include information regarding testing requirements and RTO. The eTime System documentation did not outline responsibilities, testing requirements, location of recovery documentation, and RTO.

TRUST SERVICES - CRITERIA, 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 a selection of software tool reports to determine if system capacity was monitored.	No deviation noted.
		Application data is backed up daily, weekly and monthly.	Reviewed the backup schedules to determine if the application was scheduled to be backed up daily, weekly and monthly.	No deviation noted.
		Vendor agreements are in place for maintenance and support services associated with networking equipment.	Reviewed vendor agreements to determine if maintenance and support services were addressed.	No deviation noted.
			Reviewed a selection of firewalls, routers, and switches to determine if hardware and software were supported by the vendor.	16 of 60 hardware devices selected were no longer supported by the vendor. 12 of 60 software versions selected were no longer supported by the vendor.
		CA-Scheduler is utilized to schedule and control backups.	Reviewed a selection of backup schedules to determine if mainframe systems were backed up.	No deviation noted.
		Backups are conducted routinely.	Reviewed a selection of schedules to determine if backups were conducted.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		The Department verifies that daily and weekly backups were completed successfully.	Reviewed a selection of verify backup reports to determine if backups were completed successfully.	No deviation noted.
			Reviewed a selection of DLM logs to determine if the replication was successful.	No deviation noted.
		The Department is notified of failed backups.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
		Failed backups are recorded on the Shift Report.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

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

	Criteria	Department’s Control	Testing Performed	Results
		The Department takes remedial action on failed backups.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
		Data replication occurs every 10 minutes between the CCF and the ADC.	Reviewed replication logs to determine if replication occurred every 10 minutes.	No deviation noted.
		Monitoring software sends an alert if the data is out of sync for more than 8 hours.	Reviewed the monitoring software to determine if an alert is sent if data is out of sync for more than 8 hours.	No deviation noted.
		Logs are maintained of the libraries replicated, their status and the time of last sync.	Reviewed a selection of logs to determine if libraries were replicated, their status and the time of last sync.	No deviation noted.

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

	Criteria	Department's Control	Testing Performed	Results
		A Remedy ticket is opened in the event of an issue.	The Department did not encounter data replication issues during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.	The Department did not encounter data replication issues during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
		The software vendor and the staff hold weekly meetings to discuss any issues.	Requested from the Enterprise Storage and Backup staff the meeting minutes.	The Department did not maintain meeting minutes.
		System automation tool controls and monitors available storage levels.	Reviewed system automation tool storage levels.	No deviation noted.
		System automation tool notifies staff via email when storage levels fall below the pre-determined threshold.	Requested from the Enterprise Storage and Backup staff the email notifications.	The Department did not maintain the email notifications.
		A Remedy ticket is created if an agency requires additional storage.	Reviewed a selection of requests for additional storage to determine if a Remedy ticket was created.	No deviation noted.

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

	Criteria	Department's Control	Testing Performed	Results
		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 various measures in place to protect against environmental factors at the CCF and Communications Building.	No deviation noted.
			Reviewed the fire extinguishers and suppression system maintenance agreements to determine compliance.	A fire suppression contract for the CCF was not in place from July 1, 2015 to August 25, 2015. A fire extinguisher contract for the CCF and Communications Building was not in place from February 29, 2016 to April 28, 2016.
			Reviewed contracts and maintenance reports to determine if the UPS and Generators had been tested.	Contractually scheduled monthly and semi-annual inspections were not conducted.

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

	Criteria	Department's Control	Testing Performed	Results
			Observed the various measures in place to protect against environmental factors at the CCF and Communications Building.	No deviation noted.
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 selection of field edits and range checks to determine if they were functioning appropriately and were providing error notifications.	18 of 43 States with income tax requirements were not included in the Central Payroll System tax tables. 2 of 25 States' (including Washington DC) tax rates were incorrect. The State of Illinois tax rate was correct.
			Reviewed a selection of agencies data to determine if edits and checks were functioning appropriately.	No deviation noted.
PI1.3	Data is processed completely, accurately, and timely as authorized in accordance with processing integrity commitments and requirements.	Applications provide various reports to ensure accuracy of information.	Reviewed various reports to determine application reports available.	No deviation noted.
		Each transaction is assigned an identifying number.	Reviewed a selection of agencies' data to determine if each transaction had an identifying number assigned.	No deviation noted.

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

	Criteria	Department's Control	Testing Performed	Results
PI1.4	Data is stored and maintained completely and accurately for its specified life span in accordance with processing integrity commitments and requirements.	The Department maintains transaction history for a defined period of time.	Reviewed the transaction history to determine time period of history.	No deviation noted.
		Access to the application's production libraries has been restricted to authorized Department personnel.	Reviewed a selection of users with access to production libraries to determine appropriateness.	No deviation noted
		Applications provide various reports to ensure accuracy of information.	Reviewed various reports to determine application reports available.	No deviation noted.
		Application data is backed up daily, weekly and monthly.	Reviewed the backup schedule to determine if the application was scheduled to be backed up daily, weekly and monthly.	No deviation noted.
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 a selection of individuals with access to print shop to determine if access was appropriate.	4 of 11 individuals selected no longer required access.

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

	Criteria	Department's Control	Testing Performed	Results
		Upon request for pick up, the individual must provide identification, sign the Report Distribution Checklist, and be on the authorization listing.	Reviewed a selection of Report Distribution Checklist to determine if the individual who picked up the print job was authorized.	1 individual listed on the Report Distribution Checkout List for 25 days selected was not on the authorization listing.
		Applications provide various reports to ensure accuracy of information.	Reviewed various reports to determine application reports available.	No deviation noted.
PI1.6	Modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.	Access to the application's production libraries has been restricted to authorized Department personnel.	Reviewed a selection of users with access to production libraries to determine appropriateness.	No deviation noted.
		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 restricted the ability to access, approve, modify and delete transactions.	No deviation noted
		Application data is backed up daily, weekly and monthly.	Reviewed the backup schedules to determine if the application was scheduled to be backed up daily, weekly and monthly.	No deviation noted.

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)

Below are responses from Department management to deviations identified by the service auditor.

