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, 2015

WILLIAM G. HOLLAND

AUDITOR GENERAL

SERVICE ORGANIZATION CONTROL REPORT

Department of Central Management Services
Bureau of Communications and
Computer Services

TABLE OF CONTENTS

CMS

ILLINOIS Bruce Rauner, Governor

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES

Tom Tyrrell, Director

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, 2014 to June 30, 2015

July 20, 2015

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

We have prepared the attached description titled "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' State of Illinois Mainframe Information Technology Environment System Throughout the Period July 1, 2014 to June 30, 2015" (the description), based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system in paragraphs 1.34-.35 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the State of Illinois Mainframe Information Technology Environment, particularly system controls intended to meet the criteria for the security, availability, and processing integrity principles set forth in the TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*)(applicable trust services criteria). We confirm, to the best of our knowledge and belief, that:

a. the description fairly presents the system throughout the period July 1, 2014 through June 30, 2015, based on the following description criteria:
    i. The description contains the following information:
        (1) The types of services provided
        (2) The components of the system used to provide the services, which are the following:
        - *Infrastructure.* The physical and hardware components of a system (facilities, equipment, and networks).
        - *Software.* The programs and operating software of a system (systems, applications, and utilities).
        - *People.* The personnel involved in the operation and use of a system (developers, operators, users, and managers).

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

(3) The boundaries or aspects of the system covered by the description and the service auditor's report.

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

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

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

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

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

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

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

(11) Relevant details of changes to 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. The controls stated in the description were suitably designed throughout the specific period to meet the applicable trust service criteria.
c. Except for the matters described in the following paragraph, the controls stated in the description operated effectively throughout the specified period to meet the applicable trust service criteria.

As noted on pages 8 and 9, controls related to:

1. For a user requiring 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, the Department does not require an email or problem report to be submitted for Active Directory password resets. As a result, the control over the reset of Active Directory passwords was not operating effectively to meet the criterion "Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them."
2. 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. As a result, the controls over the reset of mainframe passwords were not operating effectively to meet the criterion "Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them."
3. The Department's Compliance Officer is responsible for monitoring and ensuring compliance with policies and procedures. However, monitoring for compliance had not been conducted. As a result, the control over the monitoring of compliance with policies and procedures was not operating effectively to meet 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."
4. The Department is to conduct periodic risk assessments, which identify threats and vulnerabilities, and assess the impact. In addition, the Department is to remediate identified risks to an acceptable level. A limited scope risk assessment related to the availability of specific applications in the event of an unplanned outage had been conducted by a third party vendor; however, the Department had not completed any other risk assessments. In addition, the Department had not developed a corrective action plan related to the risks identified by the vendor. As a result, the controls over risk assessments were not operating effectively to meet the criterion "The Department (1) identifies potential threats that would impair system security, availability, and processing integrity commitments and requirements, (2) analyzes the significance of

risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies), the Department designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy, and 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."

5. Department staff and users are instructed to contact the Help Desk or their supervisor to report any and all security, availability and processing issues. Staff and users may contact the Help Desk via phone or email to report an incident. When a report is received, the Help Desk staff opens a ticket in Remedy and records the incident, as well as the user name, agency, contact information and a detailed incident description. The ticket is tracked through Remedy until resolution. However, the Department did not provide the auditor detailed documentation in order for procedures to be performed. As a result, the control over security, availability and processing issues was not operating effectively to meet the criterion "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."
6. The Security Compliance Solution and Infrastructure Services are responsible for monitoring IT network resources and when issues are identified, appropriate units are contacted for remediation. However, the Department did not provide the auditor information on tools or reports in order for procedures to be performed. As result, the control over monitoring IT network resources was not operating effectively to meet the criterion "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."
7. 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.

Sincerely,

HBhatt

Hardik Bhatt Chief Information Officer/Deputy
Director State of Illinois, Office of the Governor

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

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

Office Of The Auditor General
William G. Holland

INDEPENDENT SERVICE AUDITOR'S REPORT

The Honorable William G. Holland
Auditor General State of Illinois

Scope

We have examined the attached Description titled "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' State of Illinois Mainframe Information Technology Environment System Throughout the Period July 1, 2014 to June 30, 2015" (the Description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the security, availability, and processing integrity principles set forth in the TSP Section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), throughout the period July 1, 2014 to June 30, 2015. 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 service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-agency controls.

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

Service organization's responsibilities
The Department of Central Management Services, Bureau of Communications and Computer Services has provided the attached assertion titled "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' Assertion Regarding the State of Illinois Mainframe Information Technology Environment System Throughout the Period July 1, 2014 to June 30, 2015", which is based on the criteria identified in management's assertion. The Department of Central Management Services, Bureau of Communications and Computer Services is responsible for (1) preparing the Description and assertion; (2) the completeness, accuracy, and method of presentation of both the Description and assertion; (3) providing the services covered by the Description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the Description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the Description based on the Description criteria set forth in the Department of Central Management Services, Bureau of Communications and Computer Services' assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants and the standards applicable to attestation engagements contained in Government Auditing Standards issued by the Comptroller General. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is fairly presented based on the Description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period July 1, 2014 to June 30, 2015.

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

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

Opinion
The Department of Central Management Services, Bureau of Communications and Computer Services states in the Description that in 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 page 63 of the Description of Tests of Controls and Results Thereof, the Department does 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, 2014 to June 30, 2015. This control deficiency resulted in not meeting the criterion "Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them."

The Department of Central Management Services, Bureau of Communications and Computer Services 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 page 63 of the Description of Tests of Controls and Results Thereof, 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. Thus, the control over the reset of mainframe passwords was not operating effectively throughout the period July 1, 2014 to June 30, 2015. This control deficiency resulted in not meeting the criterion "Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them."

The Department of Central Management Services, Bureau of Communications and Computer Services states in the Description that the Department's Compliance Officer is responsible for monitoring and ensuring compliance with policies and procedures. However, as noted on page 46 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, 2014 to June 30, 2015. This control deficiency resulted in not meeting the criterion "The Department has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security, availability, and processing integrity."

The Department of Central Management Services, Bureau of Communications and Computer Services also states in the Description that the Department is to conduct periodic risk assessments, which identify threats and vulnerabilities, and assess the impact. In addition, the Department is to remediate identified risks to an acceptable level. However, as noted on pages 52, 53, and 54 of the Description of Tests of Controls and Results Thereof, a limited scope risk assessment related to the availability of specific applications in the event of an unplanned outage had been conducted by a third party vendor; however, the Department had not completed any other risk assessments. In addition, the Department had not developed a corrective action plan related to the risks identified by the vendor. Thus, the control over risk assessments was not operating effectively throughout the period July 1, 2014 to June 30, 2015. This control deficiency resulted in not meeting the criterion "The Department (1) identifies potential threats that would impair system security, availability, and processing integrity commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies), the Department designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy, and 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 of Central Management Services, Bureau of Communications and Computer Services states in the Description that Department staff and users are instructed to contact the Help Desk or their supervisor to report any and all security, availability and processing issues. Staff and users may contact the Help Desk via phone or email to report an incident. When a report is received, the Help Desk staff opens a ticket in Remedy and records the incident, as well as the user name, agency, contact information and a detailed incident description. The ticket is tracked through Remedy until resolution. However, as noted on page 78 of the Description of Tests of Controls and Results Thereof, the Department did not provide the auditor detailed documentation in order for procedures to be performed to evaluate the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the control. Thus, the control over security, availability and processing issues was not operating effectively throughout the period July 1, 2014 to June 30, 2015. This control deficiency resulted in not meeting the criterion "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."

In addition, the Department of Central Management Services, Bureau of Communications and Computer Services also states in the Description that the Security Compliance Solution and Infrastructure Services are responsible for monitoring IT network resources and when issues are identified, appropriate units are contacted for remediation. However, as noted on pages 75 and 76 of the Description of Tests of Controls and Results Thereof, the Department did not provide the auditor information on tools or reports in order for procedures to be performed to evaluate the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the control. Thus, the control over monitoring IT network resources was not operating effectively throughout the period July 1, 2014 to June 30, 2015. This control deficiency resulted in not meeting the criterion "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."

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

a. the Description fairly presents the system that was designed and implemented throughout the period July 1, 2014 to June 30, 2015.

b. the controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period July 1, 2014 to June 30, 2015, the subservice organization applied, the types of controls expected to be implemented at the subservice organization and incorporated in the design of the system, and user-agencies applied the complementary user-agency controls contemplated in the design of the Department of Central Management Services, Bureau of Communications and Computer Services' controls throughout the period July 1, 2014 to June 30, 2015.

c. the controls tested, which together with the types of controls expected to be implemented at the subservice organization and incorporated in the design of the system, and the complementary user-agency controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period July 1, 2014 to June 30, 2015.

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

Controls Did Not Operate During the Period Covered by the Report
As indicated on pages 71, 72, 76, 89,90, 94, and 95 of the Department of Central Management Services, Bureau of Communications and Computer Services' Description, the Department did not encounter any failed backups during the period July 1, 2014 to June 30, 2015; 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."

Other Information Provided by the Department of Central Management Service, Bureau of Communications and Computer Services That is Not Covered by the Service Auditors' Report
The information attached to the Description titled "Other Information Provided by the Department of Central Management Services, Bureau of Communications and Computer Services That Is Not Covered by the Service Auditor's Report" describes staffing trends, user agency listings, and the Department's Corrective Action Plan. It is presented by the management of the Department of Central Management Services, Bureau of Communications and Computer Services to provide additional information and is not a part of the Department of Central Management Services, Bureau of Communications and Computer Services' Description of the State of Illinois Mainframe Information Technology Environment System made available to user-agencies during the period from July 1, 2014 to June 30, 2015. Information about the Department of Central Management Services, Bureau of Communications and Computer Services' staffing issues, user listings, and Department's Corrective Action Plan have not been

subjected to the procedures applied in the examination of the Description of the State of Illinois Mainframe Information Technology Environment System and the suitability of the design and operating effectiveness of controls to meet the related criteria stated in the Description of the State of Illinois Mainframe Information Technology Environment System, and, accordingly, we express no opinion on it.

Other Information Provided by the Service Auditor That is Not Covered by the Service Auditor's Report

The information attached to the Description titled "Other Information Provided by the Auditors That Is Not Covered by the Service Auditor's Report" provides additional information in regards to the Description of the Department's mainframe capacity and information not provided during the audit provides additional information and is not a part of the Department of Central Management Services, Bureau of Communications and Computer Services' Description of the State of Illinois Mainframe Information Technology Environment System made available to user-agencies during the period from July 1, 2014 to June 30, 2015. Information about the Department's mainframe capacity and information not provided during the audit have not been subjected to the procedures applied in the examination of the Description of the State of Illinois Mainframe Information Technology Environment System and the suitability of the design and operating effectiveness of controls to meet the related criteria stated in the Description of the State of Illinois Mainframe Information Technology Environment System, and, accordingly, we express no opinion on it.

