



---

**STATE OF ILLINOIS**

---

**OFFICE OF THE AUDITOR GENERAL**

---

**SERVICE ORGANIZATION CONTROL REPORT**  
**DEPARTMENT OF CENTRAL MANAGEMENT SERVICES**  
**BUREAU OF COMMUNICATIONS &**  
**COMPUTER SERVICES**

**JULY 2012**

---

---

**WILLIAM G. HOLLAND**

---

**AUDITOR GENERAL**

---



**SERVICE ORGANIZATION CONTROL  
REPORT**

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

**July 2012**



## TABLE OF CONTENTS

Management of the Department of Central Management Services' Assertion Regarding the State of Illinois Information Technology Environment 'System' .....	1
Independent Service Auditor's Report .....	5
Description of the Department of Central Management Services, Bureau of Communications and Computer Services' State of Illinois Information Technology Environment 'System' .....	11
Background .....	11
Components of the System .....	11
Infrastructure .....	11
Software .....	12
People .....	14
Procedures .....	18
Data .....	18
Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring of Controls .....	19
Control Environment.....	19
Security Policies .....	20
Risk Assessment Process .....	24
Information and Communication Systems .....	24
Monitoring Controls.....	24
Boundaries of the System.....	25
Trust Services Criteria and Related Controls.....	26
Complementary User-Entity Controls.....	27
Description of Test of Controls and Results Thereof.....	29
Trust Services - Security Principle, Criteria, Related Controls and Test of Controls.....	30
Trust Services - Availability Principle, Criteria, Related Controls and Test of Controls .....	67
Trust Services - Processing Integrity Principle, Criteria, Related Controls and Test of Controls.....	113
Other Information Provided by the Department that is Not Covered by the Service Auditor's Report .....	165
Department's Corrective Action Plan.....	166
Department's Analysis of Staffing Trends .....	172
Department's Information Related to the New Alternate Data Center .....	173
Listing of User Agencies of the State of Illinois Information Technology Environment .....	174
Listing of User Agencies of the Accounting Information System .....	176
Listing of User Agencies of the Central Inventory System .....	177
Listing of User Agencies of the Central Payroll System.....	178
Listing of User Agencies of the Central Time and Attendance.....	179
Acronym Glossary .....	180



Management of the Department of Central Management Services, Bureau of Communications and Computer Services' Assertion Regarding the State of Illinois Information Technology Environment 'System' for the Period July 1, 2011 to June 30, 2012

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 Information Technology Environment 'System' Throughout the Period July 1, 2011 to June 30, 2012" (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 Information Technology Environment, particularly system controls intended to meet the criteria for the security, availability, and processing integrity principles set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that:

a. The description fairly presents the State of Illinois Information Technology Environment 'System' throughout the period July 1, 2011 to June 30, 2012 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

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

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

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

(9) Relevant details of changes to the Department of Central Management Services, Bureau of Communications and Computer Services, State of Illinois Information Technology Environment during the period covered by the description

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

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





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

Acting Deputy Director

Date 7/2/12

**This page intentionally left blank**

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



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

**Office Of The Auditor General**  
**William G. Holland**

## **INDEPENDENT SERVICE AUDITOR'S REPORT**

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

We have examined the attached description titled “Description of the Department of Central Management Services, Bureau of Communications and Computer Services’ State of Illinois Information Technology Environment ‘System’” throughout the period July 1, 2011 to June 30, 2012 (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 TSP Section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, and Processing Integrity (AICPA, *Technical Practice Aids*) (applicable trust services criteria), throughout the period July 1, 2011 to June 30, 2012. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of the Department of Central Management Services, Bureau of Communications and Computer Services’ controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

### *Service organization’s responsibilities*

The Department of Central Management Services, Bureau of Communications and Computer Services has provided the attached assertion titled “Management of the Department of Central Management Services, Bureau of Communications and Computer Services’ Assertion Regarding the State of Illinois Information Technology Environment ‘System’” throughout the period July 1, 2011 to June 30, 2012, 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; 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, 2011 to June 30, 2012.

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 accompanying description of the Department of Central Management Services, Bureau of Communications and Computer Services State of Illinois Information Technology Environment 'System' on page 21 states "changes to applications, such as the common systems (Accounting Information System, Central Inventory System, Central Payroll System and the Central Time and Attendance System) follow the Enterprise Application & Architecture (EAA) Change Management Flowchart". However, as noted on pages 118 to 120 of the Description of Tests of Controls and the Results Thereof, the Flowchart does not include requirements for:

- Management approvals,
- Assignment of a unique tracking number,
- Prioritization or categorization of the request,

- Testing or documentation of testing requirements, and
- Requirements for a post implementation review.

As a result, the controls are not suitably designed to meet the criterion “Controls provide reasonable assurance that only authorized, tested, and documented changes are made to the system.”

In addition, the description of the Department of Central Management Services, Bureau of Communications and Computer Services State of Illinois Information Technology Environment ‘System’ states that in order for an individual’s mainframe password to be reset, an email with the individual’s name, agency, mainframe ID and telephone number was to be emailed to the Help Desk. The Help Desk or the Department’s Coordinator was to verify the information and phone the individual with the temporary password. Temporary passwords were not to be left on voice mail or emailed to the individual. However, as noted on pages (45-47, 90-93, 134-137) of the Description of Tests of Controls and the Results Thereof, the Department’s Coordinator would receive telephone calls and direct emails requesting mainframe password resets. In the event the individual would telephone the Department’s Coordinator, who would reset the password at that time. If the individual would send an email, the Department’s Coordinator would respond to the email with the temporary password. Thus, control over the reset of mainframe passwords were not operating effectively throughout the period July 1, 2011 to June 30, 2012. This control deficiency resulted in not meeting the criterion “The process to make changes and updates to user profiles.”