Principle	Criteria	Correction Action Plan
Common Criteria	CC1.4	The Department will conduct periodic review of employees' and contractors' completion of security awareness training.
	CC1.4	The Department will conduct periodic review of employees' completion of security awareness training.
	CC1.4	The Department will conduct periodic review of contractors' completion of security awareness training.
	CC1.4	The Department will conduct periodic review for compliance.
	CC2.2	The Department will conduct periodic review of employees' completion of security awareness training.
	CC2.2	The Department will conduct periodic review of contractors' completion of security awareness training.
	CC2.2	The Department will review policies to ensure they address requirements for requesting, obtaining, modifying, and revocation of access rights, periodic review of access, and supervisory notification regarding security issues.
	CC2.3	The Department will review policies to ensure they address requirements for requesting, obtaining, modifying, and revocation of access rights, periodic review of access, and supervisory notification regarding security issues.
	CC2.3	The Department will conduct periodic review of employees' completion of security awareness training.
	CC2.3	The Department will conduct periodic review of contractors' completion of security awareness training.
	CC2.4	The Department will review policies to ensure they address requirements for requesting, obtaining, modifying, and revocation of access rights, periodic review of access, and supervisory notification regarding security issues. The Department will review procedures to ensure they address the Mainframe Security Request Form.

	CC2.5	The Department will review security policies to determine if appropriate personnel are notified and what actions should be taken after notification.
	CC2.5	The Department will review policies and procedures to determine adequate guidance for reporting lost or stolen assets.
	CC2.5	The Department will conduct periodic review of security issues to determine compliance with procedures.
	CC2.5	The Department will review and update MORT policies to more accurately reflect current environment.
	CC2.6	The Department will ensure relevant items are discussed in change meetings and documented.
	CC3.1	The Department will implement controls to identify, analyze and mitigate potential threats.
	CC3.2	The Department will review controls related to the assessment and mitigation of risk.
	CC3.3	The Department will review controls related to the assessment and mitigation of risk.
	CC5.1	The Department will conduct periodic reviews of security software profiles to determine if access to system resources are adequate.
	CC5.1	The Department will conduct periodic reviews of security software profiles for primary systems programming groups and support staff to determine if access to system resources is correct.
	CC5.1	The Department will ensure firewalls, routers, and switches are configured with appropriate banner warning.
	CC5.2	The Department will develop procedures to ensure all applicable ESR field are complete.
	CC5.2	The Department intends to research, acquire and implement an Active Directory solution for capturing AD modifications.
	CC5.2	The Department intends to research, acquire and implement a mainframe solution for capturing mainframe security password modifications.
	CC5.2	The Department will review mainframe password reset procedures to ensure compliance.

	CC5.2	The Department will review Active Directory password policies and procedures to ensure users can be verified.
	CC5.2	The Department will ensure procedures for granting and removing access is performed in a timely manner.
	CC5.2	The Department will develop and implement processes that include contractor separation.
	CC5.3	The Department will ensure firewalls, routers, and switches are configured with appropriate banner warning.
	CC5.4	The Department will develop procedures to ensure all applicable ESR field are complete.
	CC5.4	The Department intends to research, acquire and implement a mainframe solution for capturing mainframe security password modifications.
	CC5.4	The Department intends to research, acquire and implement an Active Directory solution for capturing AD modifications.
	CC5.4	The Department will communicate to its managers that an email should be submitted before a mainframe security password can be reset.
	CC5.4	The Department will review Active Directory password policies and procedures to ensure users can be verified.
	CC5.4	The Department intends to develop and implement processes to ensure separated employees are deactivated in a timely manner.
	CC5.4	The Department will ensure firewalls, routers, and switches are configured with appropriate banner warning.
	CC5.5	The Department will work with DCMS Facilities Management to review and update the ID badge process to ensure access is appropriately approved and documentation is maintained.
	CC5.5	The Department will work with DCMS Facilities Management to periodically review access.
	CC5.5	The Department will ensure Admittance Registers for visitors are properly completed.
	CC5.5	The Department will develop and implement processes that include contractor separation.

	CC5.5	The Department will work with DCMS Facilities Management to ensure separation notification is received and access is timely deactivated.
	CC5.6	The Department intends to review, update and implement a process to ensure laptops and desktops are running the latest operating systems. The Department will also review the process for ensuring laptops have the latest patch installed.
	CC5.7	The Department will review the process for which information is maintained for laptops/desktops deployment to determine if encryption has been installed.
	CC5.8	The Department intends to implement a process for monitoring and tracking desktops and laptops anti-virus installations.
	CC6.1	The Department will review mainframe password reset procedures to ensure compliance.
	CC6.1	The Department will review Active Directory password policies and procedures to ensure users can be verified.
	CC6.1	The Department will review, update and implement processes regarding monitoring of failed ICN configuration backups.
	CC6.1	The Department will review, obtain and implement a system automated solution that notifies staff when storage levels fall below a predetermined threshold.
	CC6.1	The Department will review policies and procedures for Missing IT Equipment to determine adequate guidance for IT Equipment that is not encrypted.
	CC6.1	The Department will review and update procedures to ensure they provide adequate guidance for reporting lost or stolen IT equipment.
	CC6.2	The Department will review policies and procedures for Missing IT Equipment to determine adequate guidance for IT Equipment that is not encrypted.
	CC6.2	The Department will review and update procedures to ensure they provide adequate guidance for reporting lost or stolen IT equipment.
	CC7.1	The Department will review and update the Guide and policy to ensure reviews are performed.

	CC7.1	The Department will review application change requirements to ensure Mainframe Checklist has been completed appropriately.
	CC7.1	The EAA Change Management Procedures will be reviewed and updated as necessary.
	CC7.1	The Department will review application changes to ensure Impact Assessments are completed, Business Owner approvals is obtained and Key Communications are noted within the ticket.
	CC7.2	The Department will emphasize compliance with the Guide and proper documentation.
	CC7.2	The Department intends to research, acquire and implement a tracking solution to ensure compliance with the Guide.
	CC7.3	The Department will ensure compliance with the Guide and proper documentation.
	CC7.3	The Department will ensure requests for changes are appropriately completed.
	CC7.3	The Department intends to research, acquire and implement a tracking solution to ensure compliance with the Guide.
	CC7.4	The Department will review testing and documentation requirements for back out and implementation plans.
	CC7.4	The Department will emphasize the importance of ensuring an authorized email is submitted when libraries are to be moved.
	CC7.4	The Department will review application change procedures to ensure move sheets are appropriately approved.
Availability	A1.1	The Department will review network configuration to ensure availability.
	A1.2	The Department will review and update its policies and plans to ensure documentation addresses changes to the recovery vendor and backup processes
	A1.2	The Department will review and update its policies and plans to ensure documentation meets processing integrity and availability requirements.
	A1.2	The Department will review network configuration to ensure availability.
	A1.2	The Department will document weekly meetings with the vendor.