Intended use

This report and the Description of Tests of Controls and Results Thereof are intended solely for the information and use of the Department of Central Management Services, Bureau of Communications and Computer Services' user-agencies of the "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' State of Illinois Mainframe Information Technology Environment System" during some or all of the period July 1, 2014 to June 30, 2015, the Auditor General, the General Assembly, the Legislative Audit Commission, the Governor, and independent auditors and practitioners providing services to such user-agencies, and regulators who have sufficient knowledge and understanding of the following:

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

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

William J. Sampias, CISA
Director, Information Systems Audits

Mary Kathryn Lovejoy, CPA, CISA
Audit Manager

July 20, 2015
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, 2014 TO JUNE 30, 2015

Background

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

The Bureau of Communications and Computer Services:

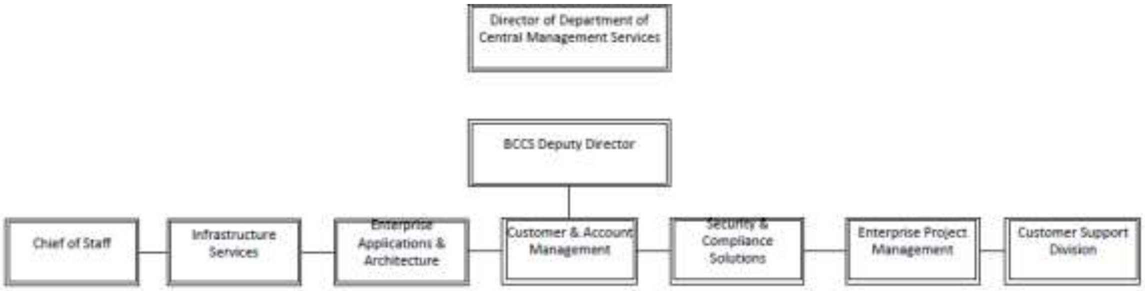
- Manages the planning, procurement, maintenance, and delivery of voice, data, wireless, video, Internet, and telecommunications services to all state government agencies, boards, commissions, and state supported institutions of higher education in Illinois, as well as other governmental and some non-governmental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

Management Philosophy

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

Organization and Management

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


Director of Department of Central Management Services
BCCS Deputy Director
Chief of Staff
Infrastructure Services
Enterprise Applications & Architecture
Customer & Account Management
Security & Compliance Solutions
Enterprise Project Management
Customer Support Division

Deputy Director

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

Chief Operating Officer

The Chief Operating Officer serves as a policy formulating administrator in planning, directing, implementing and administering the Customer and Account Management group. The Customer and Account Management group is responsible for the telecommunications and network services operations.

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

- Field Operations / Regional Technology Centers (RTC)
  Field Operations is responsible for maintaining nine Regional Technology Centers located throughout the State and assisting Network Services in maintaining Illinois Century Network Point-of-Presence (POP) sites throughout the State. Field Operations staff works directly with customers of the network providing a range of services including WAN consultation and design, sales and billing, on-site installation and repair, and ongoing tier II technical support. Field Operations staff manages customers' Domain Name Service (DNS), content filtering, bandwidth utilization reports, and customer records. Customers include State agencies, colleges and universities, K12 schools, libraries, museums, and local municipalities.

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

  - Network Operations is responsible for installing, maintaining and managing the ICN Backbone, including the State's owned and leased fiber optic infrastructure, optical equipment, routers, firewalls, switches, Point-of-Presence (POP) sites, WAN monitoring tools and WAN services.

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

  - Enterprise Network Support is responsible for design and support of State agencies network access. Responsibilities include installation and support of access routers, Wide Area Network (WAN) switches, capital complex fiber, Domain Name Service (DNS), and Internet. Enterprise Network Support also performs tier III technical support for the Customer Management Service (CMC) and directly to state agencies.

Chief of Staff

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

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

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

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

Chief Technology Officer

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

- Data Center Operations
  - Mainframe Services is responsible for the mainframe operating systems, database systems, and software installation, maintenance, and support function/services.
  - Enterprise Storage and Backup is responsible for the oversight and management of the storage and backup systems across all platforms.

Midrange Services is responsible for the midrange operating systems, database systems, software installation, hardware installation, maintenance, desktop/laptop/midrange server anti-virus, and support function/services.

- Enterprise Production/Data Center Operations
    - Library Services is responsible for the change management process for migration of mainframe application programs to the production environment. 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 Department's 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.

    - Midrange I/O Services is responsible for scheduling, initiating, monitoring and error resolution of the nightly and weekend processing for the midrange platform.

    - Mainframe Backup and Monitoring is responsible for control and scheduling 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:(1) weekly for full system and subsystem volume backups; (2) daily for incremental system and subsystem volume backups. They are responsible for control and monitoring of available storage levels.

- Customer Administration & Software Distribution
    - Customer Administration & Support is responsible for information technology active directory content related but not limited to accounts, groups, organizational units (OU), folders, printers, and PCs.

    - Software Distribution provides the automation of the deployment, patching, upgrading, and removal of software applications without physically visiting each desktop or laptop.

- Customer Service Center (CSC)
  The CSC serves as a central point of contact for requesting new services or to report a problem encountered with existing support services. CSC processes and manages telecommunications and networking service requests and incidents, procedures and manages telecommunication vendor performance.

- End User Support Service
  End User Support supports the configuration, installation, internet connectivity, maintenance, troubleshooting, break/fix and upgrades of personal computers.

Chief Information Security Officer

The Chief Information Security Officer serves as a policy making official responsible for policy development, planning, implementation, and administration of the Security and Compliance Solutions division. The Chief Information Security Officer is responsible for overseeing and implementing the sensitive and confidential Information Technology security program for agencies, boards and commissions under the jurisdiction of the Governor.

- Security and Compliance Solutions (S&CS)
  Security and Compliance Solutions has the following responsibilities:
    - Providing the IT security program statewide to agencies;
    - Communicating security principles through issuance of policies and hosting education opportunities;
    - Alerting users to known occurrences or potential imminent threats that could cause risk to cyber resources;
    - Notifying the applicable management of non-compliance/violations of the systems security;
    - Developing and assessing risk associated with specific business information systems and developing appropriate remediation plans;
    - Conducting security testing of the infrastructure; and
    - Developing and maintaining the statewide disaster recovery services for the State's Information Technology infrastructure.

Enterprise Applications and Architecture

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

Department management reviews the organizational structures and staffing vacancies at their weekly management meetings.

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

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

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

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

New Department staff 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.

Communication

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

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

The Department has posted the following policies on their website.

Information Technology Policies

- Data Classification Policy;
- Enterprise Desktop/Laptop Policy;
- General Security for Statewide IT Resources Policy;
- General Security for Statewide Network Resources Policy;
- IT (Information Technology) Recovery Policy;
- Recovery Methodology;
- IT Resource Access Policy;
- Laptop Data Encryption Policy;
- Backup Retention Policy;
- Statewide CMS/BCCS Facility Access Policy; and
- IT (Information Technology) Risk Assessment Policy.

General Policies

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

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

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

Risk Management

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

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

Monitoring

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

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

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

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

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

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

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

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

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

Logical and Physical Environment

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

- The primary operating systems:
    - Zero Downtime Operating System (z/OS). z/OS is a complex operating system used on mainframes and functions as the system software that controls the initiation and processing of work within the computer.
    - z/Virtual Machine (z/VM) is a time-sharing, interactive, multi-programming operating system.

- The primary subsystems:
    - The Customer Information Control System (CICS) is a software product that enables online transaction processing. CICS allows numerous transaction types, entered from multiple terminals, to be processed concurrently by user written application programs. CICS acts as an interface between the operating system and application programs.
    - DataBase 2 (DB2) is a relational database management system for z/OS environments.
    - Information Management System (IMS), which is an online database software subsystem, is used as the control architecture under which online database system applications process. An IMS system is capable of running many different applications within a single definition of one or more "Message Processing Region" and one "Control Region".

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

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

There are two individuals primarily responsible for the security, administration and support;

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

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

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

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

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

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

In order for the Security Software Coordinator or the Security Software Administrator for CMS/BCCS/S&CS to create an ID 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 ID, the Chief Information Security Officer is required to approve the Mainframe Security Request Form.

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

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

In the event a user requires their password to be reset, they contact the Help Desk via email, submit a problem report or utilize the BCCS Identity Management (BIM) Solution.

In the event the user does not utilize the Department's BIM to reset their 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, ID, and a phone number to be contacted. The Help Desk staff will contact the user at the number given, reset the 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 RACF password, an ESR will be assigned to the Security Software Coordinator or the Security Software Administrator for CMS/BCCS/S&CS in order to reset the password. Upon receipt, the Security Software Coordinator or the Security Software Administrator for CMS/BCCS/S&CS will reset the password with a temporary password and phone the individual.

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

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

The Department also maintains the State of Illinois Statewide Network, which consists of firewalls, routers and switches. Network Operations, Regional Technology Offices, and Enterprise Network Support are primarily responsible for networking equipment at the core, distribution, and access levels; while LAN Services is primarily responsible for networking equipment at the Data Centers and LAN infrastructure at supported agencies.

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

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

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

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

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

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

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

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

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

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

SolarWinds Network Configuration Manager (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.

The Department has implemented network monitoring tools that allow the Technical Safeguards Unit, LAN Services, and Network Services to monitor inbound and outbound network traffic. The monitoring tools are used to detect and defend against malicious worms, Trojans, malware, viruses as well as to investigate possible security breach, identify sources of attacks, and ensure conformance to CMS/BCCS IT policies, and monitor system and user activities where appropriate.

NetScout provide multiple functions and include historic and real time packet analysis for problem determination, and real time alerting. Whereas, QRadar includes incident response, reviewing logs, web Log analysis and vulnerability analysis.

Authorized staff from the Technical Safeguards Unit, LAN Services, and Network Services monitors system logs and email the appropriate divisions of the enterprise to investigate or remediate identified security risks.

Communication of identified incident may include the following enterprise divisions:

- CMS/BCCS Infrastructure Services and Network Services may be contacted to thoroughly investigate the incident.

- Appropriate law enforcement may be contacted as applicable.
- CMS/BCCS will work to identify the threat source and extent of damages, virus activity, network attack, insider fraud, or account compromise.
- CMS/BCCS Midrange Computing and Network Services may be contacted to isolate the affected system(s)

Department staff and users are instructed to contact the Help Desk, who will distribute incidents to the proper IT support group using the Remedy System. Staff and users may contact the Help Desk via phone or email to report an incident.

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

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

Cisco equipment availability is maintained by either a SMARTnet 4-hour coverage or a combination of Next Business Day (NBD) coverage and hardware sparing depending on the criticality of the equipment. 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 the State. SMARTnet does not cover equipment which has reached End-of-Support.

The State's fiber optic wave transmission system operates on Fujitsu DWDM equipment. This equipment is maintained through an element based maintenance plan from Fujitsu. Each node is an element and all cards are covered that are in the chassis. As with the Cisco maintenance plan, this approach also includes replacement and sparing based on equipment criticality.

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

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

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

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

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

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

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

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

Agencies are responsible for submitting an ESR 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.

In order to access the Department's environment, the user is required to have a user ID and password. To obtain an ID, the agency's IT Coordinator submits a completed and approved Enterprise Service Request 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, they contact the Help Desk via email, submit a problem report or utilize one of the Department's two Self-Service Solutions: BCCS Identity Management (BIM) Solution or the Forefront Identity Manager (FIM) Solution.

In the event the user does not utilize the Department's one of the Solutions to reset their 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, ID, and a phone number to be contacted. The Help Desk staff will contact the user at the number given, reset the 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.

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

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

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

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

Additionally, security alarms have been placed throughout the facilities. If an alarm is triggered, an alert 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 of employment, the Exit Form is sent to the employee'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 employees who forget their badge, are required to sign-in and register with security guards to gain access to the facilities. The security guard on duty receives the individual's driver's license for authorization with the Hirsch Velocity System. Once reviewed, the security guard provides a badge based on the individual's access rights. Visitors are provided a visitor badge, which will not allow access, and must be escorted by an authorized individual.

The Department has installed preventive environmental measures at the facilities:

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

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

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

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

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

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 personnel at the guard's desk or the loading dock. At that time, the agency personnel must provide appropriate identification. The print shop staff then verifies their authorization via the Focal system. Upon verification, the agency personnel sign the Report Distribution Checklist.

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

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

Change Control

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

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

The level of approval is dependent upon the impact of the change. Transparent changes are low impact changes which have little to no impact and are required to be approved by Group Managers. Medium and high impact changes are changes which may have an impact on the environment or 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 by each division.

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

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

A post implementation review is required for changes which causes 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. All 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 will be managed via the EPM Portal and the Application Life cycle Management Methodology.