In addition, the description of the Department of Central Management Services, Bureau of Communications and Computer Services State of Illinois Information Technology Environment ‘System’ states “Department staff have been assigned responsibility for monitoring and ensuring compliance with security policies.” According to the security policies, the Department and security personnel were responsible for the monitoring, auditing, tracking, and for the validation of compliance with the policies and procedures. Additionally, they were responsible for investigating violations of laws, policies, and procedures. However, as noted on pages (57, 102-103, 147) of the Description of Tests of Controls and the Results Thereof, the security policies did not define who security personnel were and we were unable to determine who, within the Department, was responsible. Thus, controls over the monitoring of noncompliance with security policies were not operating effectively throughout the period July 1, 2011 to June 30, 2012. This control deficiency resulted in not meeting the criterion “Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.”

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

- a. the description fairly presents the system that was designed and implemented throughout the period July 1, 2011 to June 30, 2012.

- 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, 2011 to June 30, 2012, and user entities applied the complementary user-entity controls contemplated in the design of the Department of Central Management Services, Bureau of Communications and Computer Services' controls throughout the period July 1, 2011 to June 30, 2012.
- c. the controls tested, which together with the complementary user-entity 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, 2011 to June 30, 2012.

#### *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."

#### *Supplementary information*

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 the new alternate data center, staffing trends, user agency listings, and 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 service organization's description of the State of Illinois Information Technology Environment made available to user entities during the period from July 1, 2011 to June 30, 2012. Information about the Department of Central Management Services, Bureau of Communications and Computer Services new alternate data center, staffing trends, user agency listing, and the Department's Corrective Action Plan have not been subjected to the procedures applied in the examination of the description of the State of Illinois Information Technology Environment 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 Information Technology Environment, and accordingly, we express no opinion on it.

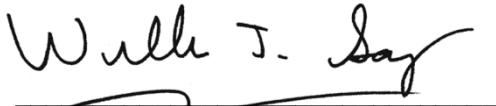
#### *Intended use*

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 entities of the "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' State of Illinois Information Technology Environment" during some or all of the period July 1, 2011 to June 30, 2012, the Auditor General, the General Assembly, the Legislative Audit Commission, the Governor, and independent auditors and practitioners providing services to such user entities, 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 entities, subservice organizations, and other parties
- Internal control and its limitations

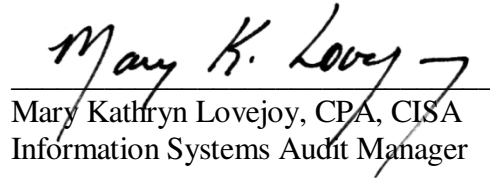
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

However, this report is a matter of public record and the distribution is not limited.



---

William J. Sampias, CISA  
Director, Information Systems Audits



---

Mary Kathryn Lovejoy, CPA, CISA  
Information Systems Audit Manager

July 2, 2012  
Springfield, Illinois

This page intentionally left blank



**DESCRIPTION OF THE  
DEPARTMENT OF CENTRAL MANAGEMENT SERVICES  
BUREAU OF COMMUNICATIONS AND COMPUTER SERVICES  
STATE OF ILLINOIS INFORMATION TECHNOLOGY ENVIRONMENT 'SYSTEM'  
THROUGHOUT THE PERIOD JULY 1, 2011 TO JUNE 30, 2012**

**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, maintaining, and delivering of voice, data, wireless, video, Internet, and telecommunications services to all state government agencies, boards, and 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.
- Maintains common applications which state government agencies, boards and commission may utilize to meet their financial requirements.

**Components of the System**

The System is comprised of the following components:

- Infrastructure (facilities, equipment, and networks),
- Software (systems, applications, and utilities),
- People (developers, operators, users, and managers), and
- Data (transaction streams, files, databases, and tables).

The following sections of this description define each of these five components comprising the System.

**Infrastructure**

The State of Illinois Information Technology Environment is housed at the Central Computer Facility (CCF), Communications Building and additional facilities throughout the State. Residing at the CCF are the supporting mainframe operating system platforms, networking components (firewalls, routers, switches), and data storage devices.

The Department is responsible for supporting and maintaining four mainframe units, which are configured into 11 production systems and 6 test systems. In addition, the Department is responsible for installing, maintaining and managing the Illinois Century Network, including approximately 3,800 circuits, egress circuits, routers, firewall, switches, fifteen Point-of-Presence sites, and various monitoring tools. The Department also maintains the Enterprise Virtual Private Network solution which allows the Department and user agencies to connect remotely to resources. The Department has configured the network in a redundant manner.

The Department maintains Direct Access Storage Devices (DASD), and tape drives for reading and writing tapes in order to provide backup and storage services.

The Department utilizes encryption technologies and access gateways for the transmission of sensitive or confidential information.

## **Software**

The Department provides a mainframe hosting environment for user agencies. The mainframe hosting services include development, testing and acceptance environments. The mainframe operating system software includes:

- The primary operating system is Zero Downtime Operating System (z/OS). z/OS is a complex operating system used on mainframes and functions as the system software that controls the initiation and processing of work within the computer. The System Management Facility (SMF) records the activity within the operating system.
- z/Virtual Machine (z/VM) is a time-sharing, interactive, multi-programming operating system for mainframes. The major subsystem supported in z/VM is NOMAD, which is business intelligence software for enterprise reporting and rapid application development.
- 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, which the Department makes available. The Department has established more than ten subsystems.
- 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”. The IMS applications can access IMS, DB2 and CICS data files. Users control their own TIMS and GIMS RACF definitions.