	A1.2	The Department will review, obtain and implement a system automated solution that notifies staff when storage levels fall below a predetermined threshold.
	A1.2	The Department will review schedules for contractually scheduled inspections to ensure monthly and semi-annual inspections are performed.
	A1.2	The Department will ensure contracts are in place to ensure scheduled inspections are performed.
	A1.2	The Department will review schedules for contractually scheduled inspections to ensure monthly and semi-annual inspections are performed.
	A1.3	The Department will review and update its policies and plans to ensure documentation meets processing integrity and availability requirements.
Processing Integrity	P1.1	The Department will review network hardware and software to ensure they are supported by the vendor
	P1.1	The Department will review the process for how vendor meetings are documented and maintained.
	P1.1	The Department will review system automation tools for notification of email notifications when storage levels fall below pre-determined thresholds.
	P1.1	The DoIT will review fire extinguishers and suppression system maintenance agreements for continuous service and testing of equipment.
	P1.1	The Department will review schedules for contractually scheduled inspections to ensure monthly and semi-annual inspections are performed.
	P1.2	The Department will review state tax rates for states where employees reside, correct them as needed, and implement a process to ensure the rates are updated.
	P1.5	The Department will review access rights to print shop to ensure access is appropriate.
	P1.5	The Department will work to ensure the report pickup procedures are followed.

Transfer of Information Technology Functions to the Department of Innovation and Technology

(Not Examined)

Executive Order 2016-01 (pages 116-124) transferred the Information Technology functions of the Department of Central Management Services, Bureau of Communications and Computer Services and State agencies in the Executive Branch to the Department of Innovation and Technology, effective July 1, 2016.

STATE OF ILLINOIS

EXECUTIVE DEPARTMENT

SPRINGFIELD, ILLINOIS

EXECUTIVE ORDER **2016-01**

EXECUTIVE ORDER CONSOLIDATING MULTIPLE INFORMATION TECHNOLOGY FUNCTIONS INTO A SINGLE DEPARTMENT OF INNOVATION AND TECHNOLOGY

WHEREAS, although the State of Illinois devotes significant resources to its information technology systems – ranking Illinois among the top five states nationally by technology expenditures – the State is considered among the bottom quartile of states nationally in digitization and other metrics of technological advancement; and

WHEREAS, much of the State's technology spending is wasted; most agencies are responsible for managing their own technologies and technology personnel, resulting in thousands of redundant and non-interoperable systems; and the State continues to use outdated systems (in some cases, dating to 1974) that are more costly to maintain; and

WHEREAS, these thousands of systems are vulnerable to cyberattack, placing private information about State employees and their dependents, consumers of State services, taxpayers, and the residents and businesses of Illinois at risk to hackers, terrorists, and criminals; and

WHEREAS, the State previously recognized and attempted to confront this problem: in 2003, the General Assembly authorized the Department of Central Management Services ("CMS") to direct the transfer and centralization of information technology functions from State agencies under the jurisdiction of the Governor to CMS; and

WHEREAS, under that authority, CMS consolidated some, but not all, information technology functions into its Bureau of Communications and Computer Services, but the results have been disappointing: many agencies continue to maintain their own infrastructure; almost all agencies continue to support their own software and application development; more than 70% of technology spending remains outside of CMS; and agencies in aggregate employ twice as many information technology personnel outside of CMS (approximately 1,200) as are employed by CMS (approximately 500); and

WHEREAS, although consolidation was not completed, it remains the best way to transform our information technology functions; to protect State data from cyberattack and breaches and to ensure compliance with data protection laws; to consolidate State technology resources, develop statewide enterprise solutions, leverage the State's buying power, and avoid inefficiencies; to reduce costs and provide better value for our investment; and to provide State agencies with state-of-the-art technology and ensure interoperability of systems and data across State agencies, enabling those agencies to provide better service to taxpayers, residents, businesses, and consumers and providers of State services; and

WHEREAS, consolidation and transformation of the State's information technology functions will be accomplished most effectively through an agency independent of CMS, in particular because: information technology is too large to be a bureau of another agency; the State's information technology headcount exceeds the combined headcount for all other functions performed by CMS; CMS is focused on other important administrative reforms; and the State must be nimble and flexible in order to meet the needs of its agencies and to provide timely, up-to-date technology services; and

WHEREAS, twenty-nine other states, as well as many local governments including the City of Chicago, have centralized responsibility for information technology functions within a single agency; and

WHEREAS, consolidation and transformation of the State's information technology functions will carry out the purposes of the 2003 legislation, now codified at 20 ILCS 405/405-410;

THEREFORE, I, Bruce Rauner, Governor of Illinois, by virtue of the executive authority vested in me by Section 11 of Article V of the Constitution of the State of Illinois, do hereby order as follows:

I. DEFINITIONS

As used in this Executive Order:

"BCCS" means the CMS Bureau of Communications and Computer Services, also known as the Bureau of Information and Communication Services, created by 2 IAC 750.40, or its successor bureau within CMS.

"Client agency" means each transferring agency or its successor and each other public agency to which DoIT provides service.

"CMS" means the Department of Central Management Services.

"DoIT" means the Department of Innovation and Technology.

"Information technology" means technology, infrastructure, equipment, systems, software, networks, and processes used to create, send, receive, and store electronic or digital information, including without limitation both computer systems and telecommunication systems. The term "information technology" shall be construed broadly to incorporate future technologies (such as sensors) that change or supplant those in effect as of the effective date of this Executive Order.

"Information technology functions" means the development, procurement, installation, retention, maintenance, operation, possession, storage, and related functions of all information technology.

"Information Technology Office" means the Information Technology Office, also known as of the Office of the Chief Information Officer, an office within the Office of the Governor, created by Executive Order 1999-05, or its successor office.

"Legacy IT division" means any division, bureau, or other unit of a transferring agency which has responsibility for information technology functions for the agency prior to the transfer of such functions to DoIT, including without limitation BCCS.

"Retained functions" means, with respect to a legacy IT division, non-information technology functions for which the legacy IT division is responsible, which are not transferred to DoIT.

"Secretary" means the Secretary of Innovation and Technology.