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

The Library Services Group is responsible for moving mainframe application changes into production for DHS, DCMS, DHFS, and 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 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. If the move is scheduled via Pan Apt, an authorization email is not required. Security software controls who has access to schedule.

The Department utilizes a set of administrative processes, driven by principles, and sponsored by Enterprise leaders to ensure that IT/Telecom investments align with business objectives, architecture standards, and Enterprise goals to prevent duplicate solutions, re-use or extend current solutions, optimize use of resources, and manage related risks.

Enterprise IT Governance process is required for state agency initiatives with a sponsor, budget, defined scope, and estimated start/end dates that are related to improvement efforts or implementation of a new system, technology, process or service.

An agency submits a Project Charter, Business Requirements, and Technical Requirements. The documents solicit information related to the design, acquisition, implementation, configuration, system availability/recovery requirements, and security requirements for the initiative.

The IT Governance Administrator meets with EA&S representatives to review, assess, and approve submitted project documentation, coordinating with domain owners and subject matter experts as necessary. Agency contacts are notified by email of a Project Charter approval. Governance documentation and approvals are maintained in the EPM Portal.

A three gate approach is used to review the project for relative alignment. The Project Charter document is reviewed for approval through Gate 1. Business Requirements and Technical Requirements are reviewed for approval through Gate 2. Upon Gate 2 approval, the Agency may begin the technical design and solicit vendor proposals. Governance staff defines a project Deployment Scope statement and provides it for Agency approval or modification until finalized for approval through Gate 3. Upon Gate 3 approval, the Agency may acquire the solution and begin related development and testing.

Backup and Restoration

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

The Mainframe Storage team uses CA-Scheduler to control and schedule backups. All 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.

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

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 Virtual Tape Disk library for the Mainframe (DLM) between the CCF and the ADC. The logs tracks library replication outcomes for DLM replicated activate. 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 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 entered if an agency requires additional storage.

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

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

The Department conducts a comprehensive test of the Category One, Stage Zero applications/data on an annual basis. In addition, the Department tests the DCMS/BCCS Infrastructure Services Recovery Activation Plan during the annual test 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; access, approve transactions, modify and delete transactions.

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

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

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

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

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

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

BOUNDARIES OF THE SYSTEM

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

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

TRUST SERVICES CRITERIA AND RELATED CONTROLS

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

COMPLEMENTARY USER-AGENCY CONTROLS

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

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

- User agencies have reviewed and adhere to the security polices located on the Department's website;
- User agencies have communicated to the Department their specific security requirements;
- User agencies have 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 bi-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, designated application information updates to the Business Reference Model, recovery exercise procedures and schedules, and ongoing communications with the Department.

This page intentionally left blank

TESTS OF OPERATING EFFECTIVENESS

Our tests of the operational effectiveness of controls were designed to cover a representative number of processes throughout the period of July 1, 2014 through June 30, 2015, for each of the controls, which are designed to achieve the applicable trust services criteria. In selecting particular tests of the operational 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**
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.

This page intentionally left blank

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

	Criteria	Department's Control	Testing Performed	Results
CC1.0	**Common Criteria Related to Organization and Management**			
CC1.1	The Department has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they relate to security, availability, and processing integrity.	Each position is to have a position description which outlines the duties and qualifications.	Reviewed a sample of positions to determine if 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.
		Department management reviews the organizational structures and staffing vacancies at their weekly meetings.	Interviewed Acting Chief Information Security Officer.	Department management reviews the organizational structure and staffing vacancies at their weekly management meetings; however, minutes are not maintained.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the Department's system controls are assigned to individuals within the Department with authority to ensure policies and other system requirements are effectively promulgated and placed in operation.	Each position is to have a position description which outlines the duties and qualifications.	Reviewed a sample of positions to determine if position descriptions had been completed.	No deviation noted.
			Reviewed the position descriptions to determine if they outlined the duties and qualifications.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
CC1.3	Personnel responsible for designing, developing, implementing, operating, maintaining and monitoring the system affecting security, availability, and processing integrity have the qualifications and resources to fulfill their responsibilities.	The Department adheres to the State's hiring procedures; Personnel Code, Union Contracts and Rutan decisions, for the hiring of staff.	Reviewed the hiring procedures; Personnel Code, Union Contract, and Rutan decisions.	No deviation noted.
			Reviewed a sample of new hires and ensured they were filled in accordance with the hiring procedures.	No deviation noted.
		Once a job description is in place, Personnel initiate a Personnel Action Request (PAR) and then an Electronic Personnel Action Request (ePAR) in order to request to fill a vacancy. Once the ePar is approved by the Administrative and Regulatory Shared Services, Department's CFO, Department's Director and the Governor's Office of Management and Budget; Administrative and Regulatory Shared Services will begin the hiring process by posting the vacant position.	Reviewed a sample of new hires to determine if a PAR and ePAR were properly completed and approved.	No deviation noted.
		Upon employment, the Administrative and Regulatory Shared Services provides new employees orientation. During orientation, new employees complete various forms and training.	Reviewed the training provided to new employees.	No deviation noted.
			Reviewed a sample of new employees to determine if they had been provided training.	1 new employee and 1 new contractor of 573 employees/ contractors had not completed security awareness training.
		The Department's training office works with managers to identify	Review the training report to determine if employees had	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		training needs, registers employees for training and tracks all training in a database.	received training.	
CC1.4	The Department has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and requirements as they relate to security, availability, and processing integrity.	The security obligations of Department staff are communicated via the mandatory annual security awareness training.	Reviewed the security awareness training report to determine if employees and contractors completed training.	No deviation noted.
		New Department staff are required to sign a statement signifying that they will comply with the security policies.	Reviewed the security awareness training to determine if confirmation of compliance with policies is required.	No deviation noted.
			Reviewed the security awareness training report to determine if new employees had confirmed compliance with policies.	1 new employee and 1 new contractor of 573 employees/ contractors had not completed security awareness training.
		Department staff reconfirm their compliance with the security policies through the annual security training.	Reviewed the security awareness training to determine if confirmation of compliance with policies is required.	No deviation noted.
			Reviewed the security awareness training report to determine if employees had confirmed compliance with policies.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		Contractors confirm their compliance with security policies through security training.	Reviewed the security awareness training to determine if confirmation of compliance with policies is required.	No deviation noted.
			Reviewed the security awareness training report to determine if contractors had confirmed compliance with policies.	No deviation noted.
		New employees and contractors are required to have background checks.	Reviewed a sample of new employees and contractors to determine if a background check had been completed.	No deviation noted.
		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.
CC2.0	**Common Criteria Related to Communications**			
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.	The Department has published on their website the Service Catalog for which agencies may utilize in determining their required services.	Reviewed the Service Catalog to determine the services and/or products offered.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
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 to determine if confirmation with policies was required.	No deviation noted.
			Reviewed the security awareness training report to determine if new employees had confirmed compliance with policies.	1 new employee and 1 new contractor of 573 employees/ contractors had not completed security awareness training.
		Department staff reconfirm their compliance with the security policies through the annual security training.	Reviewed the security awareness training report to determine if confirmation with policies was required.	No deviation noted.
			Reviewed the security awareness training report to determine if employees had confirmed compliance with policies.	No deviation noted.
		Contractors confirm their compliance with security policies through security training.	Reviewed the security awareness training report to determine if confirmation with policies was required.	No deviation noted.
			Reviewed the security awareness training report to determine if contractors had confirmed compliance with policies.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		The Department has published on their website the Service Catalog for which agencies may utilize in determining their required services.	Reviewed the Service Catalog to determine the services and/or products offered.	No deviation noted.
		The Department has implemented several policies to address an array of security issues; physical and logical.	Reviewed security policies to determine if they address physical and logical security issues.	The policies did not address: - the requirements for requesting, obtaining, and modifying access (documentation, tracking and approvals), -the periodic review of access rights, -the revocation of access rights, -the actions supervisors were to take when notified of a security issue.
CC2.3	The Department communicates the responsibilities of internal and external users and others whose roles affect system operation.	New Department staff are required to sign a statement signifying that they will comply with the security policies.	Reviewed the security awareness training report to determine if confirmation with policies was required.	No deviation noted.
			Reviewed the security awareness training report to determine if new employees had confirmed compliance with policies.	1 new employee and 1 new contractor of 573 employees/ contractors had not completed security awareness training.

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

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

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

	Criteria	Department's Control	Testing Performed	Results
		The Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provided guidance to users for the reporting of lost or stolen assets.	Reviewed policies to determine if they provided guidance for reporting lost or stolen assets.	No deviation noted.
			Reviewed a sample of lost/stolen assets to determine compliance with policies.	1 of 4 stolen/lost laptops did not have an analysis completed to determine if encryption had been installed.
		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.	The Computer Security Incident Process was not effective until April 3, 2015.
			Reviewed a sample of security issues to determine compliance with procedures.	3 of 3 MORTs did not have the required MORT escalation notification or email attached to the Remedy ticket.
CC2.6	System changes that affect internal and external system user responsibilities or the Department's commitments and requirements relevant to security,	Infrastructure changes are communicated to users and management via the CAC meetings; which the meeting minutes are	Reviewed a sample of CAC meeting minutes to ensure they were posted on the SharePoint site.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
	availability, and processing integrity are communicated to those users in a timely manner.	posted on the ECM SharePoint site.	Reviewed a sample of Request For Changes (RFC) to determine if they were included in CAC meeting minutes on the SharePoint Site.	-1 of 68 RFCs was not included in the CAC Meeting minutes. -1 of 68 RFCs was discussed and agency approved; however, not CAC approved.
		Agencies have access to the ECM SharePoint site.	Reviewed a listing of agencies with access to the SharePoint site.	No deviation noted.
		Emergency changes are communicated to users post implementation via the CAC meeting.	Reviewed a sample of emergency changes to determine if they were included in the CAC meeting minutes on the SharePoint Site.	No deviation noted.
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**			
CC3.1	The Department (1) identifies potential threats that would impair system security, availability, and processing integrity commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies).	The Department is to conduct periodic risk assessments which identify threats and vulnerabilities, and assesses their impact.	Reviewed the risk assessment report to determine the identified threats, vulnerabilities and the assessed impact.	The Department conducted a limited scope assessment of the Department's ability to support specific operations in the event of unplanned or unscheduled outages. The Department had not conducted any other assessments.