In addition, the Department maintains four applications, known as the “common systems”, which all State agencies, boards, and commissions may utilize:

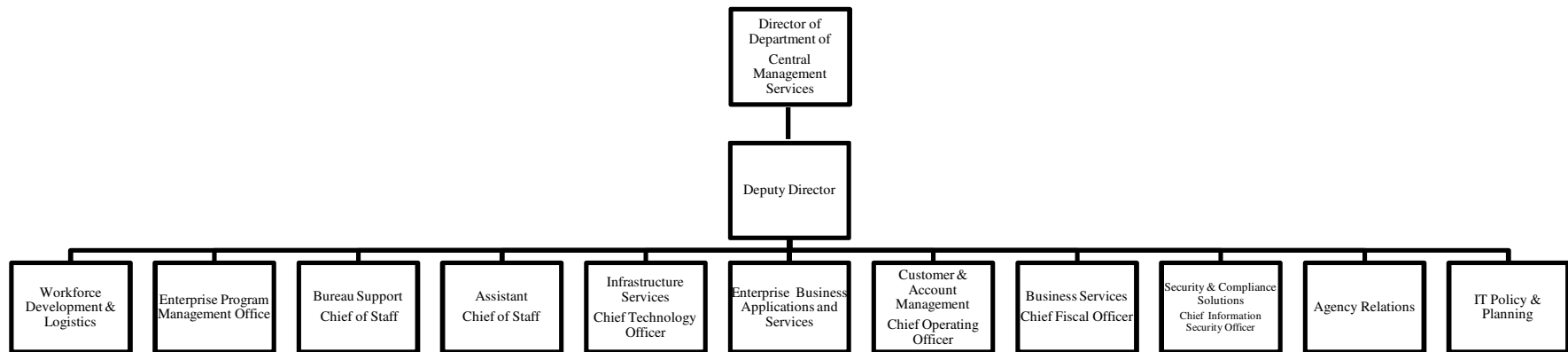
- The Accounting Information System (AIS) is an automated expenditure control and invoice voucher processing system. Appropriation, obligation, cash and vendor processing functions support the invoice processing. AIS allocates invoice amounts into sub accounts and allows users to track cost centers. Vouchers are created in AIS

according to the Comptroller's Statewide Accounting Management System (SAMS) procedures.

- The Central Inventory System (CIS) is an automated asset inventory control system, which also allows the user agency to track depreciation. CIS allows user agencies to maintain records of inventory and to comply with the Department's Property Control Division's rules of reporting and processing.
- The Central Time and Attendance System (CTAS) is an online system used to maintain "available benefit time". CTAS provides for attendance information to be recorded using either the positive or exception method.
- The Central Payroll System (CPS) provides assistance in preparing payrolls for state agencies. CPS enables State agencies to maintain automated pay records and generates a file that is submitted to the Comptroller's Office for the production of payroll warrants.

## People

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



### Deputy Director

The Deputy Director of the Bureau of Communications and Computer services is responsible for the overall management of all Information Technology and Telecommunication functions, which includes services provided to all state agencies as well as other Illinois government entities. The Deputy Director works with Department senior management, the Governor's Office and the State 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. Customer and Account Management is the single point of contact for user service requests, service provisioning, and incident management.

- Customer Service Center (CSC)  
The CSC serves as the central point of contact for telecommunications and information technology users. The CSC serves as a Service Desk to handle process and manage incidents and requests for services.
- Communications Management Center (CMC)  
The CMC is responsible for all network trouble resolutions, surveillance and ongoing technical support. The CMC is operational 24x7, and handles after hours calls of the Customer Service Center (CSC).
- Field Operations / Regional Technology Centers (RTC)  
Field Operations is responsible for maintaining nine Regional Technology Centers located throughout the State and assisting Network Services in maintaining Illinois Century Network Point-of-Presence (POP) sites throughout the State.
- Network Services  
Network Services is responsible for management and oversight of the Illinois Century Network (ICN), the Illinois Wireless Information Network, and all engineering responsibilities related to State of Illinois telecommunications services.
  - Network Operations is responsible for installing, maintaining and managing the ICN Backbone including backbone circuits, egress circuits, routers, firewalls, switches, fifteen Point-of-Presence (POP) sites, WAN monitoring tools and WAN services. Additionally, Network Operations provides tier III network support to other staff within Network Services.
  - Enterprise Network Support is responsible for design and support of State agencies network access. Responsibilities include installation and support of access routers, WAN switches, VOIP, video conferencing, fiber, DNS, and Internet. Network Integration also performs tier III technical support for the 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 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 coordinate and facilitate 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 Technology Officer

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

- Data Center Operations

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

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

- Enterprise Production/Operations

Library Services is responsible for media initiation, inventory, tracking, lifecycle management, and business continuity media management.

Production Control is responsible for computer job scheduling and monitoring.

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

- LAN Services

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

### Enterprise Business Applications and Services

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

### Agency Relations

Agency Relations Liaisons (ARL) establishes and maintains user relationships, and serves as an advocate and facilitator. Agency Relations primary focus is user relationship management, event coordination and marketing and communications.

### 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).

### IT Policy and Planning

The IT Policy and Planning division performs senior-level project management and serves as a policy and planning advisor to the Deputy Director.

### Chief Information Security Officer

The Chief Information Security Officer serves as a policy making official responsible for the 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

Security and Compliance Solutions has the following responsibilities:

- Provides the IT security program statewide to agencies
- Communicating security principles through issuance of policy 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,
- Developing and maintaining the statewide disaster recovery services for the State’s Information Technology infrastructure.

## **Procedures**

The Department has developed and communicated to Department staff security procedures over the following areas:

- Data classification,
- Authorization, changes and termination of information system access,
- System security administration,
- Network operations,
- Maintenance and support of systems and necessary backups and off site storage,
- Maintenance of restricted access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices, and
- Incident response (physical and logical).

## **Data**

The Department provides four applications (AIS, CIS, CPS and CTAS) which user agencies may utilize. The origination, input, accuracy and output of information is the responsibility of the user agencies. Each transaction entered is assigned an identifying number.

User manuals provide guidance to users on data entry, edits, and error correction procedures. Additionally, the manuals outline various reports which the user agency may produce.

Distribution of digital output is restricted to authorized users through the management of system software tools or online viewing software. Distribution of hardcopy output is restricted through physical and manual controls. Hardcopy output is printed at a secure facility with security guards. Upon request for pick up, the individual must identify themselves and be verified against an authorization listing.



## **RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION SYSTEMS, AND MONITORING OF CONTROLS**

### **Control Environment**

#### 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 and user's data and information. The Bureau of Communications and Computer Services management meets weekly to ensure the importance of security is passably communicated to all levels within the Department. The Department has established overall security policies and procedures, which have been communicated to staff and users, via the website. In designing its controls, the Department has taken into consideration the relevance of the control in order to meet the relevant trust criteria.