"Transferring agency" means each agency, authority, board, bureau, commission, council, department, division, instrumentality, office, or unit of the Executive Branch of State government which is directly responsible to the Governor and is transferring functions, employees, property, or funds to DoIT pursuant to this Executive Order.

II. CREATION OF DEPARTMENT OF INNOVATION AND TECHNOLOGY

The Information Technology Office, also known as the Office of the Chief Information Officer, is hereby reconstituted as a new principal department of the Executive Branch of State government, directly responsible to the Governor, called the Department of Innovation and Technology ("DoIT"). BCCS shall be consolidated into DoIT as of July 1, 2016.

The head officer of DoIT shall be known as the Secretary of Innovation and Technology ("Secretary"). The Secretary shall be the chief information officer for the State and the steward of State data, with respect to those agencies under the jurisdiction of the Governor. The Secretary shall be appointed by the Governor, with the advice and consent of the Senate. DoIT may employ or retain other persons to assist in the discharge of its functions, subject to the Personnel Code. DoIT shall be subject to all of the general laws applicable to Executive Branch agencies.

The mission of DoIT is to deliver best-in-class innovation and technology to client agencies to foster collaboration among client agencies, to empower client agencies to provide better service to residents of Illinois, and to maximize the value of taxpayer resources. DoIT shall be responsible for the information technology functions on behalf of client agencies.

DoIT shall develop and implement data security and interoperability policies and procedures that ensure the security and interoperability of State data, including in particular data that are confidential, sensitive, or protected from disclosure by privacy or other laws, while recognizing and balancing the need for collaboration and public transparency. DoIT shall ensure compliance with applicable federal and State laws pertaining to information technology, data, and records of DoIT and the client agencies, including without limitation the Freedom of Information Act (5 ILCS 140/1 *et seq.*), the State Records Act (5 ILCS 160/1 *et seq.*), the Personal Information Protection Act (815 ILCS 530/1 *et seq.*), the federal Health Insurance Portability and Accountability Act (HIPAA), the federal Health Information Technology for Economic and Clinical Health Act (HITECH Act), and the federal Gramm-Leach-Bliley Act.

DoIT may establish, through the Secretary, charges for services rendered by DoIT to client agencies for which funds are provided directly to the client agency. In establishing charges, the Secretary shall consult with client agencies, ensure that charges are transparent and clear, and minimize or avoid charges for costs for which DoIT has other funding sources available.

Following the transfer of information technology functions to DoIT pursuant to Section IV of this Executive Order, client agencies shall continue to apply for and otherwise seek federal funds and other capital and operational resources for technology for which the agencies are eligible and, subject to compliance with applicable laws, regulations, and grant terms, make those funds available for use by DoIT. DoIT shall assist client agencies in identifying funding opportunities and, if funds are used by DoIT, ensuring compliance with all applicable laws, regulations, and grant terms.

DoIT and each client agency continue to have whatever authority is provided to them pursuant to the Intergovernmental Cooperation Act and other applicable law to enter into interagency contracts. To the extent permitted by law, DoIT may enter into such contracts to use personnel and other resources that are retained by transferring agencies or other public agencies, to provide services to public agencies within the State in addition to transferring agencies, and for other appropriate purposes to accomplish DoIT's mission.

III. TRANSITION

Beginning on the effective date of this Executive Order, DoIT and the transferring agencies shall work cooperatively to prepare for the transfer of functions, employees, property, and funds pursuant to Section IV of this Executive Order, and to carry out other actions required to give effect to such transfers, as of July 1, 2016. The transferring agencies shall provide DoIT with access to personnel and other resources necessary to accomplish such transition. During the transition period:

1. Under the direction of the Governor, the Secretary, in consultation with the transferring agencies and labor organizations representing the affected employees, shall identify each position and employee who is engaged in the performance of functions transferred to DoIT, or engaged in the administration of a law the administration of which is transferred to DoIT, to be transferred to DoIT pursuant to Section IV(1) of this Executive Order. An employee engaged primarily in providing administrative support to a legacy IT division or information technology personnel may be considered engaged in the performance of functions transferred to DoIT. The Secretary shall ensure compliance with all applicable provisions of the Personnel Code and collective bargaining agreements, including providing any notices required thereunder within the applicable time periods.

2. Under the direction of the Governor, the Secretary, in consultation with the transferring agencies, shall identify personnel records, documents, books, correspondence, and other

property, both real and personal, affected by the reorganization to be transferred to DoIT pursuant to Section IV(2) of this Executive Order. Such property may include contracts pertaining to the functions transferred to DoIT.

3. Under the direction of the Governor, the Director of the Governor's Office of Management and Budget, in consultation with the Secretary and the transferring agencies, shall identify the unexpended balances of both Fiscal Year 2016 and Fiscal Year 2017 appropriations and other funds, or the relevant portions thereof, to be transferred to DoIT pursuant to Section IV(3) of this Executive Order.

IV. TRANSFER OF FUNCTIONS

As of July 1, 2016, the responsibility for information technology functions shall be transferred from each transferring agency to DoIT. These functions derive from the statutes set out on Exhibit A to this Executive Order. In connection with such transfer, as of July 1, 2016:

1. Each position and employee who is engaged in the performance of functions transferred to DoIT, or engaged in the administration of a law the administration of which is transferred to DoIT (as identified pursuant to Section III of this Executive Order), and the employee in each such position, shall be transferred to DoIT, pursuant to the provisions of any applicable collective bargaining agreement. The status and rights of any such employee, the State, and its agencies under the Personnel Code shall not be affected by this reorganization.

2. All personnel records, documents, books, correspondence, and other property, both real and personal, affected by the reorganization (as identified pursuant to Section III of this Executive Order) shall be delivered and transferred to DoIT or to the State Archives.

3. The unexpended balances of Fiscal Year 2016 and Fiscal Year 2017 appropriations and other funds available for use by a transferring agency in connection with the functions transferred to DoIT or the relevant portions thereof (as identified pursuant to Section III of this Executive Order and deemed necessary by the Governor) shall be transferred to DoIT and expended for the purposes for which the appropriations or other funds were originally made or given to the transferring agency.

4. With respect to each transferring agency, this reorganization shall not affect (i) the composition of any multi-member board, commission, or authority, (ii) the manner in which any official of the agency is appointed, (iii) whether the nomination or appointment of any official of the agency is subject to the advice and consent of the Senate, (iv) any eligibility or qualification requirements pertaining to service as an official of the agency, or (v) the service or term of any incumbent official serving as of the effective date of this Executive Order.