	Criteria	Department's Control	Testing Performed	Results
		The Department is to remediate any risk identified.	Interviewed the Chief Information Security Officer.	The Department had not developed a corrective action plan.
CC3.2	The Department designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.	The Department is to conduct periodic risk assessments which identify threats and vulnerabilities, and assesses their impact.	Reviewed the risk assessment report to determine the identified threats, vulnerabilities and the assessed impact.	The Department conducted a limited scope assessment of the Department's ability to support specific operations in the event of unplanned or unscheduled outages. The Department had not conducted any other assessments.
		The Department is to remediate any risk identified.	Interviewed the Chief Information Security Officer.	The Department had not developed a corrective action plan.
		As part of the annual comprehensive test of Category One, Stage Zero applications/data, the DCMS/BCCS Infrastructure Services Recovery Activation Plan is tested.	Reviewed the DCMS/BCCS Infrastructure Services Recovery Activation Plan (Plan) and testing documentation to determine if the Plan had been tested.	No deviation noted.
CC3.3	The Department (1) identifies and assesses changes (for example, environmental, regulatory, and technological changes) that could significantly affect the system of internal control for security,	The Department is to conduct periodic risk assessments which identify threats and vulnerabilities, and assess the impact.	Reviewed the risk assessment report to determine the identified threats, vulnerabilities and the assessed impact.	The Department conducted a limited scope assessment of the Department's ability to support specific operations

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

	Criteria	Department's Control	Testing Performed	Results
		the applicable division for resolution	created and assigned for resolution.	
		The Daily Shift Report documents the activity conducted on all mainframe production systems and incident calls received at the Operations Center.	Review a sample 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, any open items are passed on, and to identify any changes which need to occur. The Checklists are reviewed by the Operations Center Supervisor.	Reviewed a sample of Operator Shift Change Checklist 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 is maintained within.	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.	No deviation noted.
		System performance is monitored via software tools.	Reviewed a sample of software tool reports to determine if system performance was monitored.	No deviation noted.
		Performance monitoring is documented via internal memorandum distributed to	Reviewed all memorandum to management regarding system performance and capacity	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		management.	during the audit period.	
		Remote Monitoring Facility (RMF) reports are run weekly and monthly.	Reviewed a sample 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 team will be alerted.	Reviewed the Data Breach Notification Policy and the Action Plan for Notification of a Security Breach to determine the process of notification in the event of a security breach.	No deviation noted.
			Interviewed Acting Chief Information Security Officer to determine if breaches complied with the Policy and Action Plan.	The Department did not encounter any breaches during the period covered by the report; therefore, no testing was performed.
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**			
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.	Logical access to mainframe information is protected through system security software.	Reviewed system options and security software reports to determine if information was protected by security software.	No deviation noted.
		The mainframe security software requires users to have an	Observed a user sign-on process to determine if an ID	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		established ID and password in order to verify the individual's identity.	and password were required to verify identity.	
			Reviewed system options and password requirements memo to determine password standards.	No deviation noted.
		The primary means of defining a user's access to resources is the system security software resource profile, which defines the level of access a user may have.	Reviewed a sample of user profiles to determine if the users' level of access was defined.	No deviation noted.
		The Department has restricted mainframe access with powerful privileges, high-level access, and access to sensitive system functions to authorized personnel.	Reviewed security software report to determine if powerful privileges, high-level access, and access to sensitive system functions were limited to authorized personnel.	No deviation noted.
		In order to access an application, a user must have a separate application ID and password in order to gain access.	Observed that the applications required a separate ID and password to gain access.	No deviation noted.
		Access to storage and backup data is limited to authorized staff.	Reviewed a sample of staff with access to storage and backup data to determine appropriateness.	No deviation noted.

	Criteria	Department’s Control	Testing Performed	Results
		Logical security controls are in place to restrict access to operating system configurations.	Reviewed system options, security reports, security software, exits, and access rights to sensitive system functions to determine if logical security controls were in place to restrict access to operating system configurations.	No deviation noted.
		Operating systems have been configured to promote security.	Reviewed system options, security reports, security software, exits, and libraries to determine if operating systems were configured and controlled to promote security.	No deviation noted.
		Staff has access to specific RACF groups which allows them to reset passwords.	Reviewed a sample of Help Desk staff to determine if their access rights were appropriate.	No deviation noted.
		In order to access the Department’s environment, the user must be assigned a user ID and password.	Observed that an ID and password was required in order to gain access to the Department’s environment.	No deviation noted.
		The Department maintained an Enterprise Virtual Private Network solution to connect remotely into resources managed and maintained by the Department.	Reviewed the VPN configurations to determine the encryption configuration and settings.	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	Reviewed a sample of firewalls, routers, and switch configurations to determine if they were configured to utilize authentication servers, logging servers, banners warning	No deviation noted.

	Criteria	Department’s Control	Testing Performed	Results
		permit specific types of network traffic.	prohibiting unauthorized access and warning of prosecution and ACLs to deny and permit specific traffic.	
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.	The mainframe security software requires user to have an established mainframe ID and password in order to verify the individual’s identity.	Observed a user sign-on process to determine if an ID and password were required to verify identity.	No deviation noted.
			Reviewed system options and password requirements memo to determine password standards.	No deviation noted.
		The primary means of defining a user’s access to mainframe resources is the security software resource profile, which defines the level of access a user may have.	Reviewed a sample of user profiles to determine if the users’ level of access was defined.	No deviation noted.
		In order to obtain an ID to access the Department’s environment, the user’s supervisor must submit an authorized ESR indicating the required access.	Reviewed sample of staff to determine if an authorized ESR indicating required access was submitted.	The Storage and Backup division did not have new hires during the period covered by the report; therefore, no testing was performed.
		Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form for new requests and submit via a Remedy Enterprise Service Request.	Reviewed a sample of new requests to determine if a Mainframe Application Access Request Form had been submitted via an Enterprise Service Request or email.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		The Mainframe Application Access Request Form indicates the access required and proper approval.	Reviewed a sample of Mainframe Application Access Request Forms to determine if the required access and proper approval was obtained.	No deviation noted.
		In the event the Mainframe Application Access Request Form is for a non-expiring ID, the CISO must approve.	Reviewed a sample of non-expiring IDs to determine if a Mainframe Application Access Request Form was approved by the CISO.	No deviation noted.
		The Exit Form is sent to the employee's supervisor indicting the items to be retrieved and the deactivation of access.	Reviewed a sample of separated employees to determine if their access had been deactivated in a timely manner.	2 of 4 separated employees did not have their access deactivated in a timely manner.
		In order to obtain an ID to access the Department's environment, the agency is to submit an authorized ESR indicating the required access.	Reviewed a sample of staff to determine if an authorized ESR was submitted.	No deviation noted.
		Upon separation from the Department, Personnel complete a PAR, which notifies the Department's CFO of the departure.	Reviewed a sample of terminated employees to determine if a PAR and Exit Form had been completed.	3 of 5 exit forms were completed after the employee's effective leave date.
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 an application, a user must have a separate application ID and password in order to gain access.	Observed that the applications required a separate ID and password to gain access.	No deviation noted.
		Mainframe security software password standards have been established.	Reviewed system options report to determine password standards.	No deviation noted.

	Criteria	Department’s Control	Testing Performed	Results
		The mainframe security software requires users to have an established ID and password in order to verify the individual’s identity.	Observed a user sign-on process to determine if an ID and password were required to verify identity and the user profile contained a name field.	No deviation noted.
			Reviewed system options and password requirements memo to determine password standards.	No deviation noted.
		The primary means of defining a user’s access to resources is the security software resource profile, which defines the level of access a user may have.	Reviewed a sample user profiles to determine if the level of access was defined.	No deviation noted.
		The Department maintained an Enterprise Virtual Private Network solution to connect remotely into resources managed and maintained by the Department.	Reviewed the VPN configurations to determine the encryption configuration and settings.	No deviation noted.
		Users establish their identity and authentication to systems and applications through the use of user IDs and passwords.	Reviewed the administrative architecture deployed on the authentication services.	No deviation noted.
			Observed a user account to determine if they were assigned a user ID and password.	No deviation noted.
			Reviewed a sample of users with powerful access rights to determine if the rights were appropriate.	No deviation noted.
		Authentication servers utilize an administrative architecture in which	Reviewed the groups to determine if the privileges	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		groups are established with specific levels of administrative privileges for individual's needs.	were appropriate.	
		Password parameters have been established on authentication servers.	Reviewed the password configurations.	No deviation noted.
			Observed a user account to determine if the password configurations had been enforced.	No deviation noted.
		Firewalls and routers are used and configured to prevent unauthorized access via authentication servers, logging servers, banners prohibiting unauthorized access and warning of prosecution and ACLs to deny and permit specific types of network traffic.	Reviewed a sample of firewalls, routers, and switch configurations to determine if they were configured to utilize authentication servers, logging servers, banners warning prohibiting unauthorized access and warning of prosecution and ACLs to deny and permit specific traffic.	No deviation noted.
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them.	Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form for new requests and submit via a Remedy Enterprise Service Request.	Reviewed a sample of new requests to determine if a Mainframe Application Access Request Form had been submitted via an Enterprise Service Request or email.	No deviation noted.
		The Mainframe Application Access Request Form indicates the access required and proper approval.	Reviewed a sample of Mainframe Application Access Request Forms to determine if the required access and proper approval was obtained.	No deviation noted.
		In the event the Mainframe Application Access Request Form is for a non-expiring ID, the CISO	Reviewed a sample of non-expiring IDs to determine if a Mainframe Application Access	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		must approve.	Request Form was approved by the CISO.	
		Password resets to Department and proxy agency user profiles are completed by submitting an email request to the Help Desk, or by accessing the Department's Identity Management website.	Reviewed a sample of password resets to determine if an email request had been submitted.	19 of 60 password resets did not have an email request submitted.
			Reviewed the Department's Identity Management Website.	No deviation noted.
		Upon termination or no longer requiring access, an Exit Form is received; the Security Coordinator or Security Software Administrator will deactivate the ID.	Reviewed a sample of separated employees to determine if their access had been deactivated in a timely manner.	2 of 4 separated employees did not have their access deactivated in a timely manner.
		Twice a year, the Security Software Administrator will send out the Security Reconciliation Report to agencies. Upon return, the Security Software Administrator will make the applicable changes.	Reviewed the bi-annual Security Reconciliation Report sent to agencies.	No deviation noted.
		An ESR is created in order for Help Desk staff to receive the appropriate access.	Reviewed a sample of new Help Desk staff to determine if an ESR had been completed.	No deviation noted.
		In the event a user's Active Directory password to be reset, they are to contact the Help Desk via email, problem report or utilize one of the two Self-Service Solutions; BCCS Identity Management Solution or the Forefront Identity Manager Solution.	Interviewed Help Desk manager.	The Department did not follow the requirement of an email or problem report to be submitted for Active Directory password resets.
			Reviewed the Department's Identity Management Website.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		In the event an Active Directory ID needs to be modified, an email or an ESR is to be received indicating the necessary modifications.	Reviewed a sample of Active Directory ID modification to determine if an email or ESR was received.	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 sample of terminated individuals to determine if access was deactivated timely.	2 of 4 separated employee's access was not deactivated in a timely manner.
		The Department maintained an Enterprise Virtual Private Network solution to connect remotely into resources managed and maintained by the Department.	Review the VPN configurations to determine the encryption configuration and settings.	No deviation noted.
		Users establish their identity and authentication to systems and applications through the use of user IDs and passwords.	Reviewed the administrative architecture deployed on the authentication services.	No deviation noted.
			Observed a user account to determine if they were assigned a user ID and password.	No deviation noted.
			Reviewed a sample of users with powerful access rights to determine if the rights were appropriate.	No deviation noted.
		Authentication servers utilize an administrative architecture in which groups are established with specific levels of administrative privileges for individual's needs.	Review the groups to determine if the privileges are appropriate.	No deviation noted.
		Password parameters have been established on authentication	Reviewed the password configurations.	No deviation noted.