#### Security Management

The Chief Information Security Officer, along with Department staff are responsible for the development and management of security over the State of Illinois Information Technology Environment. The Chief Information Security Officer is responsible for the policy development, planning, implementation, and administration. The security policies are reviewed and approved by the Department's Director, Deputy Director, Deputy General Counsel and the Chief Information Security Officer.

The common system application managers are responsible for the development and management of the applicable user manuals.

Department staff are assigned the responsibility for the monitoring and ensuring compliance with the security policies.

During the annual security training and awareness program, new Department staff are required to sign a statement signifying that they have read, understand, and will comply with the security policies. Additionally, Department staff reconfirm their compliance with the security policies through the annual security training. Contractors are required to take the annual security awareness training and certify they will comply with all security policies.

The Department adheres to the State's hiring procedures for the hiring of staff. The Department's position descriptions, which define job requirements are available upon request and are posted for open positions. Additionally, Department staff are notified when position descriptions are updated.

Annual performance evaluations are completed. Staff is provided training based on their position's requirements. The Department conducts cross training for key positions.

The Department's Security and Compliance Solutions Division participates in user groups and subscribes to services related to computer viruses.

## **Security Policies**

The following policies and related processes identify and document the physical and logical security, availability, and processing requirements of Department staff and users:

### Information Technology Policies

- Data Classification and Protection 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,
- 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,
- Wireless Communication Device Policy.

### User Manuals

- Accounting Information System User Manual,
- Central Inventory System User Manual,
- Central Payroll System User Manual, and
- Central Time and Attendance System User Manual.

## **Personnel Security**

Background checks are performed on all Department staff requiring access to Department resources. Department employees are subject to the Department's procedures/process for accessing systems. Additionally, Department staff and users are instructed to report security incidents/issues to the Department's Help Desk or supervisor.

## Physical Security

The Central Computing Facility (CCF) and Communications Building, which house the State of Illinois Information Technology Infrastructure, provide the following features:

- The CCF and the Communications Building maintain high security standards for building access and perimeter monitoring. The interior and exterior of the facilities are monitored and access enforced by card key access. In order to obtain a card key, an ID Badge Request Form is to be completed and approved by the authorized manager. In addition, a valid ID must be presented.
- Visitors are required to be escorted, in addition to signing in and out.
- The facilities are guarded by security guards 24x7. Video surveillance is used to monitor the CCF and the Communications Building and is monitored by the security guards.
- The fire detection devices are monitored by the Command Center. The monitoring system informs the Command Center of the specific alarm. The CCF computer room fire suppression system is Underwriter Laboratory approved and utilizes an environmentally friendly agent; FM-200. Additionally, the CCF and the Communications Building have fire extinguishers installed throughout each facility.
- The CCF has sensors installed below the raised floor to detect water leakage.
- The CCF and the Communications Building are equipped with uninterruptible power supplies (UPS) in the event of a power failure. In the event of a power failure, the UPS would engage immediately drawing power from the battery farm and generators.

The Department's offsite storage facility has physical access controls in place. Additionally, only authorized Department staff are able to access the offsite storage facility.

The Department has preventive maintenance agreements in place and conducts scheduled maintenance for key system hardware components.

## Change Management

The Department has implemented a formal change management process which requires tracking, approval, testing, and backout plans for infrastructure changes. Changes to the infrastructure (except for the common system applications) are initiated as the result of an ESR (Enterprise Service Request), a configuration change, or an internal work assignment. The Remedy Change Control System is used to create, review, approve and track change requests.

Infrastructure change requests are reviewed by the Change Management Unit. Infrastructure changes to be reviewed are made available to members of the Change Advisory Council (CAC) before the meeting. In addition, the results of the meeting are made available via the ECM SharePoint site. Users have access to the ECM SharePoint site.

Emergency infrastructure changes follow the defined change management process, but at an accelerated timeline.

Changes to applications, such as the common systems, follow the EAA Change Management Flowchart. Change requests may originate via Remedy or the Enterprise Project Management

system. Once management determines the type of change, the change is to be tracked via Remedy or the Enterprise Project Management system.

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

Standards provide guidance on the configuration and deployment of network devices. Tools are in place to assist in the deployment of and reporting on configurations.

The IT Governance process governs the acquisition of systems, and technology. As part of the IT Governance process, user agencies are to classify their data in accordance with the Data Classification and Protection Policy.

### System Monitoring

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 Department utilizes various tools to review and assess the infrastructure and vulnerabilities.

### Problem Management

Department staff and users are instructed to contact the Customer Service Center (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 records the incident, as well as the user name, agency, contact and a detailed incident description. The ticket is tracked through Remedy until resolution.

### Backup and Recovery

The Department provides recovery services for the mainframe infrastructure in order to minimize the risk of disrupted services or loss of resources using vendor contracted services. The recovery of the user agency applications and data are the responsibility of the user agency.

The Department maintains information on State agencies critical applications, via the Business Reference Model. State agencies are required to categorize, prioritize and define critical information. This information informs the Department of the required recovery capacity needs.

The Department has developed policies and procedures, which are tested annually, to assist with the recovery of the infrastructure.

System data is backed up daily and weekly, with the weekly copies sent to the off-site storage facilities. Access to backup devices, scheduling utilities, systems, and media is restricted to authorized staff.

The Department maintains an inventory of the backups, along with their location. An annual verification is conducted.

### System Account Management

Resource Access Control Facility (RACF) security software is utilized to restrict access to defined systems, subsystems, and applications (common systems). RACF enforces the individual's accountability over data and system resources by positively verifying the individual's authority to utilize the system resource or data.

A user ID is used to identify the client along with a password to verify the user's identity. The Department maintains a log of all access attempts, which is used to monitor unauthorized access attempts and identify areas of weakness. System options and parameters are implemented to protect data and resources.

Users are required to establish their identity and authenticate to systems and applications through the use of user IDs and passwords. Unique user IDs are assigned to individual users, with the sharing of individual IDs prohibited. Password configurations have been established.

Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form and submit via a Remedy Enterprise Service Request. The Mainframe Application Access Request Form indicates the access required and proper approval. Changes, updates, and password resets to Department and proxy agency user profiles are completed by the Department's RACF Coordinator and/or the RACF Security Administrator. Changes are made based on the approved Mainframe Application Access Request Form submitted via a Remedy Enterprise Service Request.

In order for an individual's mainframe password to be reset, an email with the individual's name, agency, mainframe ID and telephone number is to be emailed to the Help Desk. The Help Desk or the Department's RACF Coordinator is to verify the information and phone the individual with the temporary password. Temporary passwords are not to be left on voice mail or emailed to the individual.

Bi-monthly the Department's RACF Coordinator receives a separation report documenting separations. The Department's RACF Coordinator will review and revoke the user's ID. Bi-annually, the Department's RACF Coordinator will send all agencies a listing of their respective users, requesting the agency to review for accuracy, note any modifications, and return to the Department.

Network Services requires manager review and approval of new access rights. LAN Services utilized the LAN Services Access Authorization in order for staff to obtain access rights. Network Services is notified by Personnel of changes in an individual's employment status and makes changes to user's access rights accordingly. Changes to LAN Services staff access rights are made based on the approved LAN Services Access Rights Authorization.

Operating system configuration defaults are restricted to authorized personnel through logical access controls. Utility programs that can read, add, change or delete data or programs are restricted to authorized personnel. Master passwords are maintained in an encrypted database and maintained in a secure safe. Authentication servers are utilized to control access, log access attempts, and alert management.

### **Risk Assessment Process**

The Security and Compliance Solutions Division assess security risk on an ongoing basis. As security threats are identified, the specific risk is assessed. Additionally, regular meetings with management and users are held to discuss security and risk issues.

Department management considers technological developments, and laws and regulations during the planning process. Additionally, management conducts meetings with user agencies to determine their future needs.

### **Information and Communication Systems**

The Department's security policies, website and user manuals assist in ensuring Department staff and users are aware of their individual roles and responsibilities concerning the security, availability, and processing integrity over the State of Illinois Information Technology Environment. Additionally, the Department communicates security events and issues to Department staff and users via email, phone and postings on the Department's website.

The security policies outline the responsibilities of the Department and the users:

- It was the responsibility of the users to understand the applicable policy and to follow the corresponding procedures.
- The Resource Custodians were responsible for understanding and adhering to the policies and for granting, reviewing, and removal of access to resources.
- The Department and security personnel were responsible for the monitoring, auditing, tracking, and for the validation of compliance with the policies and procedures. Additionally, they were responsible for investigating violations of laws, policies, and procedures.

The Department has published on their website the Service Catalog, which documents the services provided, in addition to the availability of specific systems. The Service Catalog documents the commitments and obligations of the Department and users.

### **Monitoring Controls**

The Department utilizes various tools to review and assess the infrastructure and vulnerabilities. Logs are analyzed; either manually or by automated tools, to identify trends that may have the potential to impact the Department's ability to achieve system security objectives. Security issues are addressed with management at various meetings.

## **BOUNDARIES OF THE SYSTEM**

The Department of Central Management Services provides all state government agencies, boards, and commissions an 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), and data storage devices. The Department maintains and provides four applications which are utilized by multiple agencies; Accounting Information System, Central Inventory System, Central Time and Attendance System and the Central Payroll System; however, the input and integrity of the data is the responsibility of the user and therefore, is 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 Security Principle, Availability Principle, and Processing Integrity Principal Criteria's, along with the Related Controls, and Test of Controls, they are an integral part of the State of Illinois Information Technology Environment System's description.



## COMPLIMENTARY USER-ENTITY 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 Information Technology Environment should maintain controls to provide reasonable assurance that:

- User agencies have reviewed and adhere to the security policies located on the Department's website.
- User agencies have communicated to the Department their specific security requirements.
- User agencies have informed the Department's Help Desk in a timely manner of any security, availability or processing issues.
- User agencies have classified their applicable applications and data based on criticality and sensitivity.
- User agencies have reviewed, updated, approved, and returned to the Department on a bi-annual basis their applicable user listings.
- User agencies are effectively utilizing security software features and perform periodic reviews of existing profiles to ensure that access rights are appropriate.
- User agencies have reviewed the effectiveness of critical manual controls over the common systems, 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 common systems.
- User agencies regularly review the users and user groups with access to the common systems 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.
- User agencies develop and maintain appropriate and viable business continuity plans, application recovery scripts, designated application information updates to the Business Reference Model, recovery exercise procedures and schedules, and ongoing communications with the Department.

This page intentionally left blank

## Description of Test of Controls and Results Thereof

## **TRUST SERVICES - SECURITY PRINCIPLE, CRITERIA, RELATED CONTROLS AND TEST OF CONTROLS**

The system is protected against unauthorized access (both physical and logical).

### **1.0 – Policies: The entity defines and documents its policies for the security of its system.**

Criteria: 1.1 - The entity's security policies are established and periodically reviewed and approved by a designated individual or group.

Department's Control: The security policies addressing logical and physical security are reviewed and approved by the Department's Director, Deputy Director, Deputy General Counsel and the Chief Information Security Officer. The Department has implemented security policies, which are posted on the Department's website.

Test Performed: Reviewed policies, Department's website, position description, and interviewed staff.

Test Results: According to the Chief Information Security Officer's position description, he was responsible for "policy development, planning, implementation and administration." Additionally, the Chief Information Security Officer was responsible for the development of "confidential comprehensive IT security plans and procedures."

The following policies, including but not limited to, were posted on the Department's website.

- Data Classification and Protection Policy, revised January 3, 2012
- General Security for Statewide IT Resources Policy, revised January 1, 2010
- General Security for Statewide Network Resources Policy, revised January 1, 2010
- IT Resource Access Policy, effective December 1, 2007
- Laptop Data Encryption Policy, revised January 1, 2010
- Statewide CMS/BCCS Facility Access Policy, revised January 1, 2010
- Change Management Policy, revised January 3, 2012
- Data Breach Notification Policy, revised January 1, 2010
- Action Plan for Notification of a Security Breach, effective August 31, 2007
- Electronically Stored Information Retention Policy, effective February 15, 2009
- IT Governance Policy, revised January 3, 2012
- Mobile Device Security Policy, effective October 1, 2009

The Department had implemented policies, which addressed logical and physical security. We reviewed the policies, noting they were reviewed and approved by the Department's Director, Deputy Director, Deputy General Counsel, and the Chief Information Security Officer.