5. Whenever any provision of any previous Executive Order or any Act provides for membership on any board, commission, authority, or other entity by a representative or designee of a transferring agency with responsibility for the functions transferred to DoIT, the Secretary, in consultation with the head of the transferring agency, shall designate the same number of representatives or designees of DoIT or the transferring agency, as appropriate.

V. LEGACY INFORMATION TECHNOLOGY DIVISIONS

Some transferring agencies have dedicated divisions, bureaus, or other units within the agency that are responsible for information technology functions ("legacy IT divisions"). The purpose of this Section V is to provide for the winding up of those legacy IT divisions.

a. Legacy IT Divisions with No Retained Functions

A legacy IT division that is responsible for only information technology functions will have no retained functions after the transfer of those functions to DoIT. In that circumstance, (i) the functions, employees, property, and funds of the legacy IT division shall be transferred to DoIT pursuant to Section IV of this Executive Order, and (ii) the head of the transferring agency shall abolish the legacy IT division as soon as practicable after July 1, 2016.

b. Legacy IT Divisions with Retained Functions

A legacy IT division that is responsible for both information technology functions and non-information technology functions will continue to be responsible for those non-information technology functions ("retained functions") after the transfer of information technology functions to DoIT. In that circumstance, (i) the information technology functions, employees, property, and funds of the legacy IT division shall be transferred to DoIT pursuant to Section IV of this Executive Order, and (ii) the transferring agency shall continue to be responsible for the retained functions, and the head of the transferring agency shall consolidate the legacy IT division into another unit of the transferring agency or shall reconstitute the legacy IT division as a non-information technology unit of the transferring agency, as determined by the head of the transferring agency, as soon as practicable after July 1, 2016.

If a legacy IT division has retained functions, employees, property, or funds which are not transferred to DoIT, then:

1. Each employee of the legacy IT division who is not transferred to DoIT shall continue to be employed by the transferring agency in a unit determined by the head of that agency. The status and rights of any such employee, the State, and its agencies under the Personnel Code shall not be affected by this reorganization.

2. All personnel records, documents, books, correspondence, and other property, both real and personal, of the legacy IT division in any way pertaining to the retained functions shall continue to be possessed by the transferring agency, within a unit determined by the head of the transferring agency.

3. The unexpended balances of appropriations and other funds available for use by a legacy IT division in connection with the retained functions shall be maintained by the transferring agency and expended for the purposes for which the appropriations or other funds were originally made or given.

4. With respect to each legacy IT division and transferring agency, this reorganization shall not affect (i) the composition of any multi-member board, commission, or authority, (ii) the manner in which any official of the agency is appointed, (iii) whether the nomination or appointment of any official of the agency is subject to the advice and consent of the Senate, (iv) any eligibility or qualification requirements pertaining to service as an official of the agency, or (v) the service or term of any incumbent official serving as of the effective date of this Executive Order.

5. Whenever any provision of any previous Executive Order or any Act provides for membership on any board, commission, authority, or other entity by a representative or designee of a legacy IT division with responsibility for retained functions, the head of the transferring agency shall designate the same number of representatives or designees of the transferring agency, as appropriate.

VI. INCONSISTENT ACTS; SPECIAL FUNDS

From the effective date of this reorganization, and as long as such reorganization remains in effect, the operation of any prior act of the General Assembly inconsistent with this reorganization is suspended to the extent of the inconsistency. In particular, but without limitation:

1. As of July 1, 2016, the information technology functions transferred from the transferring agencies to DoIT shall be the responsibility of DoIT, notwithstanding any statute that provides in particular that such function shall be carried out by CMS or a transferring agency (including without limitation 20 ILCS 405/405-10, 405-20, 405-250, 405-255, 405-260, 405-265, and 405-270).

2. As of July 1, 2016, the authority of CMS to expend funds of the Statistical Services Revolving Fund (a special fund of the State established pursuant to 30 ILCS 105/5.55, 6p-1, and 8.16a) and the Communications Revolving Fund (a special fund of the State established pursuant to 30 ILCS 105/5.12, 6p-2, and 8.16b), or the successor funds, shall be transferred to DoIT; and the authority of the Director of CMS to approve any contract

or obligation incurred for any expenditure from either such special fund shall be transferred to the Secretary.

VII. REPORT TO THE GENERAL ASSEMBLY

DoIT shall provide a report to the General Assembly not later than December 31, 2016 and annually thereafter for three years, that includes data on the economies effected by the reorganization and an analysis of the effect of the reorganization on State government. The report shall also include the DoIT's recommendations for further legislation relating to reorganization.

A copy of such report shall be filed with the Speaker, the Minority Leader, and the Clerk of the House of Representatives; the President, the Minority Leader, and the Secretary of the Senate; the Legislative Research Unit; and the State Government Report Distribution Center for the General Assembly.

VIII. SAVINGS CLAUSE

1. The rights, powers, duties, and functions transferred to the DoIT by this Executive Order shall be vested in, and shall be exercised by, DoIT. Each act done in exercise of such rights, powers, duties, and functions shall have the same legal affect as if done by the agency from which they were transferred. Every person shall be subject to the same obligations and duties and to the associated penalties, if any, and shall have the same rights arising from the exercise of these obligations and duties as if exercised subject to that agency or the officers and employees of that agency.

2. This Executive Order shall not affect any act undertaken, ratified or cancelled or any right occurring or established or any action or proceeding commenced in an administrative, civil, or criminal case before this Executive Order takes effect, but these actions or proceedings may be prosecuted and continued by the successor agency in cooperation with another agency, if necessary.

3. This Executive Order shall not affect the legality of any rules in the Illinois Administrative Code that are in force on the effective date of this Executive Order, which rules have been duly adopted by the pertinent agencies. Any rules, regulations, and other agency actions affected by the reorganization shall continue in effect and be transferred together with the transfer of functions. If necessary, however, the affected agencies shall propose, adopt, or repeal rules, rule amendments, and rule recodifications as appropriate to effectuate this Executive Order. These rule modifications shall coincide with, if applicable, the transfer of functions to DoIT.

4. Whenever reports or notices are now required to be made or given or paper or documents furnished or served by any person in regard to the functions transferred from an agency to DoIT pursuant to this Executive Order, the same shall be made, given, furnished, or served in the same manner to or upon DoIT.

5. This Executive Order does not contravene, and shall not be construed to contravene, any federal law, State statute (except as provided in Section VI of this Executive Order), or collective bargaining agreement.