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

	Criteria	Department's Control	Testing Performed	Results
		If an alarm is triggered, an alert notifies the Velocity System.	Determined who monitored the alarms.	No deviation noted.
		The Department has created preventive measures at the CCF in order to prevent unauthorized access.	Observed the measures at the CCF to prevent unauthorized access.	No deviation noted.
		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 is utilized to restrict access to the facilities and within.	No deviation noted.
		In order to obtain a card key, an ID Badge Request Form is to be completed; approval must be obtained from an authorized manager, presentation of a valid ID and a completed background check prior to access being granted.	Reviewed a sample of new employees and contractors ID Badge Request Forms to determine if the Forms were properly approved and if a background check had been completed prior to access being granted.	2 of 7 employees did not have an ID Badge Request Form and 1 of 7 did not have a background check completed.
		Access to restricted areas is based on the employee and contractor's duties.	Reviewed a sample of employees and contractors with access to the CCF, Communications Building, and sensitive area to determine appropriateness.	3 of 22 individuals had access to sensitive areas that was no longer required. 2 of 22 individual's access rights to sensitive areas was not timely removed.
		Visitors are required to sign in and out, provide their driver's license, and be escorted.	Reviewed a sample of visitor logs to determine if they were properly completed.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
			Observed visitors being escorted.	No deviation noted.
		Employees and contractors who have forgotten their cardkey are required to sign-in, and provide their driver's license. The employee or contractor is provided a cardkey with access based on the authorization within the cardkey system.	Reviewed a sample of Admittance Registers to determine if the employee or contractor signed in and were provided the appropriate badge based on the authorization within the cardkey system.	No deviation noted.
		Visitors are provided visitor badges, which does not permit access to or within the CCF and Communications Building.	Observed the operation of visitor badges to determine that access to and within the CCF and Communications Building was not permitted.	No deviation noted.
		The Exit Form is sent to the employee's supervisor to ensure collection of equipment and termination of access.	Reviewed a sample of terminated employees and contractors to determine timely deactivation of access.	All terminated individual's access was terminated. However, the Department did not maintain documentation to support access termination dates and the requests for access termination were 1 to 23 days after the termination date for 4 of 10 individuals tested.
		Upon separation from the Department, Personnel complete a	Reviewed a sample of terminated employees to	3 of 5 exit forms were completed

	Criteria	Department’s Control	Testing Performed	Results
		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.	determine if a PAR and Exit Form had been completed.	after the employee’s effective leave date.
CC5.6	Logical access security measures have been implemented to protect against security, availability, and processing integrity threats from sources outside the boundaries of the system.	Logical access to information is protected through system security software.	Reviewed system options and security software reports to determine if information was protected by security software.	No deviation noted.
		Network diagrams are maintained depicting the infrastructure and placement of firewalls, routers, and switches.	Reviewed network diagrams to determine the placement of firewalls, routers, and switches.	No deviation noted.
		The Department maintained an Enterprise Virtual Private Network solution to connect remotely into resources managed and maintained by the Department.	Reviewed the VPN configurations to determine the encryption configuration and settings.	No deviation noted.
		Laptop and desktop operating systems are updated as required by the vendor.	Reviewed the Department’s compliance report to determine if the operating system had been updated on the laptops and desktops.	1,637 of 38,339 laptops and desktops were not running the latest version of the operating system.
			Reviewed a sample of desktops and laptops to determine if the latest patches had been installed.	18 of 40 desktops and laptops did not have the latest patch installed.
CC5.7	The transmission, movement, and removal of information is restricted to authorized users and processes, and is	The Data Classification and Protection Policy documents the data classification schema used to	Reviewed the Data Classification and Protection Policy to determine if the data	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
	protected during transmission, movement, or removal enabling the Department to meet its commitments and requirements as they relate to security, availability, and processing integrity.	value and classify information generated, accessed, transmitted or stored.	classification schema utilized to value and classify information generated, access, transmitted or stored.	
		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.
		The Business Reference Model collects and stores information related to application and data processing services provided based on the Data Classification and Protection Policy.	Reviewed the Business Reference Model to determine if it collected and stored information related to application and data process services provided based on the Data Classification and Protection Policy.	1,409 of 1,845 Department and agency applications had not been categorized.
		Laptops deployed after December 1, 2007 have encryption installed.	Reviewed a sample of laptops/desktops deployed after December 1, 2007 to determine if encryption had been installed	Information to determine if encryption had been installed on 11 of 40 laptops was not available.
		The Department makes available encryption technologies and access gateways for the transmission of sensitive or confidential	Reviewed the VPN configurations to determine the encryption configuration and settings.	No deviation noted.

	Criteria	Department’s Control	Testing Performed	Results
		information.	Reviewed the web portal utilized to login to the VPN to determine if a banner indicated the system was only for use by authorized users, use may be monitored, and user’s requirements to ensure devices connection to resources via the VPN were current on security and antivirus patches.	No deviation noted.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software.	Antivirus is installed on laptops and desktops.	Reviewed a sample of laptops and desktops to determine if antivirus was installed.	Information to determine if antivirus had been installed on 16 of 40 laptops and desktops was not available.
		Antivirus is updated on laptops and desktops at least daily.	Reviewed a sample of laptops and desktops with antivirus updated to determine if the antivirus was up to date .	No deviation noted.
		The Department has tools in place to monitors laptops and desktops to ensure the antivirus is updated.	Reviewed compliance report to determine if antivirus software was monitored on laptops and desktops.	No deviation noted.
		The Department utilizes tools to push and monitor Microsoft patches.	Reviewed compliance report to determine if patches were monitored on laptops and desktops.	No deviation noted.
		The ability to install, modify, and replace operating systems is limited to authorized staff.	Reviewed access rights to determine if the ability to install, modify, and replace	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
			operating system was limited to authorized staff.	
		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.
CC6.0	**Common Criteria Related to System Operations**			
CC6.1	Vulnerabilities of system components to security, availability, and processing integrity breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities.	CA-Scheduler is utilized to schedule and control backups.	Reviewed a sample of backup schedules to determine if mainframe systems were backed up.	No deviation noted.
		Backups are conducted routinely.	Reviewed a sample of schedules to determine if backups were conducted routinely.	No deviation noted.
		The Department verifies the daily and weekly backups completed successfully.	Reviewed a sample of the verify backup reports to determine if backups were completed successfully.	No deviation noted.
			Reviewed a sample of logs to determine if the replication was successful.	No deviation noted.
		The Department is notified of failed backups.	Reviewed a sample of failed backups to determine if the Department was notified.	The Department did not encounter failed backups during the period covered by the report; therefore, no testing was performed.

	Criteria	Department's Control	Testing Performed	Results
		Failed backups are recorded on the Shift Report.	Reviewed a sample of failed backups to determine if they were reported on the Shift report.	The Department did not encounter failed backups during the period covered by the report; therefore, no testing was performed.
		Library Services maintains a listing of backups which are scheduled to be ran on SharePoint.	Reviewed a sample of schedules which were maintained on SharePoint.	No deviation noted.
		The day after the backup is scheduled to run, a report is ran to determine the success/failure of the job.	Reviewed a sample of backup logs to determine the success or failure of the job.	No deviation noted.
		System automation tool controls and monitors available storage levels.	Reviewed system automation storage levels.	No deviation noted.
		System automation tool notifies staff via email when storage levels fall below the pre-determined threshold.	Reviewed a sample of email notifications to determine if staff was notified when storage levels fell below the pre-determined threshold.	The Department does not maintain the email notifications.
		A Remedy ticket is created if an agency requires additional storage.	Reviewed of sample of requests for additional storage to determine if a Remedy ticket had been completed.	No deviation noted.
		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	Reviewed a sample of Daily Shift Reports to determine if	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		and a Remedy Ticket is created.	problems, issues, and incidents were reported.	
		For any incident in which the Operations Center cannot resolve, the Remedy Ticket is assigned to the applicable division for resolution.	Reviewed a sample of Daily Shift Reports to determine if a Remedy Ticket had been created and assigned for resolution.	No deviation noted.
		In the event a user encounters a security issue, the Department's website instructs them to contact the Help Desk.	Reviewed the website to determine if instructions for contacting the Help Desk were included.	No deviation noted.
		The Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provides guidance to the user for the reporting of lost or stolen assets.	Reviewed the Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy to determine if guidance was provided to users.	No deviation noted.
		Upon notification of a lost or stolen asset, the Help Desk staff is to create a Remedy ticket, attach the police report and assign the ticket to the Asset Management staff.	Reviewed a sample of lost/stolen devices to determine if a Remedy Ticket had been created and a police report was attached to the ticket.	No deviation noted.
		EUC is to be notified in order to determine if the equipment had encryption installed. If encryption was not installed, EUC was to determine if confidential information was retained and notify the S&CS Group if it was.	Reviewed a sample of lost/stolen devices to determine if EUC had conducted an analysis to determine if encryption was installed.	1 of 4 stolen/lost laptops did not have an analysis completed to determine if encryption had been installed.
		Users are required to email or submit a problem report via the Department's website to the Help	Reviewed a sample of password resets to determine if an email or problem report	19 of 60 password resets did not have an email request

	Criteria	Department's Control	Testing Performed	Results
		Desk requesting a RACF mainframe password reset. The request is included the user's name, ID, and a phone number to be contacted.	had been submitted indicating the user's name, ID and phone number.	submitted.
		Records exist for monitoring and documenting operating system actions.	Reviewed system files to determine if records exist for monitoring and documenting operating system actions.	No deviation noted.
		System performance is monitored via software tools.	Reviewed a sample of software tool reports to determine if system performance was monitored.	No deviation noted.
		Performance monitoring is documented via internal memorandum distributed to management.	Reviewed all memorandum to management regarding system performance and capacity during the audit period.	No deviation noted.
		Remote Monitoring Facility (RMF) reports are run weekly and monthly.	Reviewed a sample of RMF reports to determine the frequency.	No deviation noted.
		Authentication servers are utilized to control access, log access attempts, and alert management.	Reviewed a sample of authentication servers to determine if they were utilized to control access, log access attempts, and alert management.	Alerts were not enabled to notify staff of failed attempts.
		The Department has tools in place to identify and log network services security breaches.	Reviewed a sample of firewalls, routers, and switch to determine if they were configured to utilize logging servers.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
			Reviewed SolarWinds to determine if monitoring of performance, bandwidth utilization, CPU utilization, etc was conducted and if alerts were sent to management.	No deviation noted.
			Reviewed a sample of devices to determine if they were connected to SolarWinds.	6 of 40 devices were not connected to SolarWinds.
		Routine backups of configurations for firewalls, routers and switches are conducted.	Reviewed a sample of networking devices to determine if they were connected to backup solutions.	6 of 40 devices were not connected to SolarWinds.
			Reviewed backup schedules to determine frequency of backups.	No deviation noted.
		The Department is notified of failed backups.	Reviewed a sample of alerts to determine if the Department was notified of failed backups.	Alerts to Network management regarding backups were not utilized.
		Network monitoring tools are utilized to monitor inbound and outbound network traffic.	Reviewed the tool utilized to monitor traffic to determine who was monitoring and the frequency of monitoring.	The Department did not provide the auditor with information on tools or reports in order for procedures to be performed.
			Reviewed reports to determine actions taken on identified threats.	The Department did not provide the auditor with information on tools

	Criteria	Department's Control	Testing Performed	Results
				or reports in order for procedures to be performed.
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 Department is notified of failed backups.	Reviewed a sample of failed backups to determine if the Department was notified.	The Department did not encounter failed backups during the period covered by the report; therefore, no testing was performed.
		The Department takes remedial action on failed backups.	Reviewed a sample of failed backups to determine the actions taken.	The Department did not encounter failed backups during the period covered by the report; therefore, no testing was performed.
		The user manuals for applications provide instructions for users to contact the Help Desk to report issues.	Reviewed user manuals to determine if they provide instruction to report issues to the Help Desk.	No deviation noted.
		The Operations Center utilizes software and the Automated Operations Console in order to continuously monitor the environment.	Observed the software utilized and the Automated Operations Console to determine if the environment was monitored.	No deviation noted.
		Problems, issues, and incidents are recorded via the Daily Shift Report and a Remedy Ticket is created.	Reviewed a sample of Daily Shift Reports to determine if problems, issues, and incidents were reported.	No deviation noted.
		For any incident in which the Operations Center cannot resolve,	Reviewed a sample of Daily Shift Reports to determine if	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		the Remedy Ticket is assigned to the applicable division for resolution.	a Remedy Ticket had been created and assigned for resolution.	
		The Daily Shift Report records the activity conducted on all production systems and incident calls received at the Operations Center.	Reviewed a sample of Daily Shift Reports to determine if the activity on production systems was recorded and incident calls were recorded.	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 within.	No deviation noted.
		The Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provides guidance to the user for the reporting of lost or stolen assets.	Reviewed the Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy to determine if guidance was provided to users.	No deviation noted.
		Upon notification of a lost or stolen asset, the Help Desk staff is to create a Remedy ticket, attach the police report and assign the ticket to the Asset Management staff.	Reviewed a sample of lost/stolen devices to determine if a Remedy Ticket had been created and a police report was attached to the ticket.	No deviation noted.
		EUC is to be notified in order to determine if the equipment had encryption installed. If encryption was not installed, EUC was to determine if confidential information was retained and notify the S&CS Group if it was.	Reviewed a sample of lost/stolen devices to determine if EUC had conducted an analysis to determine if encryption was installed.	1 of 4 stolen/lost laptops did not have an analysis completed to determine if encryption had been installed.