During our review of the policies, we noted there was no formal policy requirement for periodic or routine reviews; however, four policies were updated during the review period.

A formal requirement to ensure periodic reviews of policies did not exist.

Criteria: 1.2 - The entity's security policies include, but may not be limited to, the following matters:

Criteria: A - Identifying and documenting the security requirements of authorized users.

Department's Control: The security policies identify and document the general security requirements.

Test Performed: Reviewed policies and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy defined the general security measures specific to the IT resources managed by the Department. The Policy outlined security measures related to validating a user's identity prior to use of resources, general controls over confidential and sensitive information, and security awareness training requirements. The Policy also stated in the event of any actual or suspected security breaches the individual was to report the issue to their immediate supervisor.

The General Security For Statewide Network Resources Policy defined the general security measures specific to the network environment managed by the Department. The Policy outlined the general standards for firewall/intrusion detection devices, wireless LANs, content filtering, vulnerability assessments, remote access, WAN, internet services, and off-net services.

The IT Resource Access Policy documented the general requirements in order to obtain physical and/or logical access to Department resources and facilities. In order to obtain access, an individual's identity was required to be validated, background check completed, and a business justification provided. Individuals requiring access to resources were to be provided a badge, digital certificate, and a user ID. Upon separation, access was to be revoked and all badges were to be returned to the Department.

The Statewide CMS/BCCS Facility Access Policy defined the requirements for the granting and revocation of an individual's physical access privileges to the Department's facilities. The Policy stated in order to obtain unescorted access to a Department facility, an individual was required to have a background check completed. In addition, an individual's identity was to be validated.

Additionally, the Statewide CMS/BCCS Facility Access Policy stated upon determination physical access was no longer required; the individual was required to return the access badge.

The Laptop Data Encryption Policy stated all newly issued and redeployed laptops were required to be equipped with full-disk encryption.

The Data Classification and Protection Policy stated data was to be classified into one of three categories; Public, Official Use Only, and Confidential. It was the responsibility of the data owner to determine the classification and to ensure appropriate security and protection protocols had been implemented.

The Mobile Device Security Policy defined the general security precautions; passwords, encryption, screen locking and timeout, to be taken with mobile devices. The Policy stated in the event a device was lost or stolen, the user was to report the incident to the Department's Help Desk.

No deviation noted.

Criteria: B - Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements.

Department's Control: The Data Classification and Protection Policy documents the data classification schema used to value and classify information generated, accessed, transmitted or stored. The IT Resource Access Policy documents the requirements for obtaining access to resources. The Electronically Stored Information Retention Policy documents the retention requirements for electronic information. The General Security For Statewide IT Resource Policy documents the destruction requirements.

Test Performed: Reviewed policies and interviewed staff.

Test Results: The Data Classification and Protection Policy was developed to inform "data owners and data users of the data classification and protection schema used by CMS/BCCS for protecting data." The Policy stated it was "applicable to all structured and unstructured data generated, accessed, transmitted, or stored on systems and networks managed by CMS/BCCS."

The Policy stated data was to be classified into one of three categories:

- Public,
- Official Use Only, and
- Confidential.

The Policy stated it was the responsibility of the data owner to determine the appropriate classification over their data and to ensure the appropriate security and protection protocols were in place. Additionally, the data owner was responsible for ensuring the proper sharing of information based on its classification.

According to the IT Resource Access Policy in order to obtain access to resources, a user was required to have a background check completed, their identity validated, and a business justification for access.

The Electronically Stored Information Retention Policy stated agencies were required to maintain records for the minimum period of time as outlined in the State Records Act (5 ILCS 160). In addition, agencies were required to obtain approval from the State Records Commission prior to the destruction of records.

According to the General Security For Statewide IT Resource Policy disclosure of confidential or sensitive information was to be restricted to authorized individuals. Additionally, the

destruction of confidential and sensitive information was to be conducted in accordance with agency specific procedures.

No deviation noted.

Criteria: C- Assessing risks on a periodic basis.

Department's Control: The IT Risk Assessment Policy documents the requirements for assessing risk.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: The IT Risk Assessment Policy stated the Department, along with the Business Owners, would conduct periodic risk assessments for “identifying threats and vulnerabilities and assessing the impact.” Additionally, risk assessments could include new systems, major modifications, application servers, networks, and processes by which the systems were administered.

The Policy also stated the Department would establish risk assessment criteria and classifications. In addition, the Department would appropriately address and remediate the risk identified in risk assessments.

No deviation noted.

Criteria: D - Preventing unauthorized access.

Department's Control: The IT Resource Access Policy documents controls for preventing unauthorized access.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: According to the IT Resource Access Policy, in order to ensure access was controlled, individuals requiring access to protected IT resources were to be “issued physical badges, and/or digital certificate, and/or an user ID.”

No deviation noted.

Criteria: E - Adding new users, modifying the access levels of existing users, and removing users who no longer need access.

Department's Control: The IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the Statewide CMS/BCCS Facility Access Policy documents the requirements for granting, assigning and revoking user access.

Test Performed: Reviewed policies and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated an individual's identity was to be validated prior to obtaining access to resources. Additionally, once it was determined an individual no longer required access, the individual was to return the IT resources and notify the appropriate parties.

In accordance with the IT Resource Access Policy, prior to obtaining access to Department resources, an individual was to have a completed background check and their identity verified. In addition, upon determination access was no longer required, the individual's rights were to be removed.

The IT Resource Access Policy stated prior to obtaining administrative access to Department resources; supervisory approval must be obtained.

However, the policies did not address the requirements for requesting and obtaining access; including but not limited to documentation, tracking, and approvals, periodic review of access rights and the process for revoking access.

The policies did not address the requirements for requesting, obtaining, modifying, removing, approving, or the periodic review of access rights.

Criteria: F - Assigning responsibility and accountability for system security.