IX. PRIOR EXECUTIVE ORDERS

This Executive Order supersedes any contrary provision of any other prior Executive Order, including without limitation Executive Order 1999-05.

X. SEVERABILITY CLAUSE

If any part of this Executive Order is found invalid by a court of competent jurisdiction, the remaining provisions shall remain in full force and effect. The provisions of this Executive Order are severable.

XI. FILINGS

This Executive Order shall be filed with Secretary of State. A copy of this Executive Order shall be delivered to the Secretary of the Senate and to the Clerk of the House of Representatives and, for the purpose of preparing a revisory bill, to the Legislative Reference Bureau.

XII. EFFECTIVE DATE

Provided that neither house of the General Assembly disapproves of this Executive Order by the record vote of a majority of the members elected, this Executive Order shall take effect 60 days after its delivery to the General Assembly.

SIGNED ORIGINAL ON FILE

Bruce Rauner, Governor

Issued by Governor: January 25, 2016
Filed with Secretary of State: January 25, 2016

EXHIBIT A
TO EXECUTIVE ORDER 2016-01

Transferring Agency	Statutes from Which Information Technology Functions Derive
Statutes generally applicable to all or multiple agencies:	5 ILCS 140/1 *et seq.* 5 ILCS 160/1 *et seq.* 20 ILCS 5/1-1 *et seq.* 20 ILCS 5/5-1 *et seq.*, including § 5-645 20 ILCS 450/1 *et seq.* 815 ILCS 530/1 *et seq.*
Capital Development Board	20 ILCS 3105/1 *et seq.*, including § 8
Deaf and Hard of Hearing Commission	20 ILCS 3932/ 1 *et seq.*, including §§ 20, 25
Department of Agriculture	20 ILCS 205/205-1 *et seq.*
Department of Central Management Services	20 ILCS 405/405-1 *et seq.*, including §§ 405-10, 405-20, 405-250, 405-255, 405-260, 405-265, 405-270, 405-272, 405-275 30 ILCS 105/1 et seq., including §§ 5.12, 5.55, 6p-1, 6p-2, 8.16a, 8.16b
Department of Children and Family Services	20 ILCS 505/1 *et seq.*, including § 11
Department of Commerce and Economic Opportunity	20 ILCS 605/605-1 *et seq.*, including § 605-85
Department of Corrections	730 ILCS 5/3-1-1 *et seq.*, including §§ 3-2-5, 3-2-7
Department of Employment Security	20 ILCS 1005/1005-1 *et seq.*
Department of Financial and Professional Regulation	20 ILCS 1205/1 *et seq.* 20 ILCS 2105/2105-1 *et seq.* 20 ILCS 3205/0.1 *et seq.* 20 ILCS 3210/1 *et seq.* Executive Orders 2014-03, 2004-06
Department of Healthcare and Family Services	20 ILCS 2205/2205-1 *et seq.*
Department of Human Rights	775 ILCS 5/1-101 *et seq.*, including § 9-101
Department of Human Services	20 ILCS 1305/1-1 *et seq.*, including §§ 1-20, 1-25
Department of Insurance	20 ILCS 1405/1405-1 *et seq.*, including § 1405-35 Executive Order 2009-04
Department of Juvenile Justice	730 ILCS 5/3-2.5-1 *et seq.*, including § 3-2.5-15
Department of Labor	20 ILCS 1505/1505-1 *et seq.*
Department of Lottery	20 ILCS 1605/1 *et seq.*, including § 9
Department of Military Affairs	20 ILCS 1805/1 *et seq.*
Department of Natural Resources	20 ILCS 801/1-1 *et seq.*, including § 1-15
Department of Public Health	20 ILCS 2305/1.1 *et seq.* 20 ILCS 2310/2310-1 *et seq.*
Department of Revenue	20 ILCS 2505/2505-1 *et seq.*
Department of State Police	20 ILCS 2605/2605-1 *et seq.*
Department of Transportation	20 ILCS 2705/2705-1 *et seq.*
Department of Veterans' Affairs	20 ILCS 2805/0.01 *et seq.*
Department on Aging	20 ILCS 105/1 *et seq.*, including § 4.01 20 ILCS 110/110-5

Transferring Agency	**Statutes from Which Information Technology Functions Derive**
Environmental Protection Agency	415 ILCS 5/1 *et seq.*, including § 4
Governor's Office of Management and Budget	20 ILCS 3005/0.01 *et seq.*, including § 3
Guardianship and Advocacy Commission	20 ILCS 3955/1 *et seq.*, including § 5
Historic Preservation Agency	20 ILCS 3405/1 *et seq.*, including §§ 3, 4, 16
Illinois Arts Council	20 ILCS 3915/0.01 *et seq.*, including § 6
Illinois Council on Developmental Disabilities	20 ILCS 4010/2001 *et seq.*, including § 2007
Illinois Emergency Management Agency	20 ILCS 3305/1 *et seq.*
Illinois Gaming Board	230 ILCS 10/1 *et seq.*, including § 5
Illinois Health Information Exchange Authority	20 ILCS 3860/1 *et seq.*, including §§ 20, 30
Illinois Liquor Control Commission	235 ILCS 5/3-1 *et seq.*, including § 3-4
Illinois Student Assistance Commission	110 ILCS 947/1 *et seq.*, including § 15
Illinois Technology Office	Executive Order 1999-05
Office of the State Fire Marshal	20 ILCS 2905/0.01 *et seq.*
Prisoner Review Board	730 ILCS 5/3-3-1 *et seq.*

Enterprise Resource Planning
(Not Examined)

The Department has been managing the ERP (Enterprise Resource Planning) program for the past year. The ERP will transform finance, human resource, and other administrative systems through the adoption of a single, modern, integrated IT platform, SAP. Three constitutional offices – the executive branch under the Governor, the Office of the Comptroller and the Office of the Treasurer – are participating in this Statewide program.

To maximize adoption and minimize risk, the State is following a phased rollout methodology, with the implementation of the finance, procurement, and grants management modules first. The first set of agencies to go live is expected this fall and will incorporate any implementation lessons learned in three subsequent phases.