	Criteria	Department's Control	Testing Performed	Results
		Staff and users are instructed to contact the Help Desk or their supervisor to report all security, availability and processing issues. Help Desk staff is to open a Remedy ticket and record the incident. The Remedy ticket is to track the issues until resolution.	Interviewed Acting Chief Information Security Officer.	The Department did not provide detailed documentation in order for procedures to be performed.
CC7.0	**Common Criteria Related to Change Management**			
CC7.1	Security, availability, and processing integrity commitments and requirements, are addressed, during the system development lifecycle including design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.	Changes are categorized and ranked according to priority.	Reviewed a sample of changes to determine if they were properly categorized and ranked according to priority.	No deviation noted.
		Emergency changes require verbal approval prior to implementation. Standard approvals are to be obtained post implementation.	Reviewed a sample of emergency changes to determine if verbal approval was obtained prior to implementation and if standard approvals were obtained post implementation.	No deviation noted.
		Transparent changes (low impact changes), which have little to no impact are required to be approved by Group Managers. Medium and high impact changes are required to be approved by Group Mangers, Change Management Team and the Change Advisory Committee (CAC).	Reviewed a sample of changes to determine if they were properly approved.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		Project Charters, Business Requirements, and Technical Requirements are required to be submitted to and approved by the Governance staff.	Reviewed a sample of IT Projects to determine if Project Charters, Technical Requirements, and Business Requirements had been submitted and approved.	No deviation noted.
		Agencies are notified by email of a Project Charter approval.	Reviewed a sample of IT Projects to determine if the agencies were notified by email of the Project Charter approval.	No deviation noted.
		Governance staff review and assess the project scope statement.	Reviewed a sample of IT projects to determine if Governance staff reviewed and assessed the project scope statement.	No deviation noted.
		Application changes are required to have the Mainframe Checklist completed.	Reviewed a sample of changes to determine if the Mainframe Checklist had been completed.	1 of 31 change tasks did not have the Mainframe Checklist completed. 1 of 31 change tasks did not have the Mainframe Checklist properly completed.
		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	Reviewed the EAA Change Management Procedures and the Application Life cycle Management Methodology.	The Application Lifecycle Management Methodology and the EAA Change Management

	Criteria	Department's Control	Testing Performed	Results
		the EPM Portal and the Application Life cycle Management Methodology.		Procedures did not address: -Required approvals, -Testing and documentation requirements, -Requirements for followup after change is moved to production, and -Emergency change requirements.
			Reviewed sample of application changes to determine compliance with the EAA Change Management Procedures and the Application Lifecycle Manual.	-1 of 1 change did not have all required fields completed; Requested Date, Estimated Downtime. -8 of 9 changes did not have the required Impact Assessment completed. -1 of 9 changes did not indicate if the required Impact Assessment had been completed.

	Criteria	Department's Control	Testing Performed	Results
				-7 of 9 changes did not have Key Communications noted within the change ticket. -2 of 10 changes did not have the Business Owner approval. -4 of 4 changes indicated the Business Owner approval was obtained; however, it was not attached as required. -1 of 1 change did not have the required ESR requesting the change be moved to the production environment.
CC7.2	Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the system commitments and requirements as they relate to security, availability, and processing integrity.	A post implementation review (PIR) is conducted on 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 sample of emergency changes to determine if a post implement review had been conducted and properly reviewed.	3 of 8 emergency RFCs did not have a PIR conducted. 2 of 60 RFCs indicated a PIR was to be completed;

	Criteria	Department's Control	Testing Performed	Results
				however, it was not attached.
			Reviewed a sample of changes which caused an outage to determine if a post implementation review had been conducted and approved.	The Department did not have a mechanism to track changes which caused an outage; therefore, detailed testing could not be conducted.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.	Each change is required to have a completed Request For Change (RFC) within Remedy. Specific fields within the RFC are to be completed as required by the Remedy Change Management Guide.	Reviewed the Guide and Policy to determine the requirements for a completed RFC.	The Guide did not provide sufficient guidance or requirements for post implementation reviews, testing levels, or back-out and implementation plans. The Policy did not provide sufficient guidance or requirements for testing, evaluating and authorizing changes prior to implementation.
			Reviewed a sample of changes determine if a RFC was properly completed.	63 of 68 RFCs did not have the Requested Date field completed as

	Criteria	Department's Control	Testing Performed	Results
				required by the Create Change Request Guide. 1 of 68 RFC did not have the Supervisor information included as required by the Create Change Request Guide.
		Approvals, plans and information associated with the change are to be attached or included within the specific RFC for record purposes.	Reviewed a sample of changes to determine if they were properly approved and if plans and information were attached.	No deviation noted.
		A post implementation review is conducted on changes which causes an outage or an emergency change. The review is conducted by the change supervisor or a Change Management Team member.	Reviewed a sample of emergency changes to determine if a post implementation review had been conducted and properly reviewed.	3 of 8 emergency RFCs did not have a PIR conducted. 2 of 60 RFCs indicated a PIR was to be completed; however, it was not attached.
			Reviewed a sample of changes which caused an outage to determine if a post implementation review had been conducted and approved.	The Department did not have a mechanism to track changes which caused an outage; therefore, detailed testing could not be conducted.

	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 sample of high impact changes to determine if backout, testing and implementation plans were attached to the RFC.	No deviation noted.
		Emergency changes require verbal approval prior to implementation. Standard approvals are to be obtained post implementation.	Reviewed a sample of emergency changes to determine if verbal approval was obtained prior to implementation and if standard approvals were obtained post implementation.	No deviation noted.
		Transparent changes (low impact changes), which have little to no impact are required to be approved by Group Managers. Medium and high impact changes are required to be approved by Group Mangers, Change Management Team and the Change Advisory Committee (CAC).	Reviewed a sample of changes to determine if they were properly approved.	No deviation noted.
		The detail of testing, and the documentation requirements for testing, backout and implementation plans are to be established by each division.	Reviewed documentation requirements	Testing and documentation requirements for backout and implementation plans had not been established.
		For moves related to DCMS applications, the developer submits a move sheet to a secure mailbox. The move sheet is then forwarded	Reviewed a sample of moves to determine if a move sheet and an authorized email was submitted which indicated the	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		to a Library Services mailbox by authorized staff.	date, time, and libraries to be moved to production.	
		Library Services standards control the moves of changes to agency applications to production libraries.	Reviewed the Library Services Standards which controlled moves to production.	No deviation noted.
		Library Services is responsible for moving agencies application changes into production. In order for a move to be completed, the agencies are required to submit an email from an authorized staff to Library Services indicating the date, time, and libraries to be moved into production.	Reviewed a sample of moves to determine if an authorized email was submitted which indicated the date, time and libraries to be moved.	No deviation noted.
		For moves related to DCMS, the developer is to submit a move sheet to a secure mailbox. The move sheet is then forward to Library Services by an authorized staff.	Reviewed a sample of moves to determine if an authorized move sheet had been submitted.	No deviation noted.
		The Operations Center staff is responsible for completing the mainframe changes. Once the change has been completed, the staff will update the Remedy Ticket indicating the move had occurred. In addition, the Remedy Ticket and the IPL screen are printed to ensure accuracy of the information.	Reviewed a sample of Remedy Tickets to determine if the Operation Center staff updated and printed the Ticket, and screen printed the IPL.	No deviation noted.
		Standards provide guidance on the configuration and deployment of network devices.	Reviewed the configuration templates and standards.	No deviation noted.

	Criteria	Department’s Control	Testing Performed	Results
		Tools are in place to assist in the deployment of and reporting on configurations.	Reviewed a sample of networking devices to determine if they were connected to SolarWinds.	6 of 40 devices were not connected to SolarWinds.

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

	Criteria	Department's Control	Testing Performed	Results
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements.	System capacity is monitored via software tools.	Reviewed a sample 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 all memorandum to management regarding system performance and capacity during the audit period.	No deviation noted.
		The network is configured in a redundant manner.	Reviewed a sample of networking devices to determine if they were configured for availability.	22 of 60 devices were not configured 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, IT Recovery Policy, and the Recovery Methodology have been developed.	Reviewed the DCMS/BCCS Infrastructure Services Recovery Activation Plan, IT Recovery Policy, and the Recovery Methodology.	The Policy and Methodology had not been updated to reflect the change in recovery vendors and backup processes.
		The Department has entered into an Interagency Agreement with the Department of Agriculture for the utilization of space for a cold site.	Reviewed the Interagency Agreement with the Department of Agriculture.	No deviation noted.
		Application recovery plans or procedures have been developed.	Reviewed the applications' recovery plan or procedures.	The Central Inventory System Plan had not updated to include changes to Vtape. The Central Payroll System Plan did

	Criteria	Department's Control	Testing Performed	Results
				not include testing requirements or Recovery Time Objective (RTO). The Central Time and Attendance System Recovery scripts had not been updated and documentation did not outline RTO. The eTime System documentation did not outline responsibilities, testing requirements, location of recovery documentation, or RTO.
		Application data is backed up daily, weekly and monthly.	Reviewed the backup schedule to determine if the applications were scheduled to be backed up daily, weekly and monthly.	No deviation noted.
			Reviewed a sample of backups to determine if the applications had been backed up.	No deviation noted.
		CA-Scheduler is utilized to schedule and control backups.	Reviewed a sample of backup schedules to determine if all mainframe systems were backed up.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		Backups are conducted routinely.	Reviewed a sample of schedules to determine if backups were conducted routinely.	No deviation noted.
		The Department verifies the daily and weekly backups completed successfully.	Reviewed a sample of the verify backup reports to determine if backups were completed successfully.	No deviation noted.
			Reviewed a sample of logs to determine the success of the replication.	No deviation noted.
		The Department is notified of failed backups.	Reviewed a sample of failed backups to determine if the Department was notified.	The Department did not encounter failed backups during the period covered by the report; therefore, no testing was performed.
		Failed backups are recorded on the Shift Report.	Reviewed a sample of failed backups to determine if they were reported on the Shift report.	The Department did not encounter failed backups during the period covered by the report; therefore, no testing was performed.
		The Department takes remedial action on failed backups.	Reviewed a sample of failed backups to determine the actions taken.	The Department did not encounter failed backups during the period covered by the report; therefore,

	Criteria	Department's Control	Testing Performed	Results
				no testing was performed.
		Data replication occurs every 10 minutes between the CCF and the ADC. Monitoring software sends an alert if the data is out of sync for more than eight hours.	Reviewed a sample of logs to determine the success of the replication.	No deviation noted.
		A Remedy ticket is opened is the event of an issue.	Reviewed of sample of Remedy tickets to determine resolution.	The Department did not encounter failed backups during the period covered by the report; therefore, no testing was performed.
		The software vendor and the staff hold weekly meeting to discuss any issues.	Reviewed a sample of meeting minutes to determine if issues were discussed.	No deviation noted.
		Logs are maintained of the libraries replicated, their status and the time of last sync.	Reviewed a sample of logs to determine if libraries were replicated, their status and the time of last sync.	No deviation noted.
		System automation tool controls and monitors available storage levels.	Reviewed system automation storage levels.	No deviation noted.
		System automation tool notifies staff via email when storage levels fall below the pre-determined threshold.	Reviewed a sample of email notifications to determine if staff was notified when storage levels fell below the pre-determined threshold.	The Department does not maintain the email notifications.
		A Remedy ticket is created if an agency requires additional storage.	Reviewed of sample of requests for additional storage to determine if a Remedy ticket had been completed.	No deviation noted.