Department's Control: The IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the General Security For Statewide Network Resource Policy document the responsibilities and accountability of system security.

Test Performed: Reviewed policies and interviewed staff.

Test Results: Each of the policies, noted above, contained the following general statements regarding responsibilities:

- It was the responsibility of the users to understand the applicable policy and to follow the corresponding procedures.
- The Resource Custodians were responsible for understanding and adhering to the policies and for granting, reviewing, and removal of access to resources.
- The Department and security personnel were responsible for the monitoring, auditing, tracking, and for the validation of compliance with the policies and procedures. Additionally, they were responsible for investigating violations of laws, policies, and procedures.

The General Security For Statewide IT Resources Policy outlined general security measures over the usage of State resources in which users were responsible for general provisions over resource use, credential rules, and inappropriate activities.

The General Security For Statewide Network Resources Policy stated it was a violation for users to circumvent the security measures put in place by the Department.



No deviation noted.

Criteria: G - Assigning responsibility and accountability for system changes and maintenance.

Department's Control: The Change Management Policy documents the responsibility and accountability of Department staff for system changes and maintenance.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: The Change Management Policy stated it was the responsibility of the Department and supported agency staff to familiarize themselves with the policy and the corresponding change management process.

The Policy stated all changes to the production IT environment would be subject to the change management process. The requests for changes would be reviewed and would ensure the appropriate communication to users had occurred.

No deviation noted.

Criteria: H - Testing, evaluating, and authorizing system components before implementation.

Department's Control: The Change Management Policy documents the process in which infrastructure changes are to follow.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: The Change Management Policy stated all changes to the production IT infrastructure were to follow the change management process. All changes required a completed Request For Change and review by the Change Advisory Committee.

The Policy did not address the requirements over testing and authorization of system components prior to implementation.

Requirements over testing and authorization of changes were not documented in the Policy.

Criteria: I - Addressing how complaints and requests relating to security issues are resolved.

Department's Control: The General Security For Statewide IT Resources Policy states users are responsible for disclosing any actions or behaviors involving a State IT resource and report on actual or suspected breaches.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated all security issue complaints and requests were to be directed to the individual's immediate supervisor. However,

we noted the Policy did not address the actions in which the supervisor was to take once a complaint or request was received.

The Policy did not address the entire process for reporting and resolving security issues.

Criteria: J - Identifying and mitigating security breaches and other incidents.

Department's Control: The General Security For Statewide IT Resources Policy and the Action Plan For Notification of a Security Breach documents the identification and notification of security breaches and other incidents.

Test Performed: Reviewed Policy, Plan, and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated if an event of misuse, theft, or abuse of information was identified, the individual was to report the event to their supervisor. However, we noted the Policy did not address the actions the supervisor was to take once a complaint or request was received. In addition, the Policy did not address the process for the identification of breaches or other incidents.

However, in the event a breach of personal information was determined, the Action Plan For Notification of a Security Breach documented the required actions to be taken. Upon determination of such a breach, the individuals were to be notified in accordance with the Personal Information Protection Act (815 ILCS 530).

The General Security For Statewide IT Resources Policy did not address the entire process for identifying, reporting, and mitigating security issues.

Criteria: K - Providing for training and other resources to support its system security policies.

Department's Control: The General Security For Statewide IT Resources Policy documents the security awareness training requirements for Department staff.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated new employees were to certify their participation in new employee orientation which addressed security awareness. Additionally, current employees were to certify annually that they had completed the security awareness training.

No deviation noted.

Criteria: L - Providing for the handling of exceptions and situations not specifically addressed in its system security policies.

Department's Control: The General Security For Statewide IT Resources Policy and the General Security For Network Resources Policy indicates it is the responsibility of the users to inform the Department, in writing of any exceptions or special use requirements.

Test Performed: Reviewed policies and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy and the General Security For Network Resources Policy stated users were to inform the Department, in writing, of any exceptions to the policies. Exceptions were granted upon approval of the Chief Information Security Officer.

No deviation noted.

Criteria: M - Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.

Department's Control: The IT Governance Policy documents the Department and the agencies responsibilities for identifying applicable laws, regulations, and other requirements as part of the new IT projects requirements.

Test Performed: Reviewed statute, Policy and interviewed staff.

Test Results: The Department carries out statutory responsibilities relating to data processing and telecommunication services (20 ILCS 405/405-10; 20 ILCS 405/405-20; 20 ILCS 405/405-250; 20 ILCS 405/405-255; 20 ILCS 405/405-260; 20 ILCS 405/405-270 and 20 ILCS 405/405-410). The Department was mandated to manage or delegate the management of the procurement, retention, installation, maintenance, and operation of all electronic data processing equipment used by State agencies to achieve maximum economy consistent with development of adequate and timely information in a form suitable for management analysis, in a manner that provides for adequate security protection and back-up facilities for that equipment.

According to the IT Governance Policy, the Department and agencies were responsible for identifying and ensuring compliance with applicable laws, regulations and applicable requirements as part of the IT Governance process.

The IT Governance Policy only addressed provisions of compliance with laws and regulations for new developments; it did not address provisions for existing systems. Additionally, the Policy did not document requirements for the identification of defined commitments, service-level agreements, and other contractual agreements.

Beyond statutory provisions, the Department did not have documented customer commitments or other agreements outlining requirements.

The Policy did not document the process for ensuring existing systems were in compliance with applicable laws and regulations. In addition, the Department did not document the identification of defined commitments, service-level agreements, and other contractual agreements.

Criteria: N - Providing for sharing information with third parties.

Department's Control: 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.

Test Performed: Reviewed policies and interviewed staff.

Test Results: The Data Classification and Protection Policy stated it was the responsibility of the data owner to determine the appropriateness of sharing of information based on the classification of the data.

Additionally, the General Security For Statewide IT Resources Policy stated the disclosure of confidential and sensitive information was to be restricted to authorized personnel.

No deviation noted.

Criteria: 1.3 - Responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, are assigned.

Department's Control: The Chief Information Security Officer has primary responsibility and accountability for the development and maintenance of the security policies.