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
2015	49	55	(6)
2016	43	40	3
TOTAL	**503**	**258**	**245**

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

1. Capital Development Board
2. Chicago State University
3. Commission on Government Forecasting and Accountability
4. Court of Claims
5. Criminal Justice Information Authority
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 Regulations
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. Eastern Illinois University
29. Emergency Management Agency
30. Environmental Protection Agency
31. Executive Ethics Commission
32. General Assembly Retirement System
33. Governor's Office of Management and Budget
34. Governors State University
35. Guardianship and Advocacy Commission
36. Historic Preservation Agency
37. House of Representatives
38. Human Rights Commission
39. Illinois Arts Council
40. Illinois Board of Higher Education
41. Illinois Civil Service Commission
42. Illinois Commerce Commission
43. Illinois Community College Board

44. Illinois Council on Developmental Disabilities
45. Illinois Deaf and Hard of Hearing Commission
46. Illinois Educational Labor Relations Board
47. Illinois Gaming Board
48. Illinois Health Information Exchange Authority
49. Illinois Housing Development Authority
50. Illinois Independent Tax Tribunal
51. Illinois Labor Relations Board
52. Illinois Law Enforcement Training and Standards Board
53. Illinois Math and Science Academy
54. Illinois Power Agency
55. Illinois Prisoner Review Board
56. Illinois Procurement Policy Board
57. Illinois Racing Board
58. Illinois State Board of Investments
59. Illinois State Police
60. Illinois State Toll Highway Authority
61. Illinois State University
62. Illinois Student Assistance Commission
63. Illinois Workers' Compensation Commission
64. Joint Committee on Administrative Rules
65. Judges' Retirement System
66. Judicial Inquiry Board
67. Legislative Audit Commission
68. Legislative Ethics Commission
69. Legislative Information System
70. Legislative Printing Unit
71. Legislative Reference Bureau
72. Legislative Research Unit
73. Northeastern Illinois University
74. Northern Illinois University
75. Office of the Architect of the Capitol
76. Office of the Attorney General
77. Office of the Auditor General
78. Office of the Comptroller
79. Office of the Executive Inspector General
80. Office of the Governor
81. Office of the Legislative Inspector General
82. Office of the Lieutenant Governor
83. Office of the Secretary of State
84. Office of the State's Attorneys Appellate Prosecutor
85. Office of the State Appellate Defender
86. Office of the State Fire Marshal
87. Office of the Treasurer
88. Property Tax Appeal Board
89. Senate Operations

90. Southern Illinois University
91. State Board of Education
92. State Board of Elections
93. State Charter School Advisory Commission
94. State Employees' Retirement System
95. State of Illinois Comprehensive Health Insurance Board
96. State Police Merit Board
97. State Universities Civil Service System
98. State Universities Retirement System
99. Supreme Court Historic Preservation Commission
100. Supreme Court of Illinois
101. Teachers' Retirement System of the State of Illinois
102. University of Illinois
103. Western Illinois University

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

1. Capital Development Board
2. Criminal Justice Information Authority
3. Department of Agriculture
4. Department of Central Management Services
5. Department of Corrections
6. Department of Financial and Professional Regulations
7. Department of Human Rights
8. Department of Insurance
9. Department of Juvenile Justice
10. Department of Labor
11. Department of Lottery
12. Department of Military Affairs
13. Department of Natural Resources
14. Department of Public Health
15. Department of Revenue
16. Department on Aging
17. Department of Veterans' Affairs
18. Emergency Management Agency
19. Environmental Protection Agency
20. General Assembly Retirement System
21. Governor's Office of Management and Budget
22. Guardianship and Advocacy Commission
23. Human Rights Commission
24. Illinois Arts Council
25. Illinois Board of Higher Education
26. Illinois Civil Service Commission
27. Illinois Commerce Commission
28. Illinois Community College Board
29. Illinois Council on Developmental Disabilities
30. Illinois Deaf and Hard of Hearing Commission
31. Illinois Educational Labor Relations Board
32. Illinois Gaming Board
33. Illinois Labor Relations Board
34. Illinois Law Enforcement Training and Standards Board
35. Illinois Prisoner Review Board
36. Illinois Procurement Policy Board
37. Illinois Racing Board
38. Illinois State Police
39. Illinois Student Assistance Commission
40. Illinois Workers' Compensation Commission
41. Judges' Retirement System
42. Judicial Inquiry Board
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's Attorneys Appellate Prosecutor
49. Office of the State Appellate Defender
50. Office of the State Fire Marshal
51. Property Tax Appeal Board
52. State Board of Education
53. State Board of Elections
54. State Employees' Retirement System
55. State Police Merit Board
56. State Universities Civil Service System
57. Supreme Court Historic Preservation Commission
58. 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. Governor’s Office of Management and Budget
14. Historic Preservation Agency
15. Illinois Deaf and Hard of Hearing Commission
16. Illinois Law Enforcement Training and Standards Board
17. Office of the Attorney General
18. Office of the Governor
19. Office of the Lieutenant Governor
20. Office of the State’s Attorneys Appellate Prosecutor

Listing of User Agencies of the Central Payroll System
(Not Examined)

1. Capital Development Board
2. Commission on Government Forecasting and Accountability
3. Court of Claims
4. Criminal Justice Information Authority
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 Regulations
11. Department of Human Rights
12. Department of Insurance
13. Department of Juvenile Justice
14. Department of Labor
15. Department of 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. Emergency Management Agency
22. Environmental Protection Agency
23. Executive Ethics Commission
24. Governor's Office of Management and Budget
25. Guardianship and Advocacy Commission
26. Historic Preservation Agency
27. House of Representatives
28. Human Rights Commission
29. Illinois Arts Council
30. Illinois Board of Higher Education
31. Illinois Civil Service Commission
32. Illinois Commerce Commission
33. Illinois Community College Board
34. Illinois Council on Developmental Disabilities
35. Illinois Deaf and Hard of Hearing Commission
36. Illinois Educational Labor Relations Board
37. Illinois Gaming Board
38. Illinois Health Information Exchange Authority
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 Power Agency

Provided by the Department of Central Management Services

44. Illinois Prisoner Review Board
45. Illinois Procurement Policy Board
46. Illinois Racing Board
47. Illinois State Board of Investments
48. Illinois State Police
49. Illinois Student Assistance Commission
50. Illinois Workers’ Compensation Commission
51. Joint Committee on Administrative Rules
52. Judges' Retirement System
53. Judicial Inquiry Board
54. Legislative Audit Commission
55. Legislative Ethics Commission
56. Legislative Information System
57. Legislative Printing Unit
58. Legislative Reference Bureau
59. Legislative Research Unit
60. Office of the Architect of the Capitol
61. Office of the Attorney General
62. Office of the Auditor General
63. Office of the Executive Inspector General
64. Office of the Governor
65. Office of the Lieutenant Governor
66. Office of the State’s Attorneys Appellate Prosecutor
67. Office of the State Appellate Defender
68. Office of the State Fire Marshal
69. Office of the Treasurer
70. Property Tax Appeal Board
71. Senate Operations
72. State Board of Education
73. State Board of Elections
74. State Employees’ Retirement System
75. State of Illinois Comprehensive Health Insurance Board
76. State Police Merit Board
77. State Universities Civil Service System
78. Supreme Court Historic Preservation Commission
79. Teachers’ Retirement System of the State of Illinois