	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 measures in place to protect against environmental factors at the CCF and Communications Building.	No deviation noted.
			Reviewed the fire extinguishers and suppression system to determine if they were up to date.	The Department did not have a maintenance contract for the fire suppression system and did not have a maintenance contract for the fire extinguishers until March 2015.
			Determine if UPS and Generators had been tested.	Contractually scheduled monthly and semi-annual inspections were not conducted.
		Preventive maintenance agreements and scheduled maintenance procedures are in place for environmental factors.	Reviewed scheduled procedures outlined in maintenance contracts.	Contractually scheduled monthly and semi-annual inspections were not conducted.
			Obtained the maintenance reports to determine if maintenance procedures were conducted in accordance with contracts.	The Department did not have a maintenance contract in place for the Fire Suppression Systems, Building Automation

	Criteria	Department's Control	Testing Performed	Results
				Systems, Fire Sprinkler System and Generator Fuel. The Department did not enter into a contract for the maintenance of fire extinguishers until March 6, 2015.
		The Department has configured the network in a redundant manner.	Reviewed a sample of networking devices to determine if they were configured for availability.	22 of 60 devices were not configured for availability.
A1.3	Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements.	As part of the annual comprehensive test of Category One, Stage Zero applications/data, the DCMS/BCCS Infrastructure Services Recovery Activation Plan is tested.	Reviewed the DCMS/BCCS Infrastructure Services Recovery Activation Plan and testing documentation to determine if the Plan had been tested.	No deviation noted.
		The agencies are to submit to the Department, the goals and outcomes of their testing for review and updating of Plans and recovery documentation.	Reviewed testing documentation from the September 2014 comprehensive test.	Test documentation for testing conducted in September 2014 lacked detail to determine if noted issues had been resolved and the outcome of the test.
		Application recovery plans or procedures have been developed.	Reviewed the applications' recovery plan or procedures.	The Central Inventory System Plan had not updated to include

	Criteria	Department's Control	Testing Performed	Results
				changes to Vtape. The Central Payroll System Plan did not include testing requirements or RTO. The Central Time And Attendance System Recovery scripts had not been updated and documentation did not outline RTO. The eTime System documentation did not outline responsibilities, testing requirements, location of recovery documentation, or RTO.

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

	Criteria	Department's Control	Testing Performed	Results
PI1.1	Procedures exist to prevent, detect, and correct processing errors to meet processing integrity commitments and requirements.	CA-Scheduler is utilized to schedule and control backups.	Reviewed a sample of backup schedules to determine if mainframe systems were backed up.	No deviation noted.
		Backups are conducted routinely.	Reviewed a sample of schedules to determine if backups were conducted routinely.	No deviation noted.
		The Department verifies the daily and weekly backups completed successfully.	Reviewed a sample of the verify backup reports to determine if backups were completed successfully.	No deviation noted.
			Reviewed a sample of logs to determine the success of the replication.	No deviation noted.
		The Department is notified of failed backups.	Reviewed a sample of failed backups to determine if the Department was notified.	The Department did not encounter failed backups during the period covered by the report; therefore, no testing was performed.
		Failed backups are recorded on the Shift Report.	Reviewed a sample of failed backups to determine if they were reported on the Shift report.	The Department did not encounter failed backups during the period covered by the report; therefore, no testing was performed.

	Criteria	Department's Control	Testing Performed	Results
		The Department takes remedial action on failed backups.	Reviewed a sample of failed backups to determine the actions taken.	The Department did not encounter failed backups during the period covered by the report; therefore, no testing was performed.
		Data replication occurs every 10 minutes between the CCF and the ADC. Monitoring software sends an alert if the data is out of sync for more than eight hours.	Reviewed a sample of logs to determine the success of the replication.	No deviation noted.
		Logs are maintained of the libraries replicated, their status and the time of last sync.	Reviewed a sample of logs to determine if libraries were replicated, their status and the time of last sync.	No deviation noted.
		A Remedy ticket is opened is the event of an issue.	Review of sample of Remedy ticket to determine resolution.	The Department did not encounter failed backups during the period covered by the report; therefore, no testing was performed.
		The software vendor and the staff hold weekly meeting to discuss any issues.	Reviewed a sample of meeting minutes to determine if issues were discussed.	No deviation noted.
		System automation tool controls and monitors available storage levels.	Reviewed system automation storage levels.	No deviation noted.

	Criteria	Department's Control	Testing Performed	Results
		System automation tool notifies staff via email when storage levels fall below the pre-determined threshold.	Reviewed a sample of email notifications to determine if staff was notified when storage levels fell below the pre-determined threshold.	The Department did not maintain the email notifications.
		A Remedy ticket is created if an agency requires additional storage.	Reviewed of sample of requests for additional storage to determine if a Remedy ticket had been completed.	No deviation noted.
		Application data is backed up daily, weekly and monthly.	Reviewed the backup schedule to determine if the applications had been scheduled to be backed up daily, weekly and monthly.	No deviation noted.
			Reviewed a sample of backups to determine if the application had been backed up.	No deviation noted.
		The Department has installed preventive environmental measures at the CCF and the Communications Building. • Fire extinguishers, • Fire suppression, • Sprinkler system, • Water detection, • Cooling/heating systems, • UPS, and Generators	Observed the measures in place to protect against environmental factors at the CCF and Communications Building.	No deviation noted.
			Reviewed the fire extinguishers and suppression system to determine if they were up to date.	The Department did not have a maintenance contract for the fire suppression system and did not have a maintenance contract for the fire extinguishers until March 2015.

	Criteria	Department’s Control	Testing Performed	Results
			Determined if UPS and Generators had been inspected.	Contractually scheduled monthly and semi-annual inspections were not conducted.
		Environmental factors are monitored at the CCF and the Communication Building.	Observed the measures in place to protect against environmental factors at the CCF and Communications Building.	No deviation noted.
		System capacity is monitored via software tools.	Reviewed a sample 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 all memorandum to management regarding system performance and capacity during the audit period.	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 maintained for equipment.	The Department did not provide maintenance contracts for fiber optic and VOIP equipment.
			Reviewed a sample of hardware and software to determine if they were supported by the vendor.	6 of 60 hardware devices were no longer support by the vendor. 10 of 60 software versions were no longer supported by the vendor.

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

	Criteria	Department's Control	Testing Performed	Results
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.	Reperformed a sample of field edits and range checks to determine if they were functioning appropriately and were providing error notifications.	27 of 51 States' (including Washington DC) tax rates were not included in the CPS tax table. 2 of 24 States' (including Washington DC) tax rates were incorrect. The State of Illinois tax rate was correct.
			Reviewed a sample of agencies data to determine if edits and checks were functioning appropriately.	No deviation noted.
PI1.3	Data is processed completely, accurately, and timely as authorized in accordance with processing integrity commitments and requirements.	Applications provide various balancing reports to ensure accuracy of information.	Reviewed the balancing reports to ensure the accuracy of information.	No deviation noted.
		Each transaction is assigned an identifying number.	Reviewed a sample of agencies data to determine if each transaction had an identifying number assigned.	No deviation noted.
PI1.4	Data is stored and maintained completely and accurately for its specified life span in accordance with processing integrity commitments and requirements.	The Department maintains transaction history for a defined period of time.	Reviewed the transaction history.	No deviation noted.

	Criteria	Department’s Control	Testing Performed	Results
		Access to the application’s production libraries has been restricted to authorized Department personnel.	Reviewed a sample of users with access to production libraries to determine appropriateness.	No deviation noted.
		Applications provide various balancing reports to ensure accuracy of information.	Reviewed the balancing reports to ensure the accuracy of information.	No deviation noted.
		Application data is backed up daily, weekly and monthly.	Reviewed the backup schedule to determine if the applications were scheduled to be backed up daily, weekly and monthly.	No deviation noted.
			Reviewed a sample of backups to determine if the applications had been backed up.	No deviation noted.
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 sample of individuals with access to print shop to determine if access was appropriate.	1 of 10 individual no longer required access.
		Upon request for pick up, the individual must provide identification, sign the Report Distribution Checklist, and be on the authorization listing.	Reviewed a sample of Report Distribution Checklist and determine if the individual who picked up the print job was authorized.	1 individual listed on the Report Distribution Checkout List for 20 days sampled was not on the authorization listing.

	Criteria	Department's Control	Testing Performed	Results
		Applications provide various balancing reports to ensure accuracy of information.	Reviewed the balancing reports to ensure the accuracy of information.	No deviation noted.
PI1.6	Modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.	Access to the application's production libraries has been restricted to authorized Department personnel.	Reviewed a sample of users with access to production libraries to determine appropriateness.	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 restricts the ability to access, approve, modify and delete transactions.	No deviation noted.
		Application data is backed up daily, weekly and monthly.	Reviewed the backup schedule to determine if the applications were scheduled to be backed up daily, weekly and monthly.	No deviation noted.
			Reviewed a sample of backups to determine if the application had been backed up.	No deviation noted.

Other Information Provided by the Service Auditor that is Not Covered by the Service Auditor's Report
(Not Examined)

Department of Central Management Services, Bureau of Communication and Computer Services Mainframe Environment

During the period July 1, 2014 to June 30, 2015, the Department's mainframe experienced maximum processing capacity in association with one of the logical systems. As a result, specific processes encountered delays. The Department stated they had ordered new hardware and estimated installation in mid-July 2015.

Information Not Provided to the Service Auditors

According to the Description, Department staff and users are instructed to contact the Help Desk or their supervisor to report any and all security, availability and processing issues. Staff and users may contact the Help Desk via phone or email to report an incident. When a report is received, the Help Desk staff open a ticket in Remedy and record the incident, as well as the user name, agency, contact information and a detailed incident description. The ticket is tracked through Remedy until resolution. As part of the auditor's testing processing, numerous times we requested detailed documentation, including a listing of security, availability and processing issues reported to the Help Desk during the period July 1, 2014 to June 30, 2015, in order to conduct detailed testing to determine if the control was operating during the period covered by the report. However, as of the end of our fieldwork, July 7, 2015, the Department had not provided the requested documentation.

Additionally, the Description states that the Security Compliance Solution and Infrastructure Services are responsible for monitoring IT network resources and, when issues are identified, appropriate units are contacted for remediation. As part of the auditor's testing processing, numerous times we requested detailed documentation, including monitoring reports and remediation documentation during the period July 1, 2014 to June 30, 2015, in order to conduct detailed testing to determine if the control was operating during the period covered by the report. However, as of the end of our fieldwork, July 7, 2015, the Department had not provided the requested documentation.

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)

Common Criteria

1.1 The Department will formalize a process to communicate organization structure and staff vacancies to Senior Management.

1.3 The Department will perform periodic review of new employees and contractors documents to ensure new employee orientation procedures are being followed.

1.4 The Department will perform periodic review of new employees and contractors documents to ensure new employee orientation procedures are being followed.

1.4 The Department will create a schedule for reviewing policies, update and monitor user responsibilities.

1.4 The Department will review policies , update and communicate user responsibilities as appropriate.

2.2 The Department will perform periodic review of new employees and contractors documents to determine if new employee orientation procedures are being followed.

2.2 The Department will review policies , update and communicate user responsibilities as appropriate.

2.3 The Department will perform periodic review of new employees and contractors documents to ensure new employee orientation procedures are being followed.

2.3 The Department will review policies , update and communicate user responsibilities as appropriate.

2.4 The Department will review policies, update and communicate user responsibilities as appropriate.

2.5 The Department will address what supervisors should do for reporting and resolving security issues.

2.5 The Department will develop a new process for encryption analysis of laptops (i.e. checklist)

2.5 The Department will communicate to the appropriate staff the MORT procedures.

2.6 The Department will communicate to CAC that approval is required for all changes.

3.1 The Department will provide a risk assessment plan to identify threats and vulnerabilities and assess their impact.

3.1 The Department will develop corrective action plans as part of the remediation effort to reduce risk

3.2 The Department will provide a risk assessment plan to identify threats and vulnerabilities and assess their impact.

3.2 The Department will develop corrective action plans as part of the remediation effort to reduce risk.

3.3 The Department will conduct risk assessments to identify threats and vulnerabilities and assess their impact.

3.3 The Department will develop corrective action plans as part of the remediation effort to reduce risk.

5.2 The Department will communicate to the appropriate staff, separation of employees must be deactivated in a timely matter.

5.2 The Department will communicate to the appropriate staff, exit forms must be effective on the actual leave date.

5.4 The Department will review procedures/process for password resets.

5.4 The Department will communicate to the appropriate staff, deactivation of separated employees must be deactivated in a timely manner.

5.4 The Department will review procedures/process for Active Directory password resets.

5.4 The Department will develop procedures for granting/removing access to staff and will ensure documentation is completed and maintained.

5.4 The Department will communicate to the appropriate staff, deactivation of separated employees must be deactivated in a timely manner.

5.5 The Department will work with its managers and the CMS Bureau of Facilities Management to ensure the ID badge request process is properly followed, building access rules are followed and access rights are revoked as necessary.

5.5 The Department will communicate with its managers that background checks must be obtained before granting access to employees in sensitive areas.

5.5 The Department will communicate with its managers, employee access to sensitive areas must be deactivated when no longer required in a timely manner.

5.5 The Department will ensure documentation is maintained for employee termination dates.

5.5 The Department will communicate to its managers exit forms are to be completed on effective leave date.

5.6 The Department will review the process for ensuring laptops are running the latest operating system version.

5.6 The Department will review the process for ensuring laptops have the latest patch installed.

5.7 The Department will review department and agency applications for categorization.

5.7 The Department will communicate to its managers encryption must be on all laptops with documentation to verify.

5.8 The Department will communicate to its managers anti virus installation must be on all laptops/desk with documentation to verify.

6.1 The Department will review, update and implement processes to ensure monitoring and alerts are maintained.

6.1 The Department will develop a new process for encryption analysis of laptops (i.e. checklist)

6.1 The Department will communicate to its managers that an email is required before changing RACF passwords

6.1 The Department will review, update and implement processes to ensure monitoring and alerts are maintained.

6.1 The Department will review process for devices for connected to Solar Winds.

6.1 The Department will review process for alerts regarding failed backups.

6.1 The Department will make every effort to provide information on tools or reports used to

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

monitor traffic in a formalized manner.

6.2 The Department will develop a new process for encryption analysis of laptops (i.e. checklist)

6.2 The Department will review documentation to include procedures for security availability and processing integrity requirements.

7.1 The Department will ensure changes are tracked from initiation to implementation. The Application Lifecycle Manual will be revised to reflect the present accepted processes and procedures for minor application changes.

7.2 The Change Management Guide will be reviewed and updated as necessary and the Department will emphasize compliance and proper documentation. Library Services will update the agency approver listing.

7.3 The Change Management Guide will be reviewed and updated as necessary and the Department will emphasize compliance and proper documentation.

7.4 The Department will establish requirements for testing, backout and implementation plans for changes.

Availability

1.1 The Department will review documents to identify if all devices are configured for availability.

1.2 The Department will review and update its policies and plans to ensure environmental protections, data backup processes, recovery infrastructure and documentation is maintained to meet processing integrity and availability requirements.

1.2 The Department will review and update its policies and plans to ensure environmental protections, data backup processes, recovery infrastructure and documentation is maintained to meet

1.2 The Department will review automation tool process for notifications when storage levels fall below pre-determined levels.

1.2 The Department will update its plan to reflect the current environment.

1.2 The Department will review schedules for contractually scheduled monthly and semi-annual inspections.

1.2 The Department will review schedules for contractually scheduled monthly and semi-annual inspections.

1.2 The Department will review process for maintenance contracts for Fire Suppression Systems, Building Automation Systems, Fire Sprinkler System and Generator Fuel.

1.2 The Department will review the process for network devices configured for availability.

1.3 The Department will update its documentation to reflect the current environment.

1.3 The Department will update its documentation to reflect the current environment.

Processing Integrity

1.1 The Department will review automation tool process for notification when storage levels fall below pre-determined levels.

1.1 The Department will review and update maintenance contracts for fire suppression system and maintenance contracts for fire extinguishers.

1.1 The Department will review scheduled monthly and semi-annual inspection contracts on a regular basis.

1.1 The Department will review on a periodic basis maintenance contracts for fiber optic and VOIP equipment.

1.1 The Department will review process to determine if hardware devices are supported by vendor

1.2 The Department will review State Taxes and correct them to ensure the rates are updated.

1.5 The Department will work to ensure the report pickup procedures are followed.

1.5 The Department will work to ensure the report pickup procedures are followed.

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)
TOTAL	**460**	**218**	**242**

*12 of 37 hires were from consolidation.
**3 of the 20 hires were from consolidation.
***3 of the 55 hires were from consolidation

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

1. Board of Higher Education
2. Capital Development Board
3. Chicago State University
4. Commission on Government Forecasting and Accountability
5. Court of Claims
6. Department of Agriculture
7. Department of Central Management Services
8. Department of Children and Family Services
9. Department of Commerce and Economic Opportunity
10. Department of Corrections
11. Department of Corrections-Correctional Industries
12. Department of Employment Security
13. Department of Financial and Professional Regulation
14. Department of Healthcare and Family Services
15. Department of Human Rights
16. Department of Human Services
17. Department of Insurance
18. Department of Juvenile Justice
19. Department of Labor
20. Department of Lottery
21. Department of Military Affairs
22. Department of Natural Resources
23. Department of Public Health
24. Department of Revenue
25. Department of Transportation
26. Department of Veterans' Affairs
27. Department on Aging
28. Eastern Illinois University
29. Environmental Protection Agency
30. Executive Ethics Commission
31. General Assembly Retirement System
32. Governors State University
33. Guardianship and Advocacy Commission
34. House of Representatives
35. Human Rights Commission
36. Illinois Arts Council
37. Illinois Civil Service Commission
38. Illinois Commerce Commission
39. Illinois Comprehensive Health Insurance Plan
40. Illinois Community College Board
41. Illinois Council on Developmental Disabilities
42. Illinois Criminal Justice Information Authority
43. Illinois Deaf and Hard of Hearing Commission
44. Illinois Educational Labor Relations Board
45. Illinois Emergency Management Agency
46. Illinois Finance Authority
47. Illinois Gaming Board
48. Illinois Health Information Exchange Authority
49. Illinois Historic Preservation Agency

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

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

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

102. State Universities Retirement System
103. Supreme Court of Illinois
104. Teachers' Retirement System of the State of Illinois
105. University of Illinois
106. Western Illinois University

Listing of User Agencies of the Accounting Information System

(Not Examined)

1. Board of Higher Education
2. Capital Development Board
3. Department of Agriculture
4. Department of Central Management Services
5. Department of Corrections
6. Department of Financial and Professional Regulation
7. Department of Human Rights
8. Department of Insurance
9. Department of Juvenile Justice
10. Department of Labor
11. Department of the 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. Environmental Protection Agency
19. General Assembly Retirement System
20. Guardianship and Advocacy Commission
21. Historic Preservation Commission
22. Human Rights Commission
23. Illinois Arts Council
24. Illinois Civil Service Commission
25. Illinois Commerce Commission
26. Illinois Community College Board
27. Illinois Council on Developmental Disabilities
28. Illinois Criminal Justice Information Authority
29. Illinois Deaf and Hard of Hearing Commission
30. Illinois Educational Labor Relations Board
31. Illinois Emergency Management Agency
32. Illinois Gaming Board
33. Illinois Labor Relations Board
34. Illinois Law Enforcement Training and Standards Board
35. Illinois Office of the State's Attorneys Appellate Prosecutor
36. Illinois Prisoner Review Board
37. Illinois Procurement Policy Board
38. Illinois Racing Board
39. Illinois Student Assistance Commission

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

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

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

1. Capital Development Board
2. Department of Agriculture
3. Department of Central Management Services
4. Department of Employment Security
5. Department of Financial and Professional Regulations
6. Department of Human Rights
7. Department of Military Affairs
8. Department of Public Health
9. Department of Transportation
10. Department of Veterans' Affairs
11. Department on Aging
12. Environmental Protection Agency
13. Historic Preservation Agency
14. Illinois Arts Council
15. Illinois Criminal Justice Information Authority
16. Illinois Deaf and Hard of Hearing Commission
17. Illinois Law Enforcement Training and Standards Board
18. Illinois Office of the State's Attorneys Appellate Prosecutor
19. Office of Management and Budget
20. Office of the Attorney General
21. Office of the Governor
22. Office of the Lieutenant Governor

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

Listing of User Agencies of the Central Payroll System

(Not Examined)

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

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

Listing of User Agencies of the Central Time and Attendance System

(Not Examined)

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

Listing of User Agencies of the eTime System

(Not Examined)

1. Capital Development Board
2. Department of Agriculture
3. Department of Central Management Services
4. Department of Commerce and Economic Opportunity
5. Department of Financial and Professional Regulations
6. Department of Human Rights
7. Department of Insurance
8. Department of Labor
9. Department of the Lottery
10. Department of Public Health
11. Department of Revenue
12. Executive Ethics Commission
13. Guardianship and Advocacy Commission
14. Illinois Comprehensive Health Insurance Plan
15. Illinois Deaf and Hard of Hearing Commission
16. Illinois Heath Information Exchange Authority
17. Illinois Prisoner Review Board
18. Illinois State Police
19. Illinois Workers' Compensation Commission
20. Property Tax Appeal Board
21. State Employees' Retirement System of Illinois

Listing of Security Software Proxy Agencies
(Not Examined)

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

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

ACRONYM GLOSSARY

ACL – Access Control List
ADC – Alternate Data Center
AIS – Accounting Information System
BCCS – Bureau of Communications and Computer Services
Bureau – Bureau of Communications and Computer Services
BRM – Business Reference Model
CAC – Change Advisory Committee
CCF – Central Computer Facility
CFO – Chief Fiscal Officer
CICS – Customer Information Control System
CIRT – Critical Incident Response Team
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
CTAS – Central Time and Attendance
CTO – Chief Technology Officer
DASD – Direct Access Storage Device
DB2 – Database 2
DCMS – Department of Central Management Services
Department – Department of Central Management Services
DNS – Domain Name Service
DP – Data Processing
DR – Disaster Recovery
EAA – Enterprise Application & Architecture
ECM – Enterprise Change Management
EoL – End of Life
ePAR – Electronic Personnel Action Request
EPMO – Enterprise Program Management Office
ESR – Enterprise Service Request
EUC – End User Computing
FISMA – Federal Information Security Management Act
FY – Fiscal Year
HIPAA – Health Insurance Portability and Accountability Act
HR – Human Resources
ICN – Illinois Century Network
ID – Identification
ISD – Infrastructure Services Division
ILCS – Illinois Compiled Statutes

IMS – Information Management System
IT – Information Technology
ITG – Information Technology Governance
LAN – Local Area Network
MORT – Major Outage Response Team
NCC – Network Control Center
NIST– National Institute of Standards and Technology
PAR – Personnel Action Request
PIR – Post Implementation Review
PKI – Public Key Infrastructure
POP – Point of Presence
RACF – Resource Access Control Facility
RFC – Request for Change
RMF – Resource Monitoring Facility
RTC – Regional Technology Center
RTO – Recovery Time Objective
SSL – Secure Socket Level
UPS – Uninterruptible Power Supply
VOIP – Voice Over Internet Protocol
VPN – Virtual Private Network
WAN – Wide Area Network
z/OS – Zero Downtime Operating System
z/VM – Zero Downtime Virtual Machine