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

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

1. Capital Development Board
2. Criminal Justice Information Authority
3. Department of Agriculture
4. Department of Central Management Services
5. Department of Commerce and Economic Opportunity
6. Department of Financial and Professional Regulations
7. Department of Human Rights
8. Department of Insurance
9. Department of Labor
10. Department of Lottery
11. Department of Public Health
12. Department of Revenue
13. Department on Aging
14. Executive Ethics Commission
15. Guardianship and Advocacy Commission
16. Illinois Deaf and Hard of Hearing Commission
17. Illinois Heath Information Exchange Authority
18. Illinois Prisoner Review Board
19. Illinois Procurement Policy Board
20. Illinois Racing Board
21. Illinois State Police
22. Illinois Workers' Compensation Commission
23. Office of the Executive Inspector General
24. Office of the Lieutenant Governor
25. Property Tax Appeal Board
26. State of Illinois Comprehensive Health Insurance Board
27. State Employees' Retirement System

Provided by the Department of Central Management Services

Listing of Security Software Proxy Agencies
(Not Examined)

1. Capital Development Board
2. Chicago State University
3. Court of Claims
4. Criminal Justice Information Authority
5. Department of Agriculture
6. Department of Central Management Services
7. Department of Corrections
8. Department of Human Rights
9. Department of Labor
10. Department of Military Affairs
11. Department of Veterans' Affairs
12. Eastern Illinois University
13. Emergency Management Agency
14. Executive Ethics Commission
15. Governor's Office of Management and Budget
16. Governors State University
17. Guardianship and Advocacy Commission
18. House of Representatives
19. Historic Preservation Agency
20. Human Rights Commission
21. Illinois Arts Council
22. Illinois Civil Service Commission
23. Illinois Commerce Commission
24. Illinois Community College Board
25. Illinois Council on Developmental Disabilities
26. Illinois Deaf and Hard of Hearing Commission
27. Illinois Educational Labor Relations Board
28. Illinois Health Information Exchange Authority
29. Illinois Housing Development Authority
30. Illinois Independent Tax Tribunal
31. Illinois Labor Relations Board
32. Illinois Law Enforcement Training and Standards Board
33. Illinois Math and Science Academy
34. Illinois Power Agency
35. Illinois Prisoner Review Board
36. Illinois Procurement Policy Board
37. Illinois State Board of Investments
38. Illinois State Toll Highway Authority
39. Illinois State University
40. Joint Committee on Administrative Rules
41. Judicial Inquiry Board
42. Legislative Audit Commission
43. Legislative Ethics Commission

44. Legislative Information System
45. Legislative Printing Unit
46. Legislative Reference Bureau
47. Legislative Research Unit
48. Northeastern Illinois University
49. Northern Illinois University
50. Office of the Architect of the Capitol
51. Office of the Attorney General
52. Office of the Comptroller
53. Office of the Executive Inspector General
54. Office of the Governor
55. Office of the Legislative Inspector General
56. Office of the Lieutenant Governor
57. Office of the Secretary of State
58. Office of the State’s Attorneys Appellate Prosecutor
59. Office of the State Appellate Defender
60. Office of the State Fire Marshal
61. Office of the Treasurer
62. Property Tax Appeal Board
63. Senate Operations
64. Southern Illinois University
65. State Board of Education
66. State Board of Elections
67. State of Illinois Comprehensive Health Insurance Board
68. State Police Merit Board
69. State Universities Civil Service System
70. State Universities Retirement System
71. University of Illinois
72. Western Illinois University

ACRONYM GLOSSARY

ACL – Access Control List
AD – Active Directory
ADC – Alternate Data Center
AIS – Accounting Information System
BCCS – Bureau of Communications and Computer Services
BIM – Identity Management Solution
Bureau – Bureau of Communications and Computer Services
CAC – Change Advisory Committee
CCF – Central Computer Facility
CFO – Chief Fiscal Officer
CICS – Customer Information Control System
CIO – Chief Information Officer
CIS – Central Inventory System
CISO – Chief Information Security Officer
CMC – Communications Management Center
CMS – Central Management Services
CPS – Central Payroll System
CPU – Central Processing Unit
CSC – Customer Solution Center
CTAS – Central Time and Attendance
DB2 – Database 2
DCMS – Department of Central Management Services
Department – Department of Central Management Services
DHCP – Dynamic Host Configuration Protocol
DHFS – Department of Healthcare and Family Services
DHS – Department of Human Services
DLM – Disk Library Management
DMVPN – Dynamic Multiple Virtual Private Network
DNS – Domain Name Service
DOT – Department of Transportation
DPH – Department of Public Health
DWDM – Dense Wavelength Division Multiplexing
EAA – Enterprise Application & Architecture
ECM – Enterprise Change Management
EPM – Enterprise Program Management
ESR – Enterprise Service Request
EUC – End User Computing
FIM – Forefront Identity Management Solution
FY – Fiscal Year
HSM – Hierarchical Storage Management
ICN – Illinois Century Network
ID – Identification
ISD – Infrastructure Services Division
ILA – In-Line Amplication

ILCS – Illinois Compiled Statutes
IMS – Information Management System
IP – Internet Protocol
IT – Information Technology
ITG – Information Technology Governance
LAN – Local Area Network
MORT – Major Outage Response Team
NBD – Next Business Day
NCM – Network Configuration Manager
NIST– National Institute of Standards and Technology
PAR – Personnel Action Request
PIR – Post Implementation Review
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
SAMS – Statewide Accounting Management System
SNMP – Simple Network Management Protocol
SMF – Simple Machine Forms
TSM – Tivoli Storage Management
UPS – Uninterruptible Power Supply
VPN – Virtual Private Network
WAN – Wide Area Network
z/OS – Zero Downtime Operating System
z/VM – Zero Downtime Virtual Machine