Test Performed: Reviewed position description and interviewed staff.

Test Results: The Chief Information Security Officer was responsible for "policy development, planning, implementation and administration." Additionally, the Chief Information Security Officer was responsible for the development of "confidential comprehensive IT security plans and procedures."

No deviation noted.

**2.0 - Communications: The entity communicates its defined system security policies to responsible parties and authorized users.**

Criteria: 2.1 - The entity has prepared an objective description of system and its boundaries and communicated such description to authorized users.

Department's Control: The Department has published the Service Catalog on its website, which documents the services provided by the Department.

Test Performed: Reviewed Service Catalog and interviewed staff.

Test Results: The Department had published on its website a Service Catalog, which outlined the basic services to be provided to users. The Service Catalog outlined the following services:

- Application Services,
- Business Services,
- Computing Services,
- Network Services, and
- Telecommunication Services.

Each service outlined the standard service provided; however, the Catalog stated specific services may be provided upon request. Additionally, the Catalog documented the hours of availability for each service, help desk contact, and the availability of disaster recovery, security, and change management.

No deviation noted.

Criteria: 2.2 - The security obligations of users and the entity's security commitments to users are communicated to authorized users.

Department's Control: The Department's security commitments and obligations are outlined in the Service Catalog, which is posted on the Department's website. The security obligations of Department staff are communicated via the mandatory annual security awareness training, security policies, and periodic emails. New Department staff are required to sign a statement signifying that they have read, understand, and will comply with the security policies. Department staff reconfirm their compliance with the security policies through the annual security training. Contractors are required to take the annual security awareness training and certify they will comply with all security policies. The security obligations of users are communicated in several different fashions; policies published on the web, emails, and security notices on the website.

Test Performed: Reviewed Service Catalog, communications to users and staff, security awareness training, security policies, security policy acknowledgements, security training, Department website, and interviewed staff.

Test Results: The Department's Service Catalog, which was posted on their website, stated standard security measures would be provided with services. If the user agency required non-standard services, such a request could be made to the Department.

According to the General Security For Statewide IT Resources Policy: new Department "employees are required to participate in employee orientation which included certifying that they have completed any required security awareness training and agreed to comply with the General Security for Statewide IT Resources Policy."

During the review period, the Department had ten new employees. We requested and reviewed the policy acknowledgment forms for them, noting no exceptions.

Additionally, the General Security For Statewide IT Resources Policy stated “current employees shall, at each annual performance evaluation, certify that they have completed any required security awareness training and agree to comply with this General Security for Statewide IT Resources.”

In February 2012, the Department conducted security awareness training for all Department staff and contractors. Security awareness training addressed various security topics. Additionally, at the conclusion of the training, the staff and contractors were required to certify they would comply “with all CMS Security Policies and failure to comply could result in discipline.”

We requested and reviewed a listing of all Department staff and contractors to ensure each had completed the security awareness training, noting eight individuals had not.

During the review period the Department sent emails to Department staff and user agencies indicating security threats, security awareness, and the announcement of the new process for resetting of passwords. In addition, the Department had posted security policies and security bulletins on their website.

Eight individuals had not completed security awareness training.

Criteria: 2.3 - Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.

Department's Control: The Chief Information Security Officer has primary responsibility and accountability for the development and maintenance of the security policies. Position descriptions have been defined and communicated to employees.

Test Performed: Reviewed position descriptions and interviewed staff.

Test Results: The Chief Information Security Officer was responsible for “policy development, planning, implementation and administration.” Additionally, the Chief Information Security Officer was responsible for the development of “confidential comprehensive IT security plans and procedures.”

Position descriptions, which define the requirements of the job were available upon request and were posted for open positions. Additionally, staff members were automatically notified when their position description was updated.

No deviation noted.

Criteria: 2.4 - The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users.

Department's Control: The process for users to inform the Department of possible security issues and other incidents is posted on the Department's website. The General Security For IT

Resources Access Policy documents the process for users to inform their supervisor of security incidents.

Test Performed: Reviewed Department's website, Policy, procedures, and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated anyone suspecting a security breach, including lost or broken IT resource assets were to report the incident to their immediate supervisor.

In addition, the Department's website instructed users to contact the Customer Service Center (Help Desk) regarding security issues. However, procedures had not been developed to ensure Help Desk staff assigned suspected breaches or security incidents to appropriate managers.

According to the Critical Incident Response Procedures, if the Major Outage Response Team and/or the Department's Infrastructure Services Team had determined an incident had occurred, they were to determine the extent and if applicable, the Critical Incident Response Team was to be notified. In the event it was determined the incident was considered minor, the Department's Help Desk was to handle.

Procedures had not been developed to ensure suspected breaches or security incidents were assigned to managers.

Criteria: 2.5 - Changes that may affect system security are communicated to management and users who will be affected.

Department's Control: Changes are communicated to users and management via the CAC meetings; in which the meeting minutes are posted on the ECM SharePoint site. Agencies have access to the ECM SharePoint site.

Test Performed: Reviewed ECM SharePoint site, CAC meeting minutes, and interviewed staff.

Test Results: Infrastructure changes were communicated to users through CAC meetings and reports on the ECM SharePoint site.

The ECM SharePoint site maintained various reports to inform the users:

- Change Advisory Committee Meeting Minutes,
- 30 Day Outage Report by Agency,
- Change Detail Report (Next 14 Days),
- Enterprise Change Schedule (Next 90 Days), and
- Overdue Change Report.

We reviewed the reports and meeting minutes from the ECM SharePoint site for July 2011 – January 2012, noting information related to changes.

Emails were sent to all agencies identifying the changes to be discussed at the upcoming CAC meeting and the email included a link to the SharePoint site.

No deviation noted.

**3.0 - Procedures: The entity placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.**

Criteria: 3.1 - Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats.

Department's Control: A risk assessment is performed periodically. As security threats are identified, they are assessed.

Test Performed: Reviewed Framework, risk assessments, and interviewed staff.

Test Results: The Department had developed the IDCMS/BCCS Security and Compliance Solutions IT Risk Management Framework (Framework), dated December 15, 2009, to assist in conducting risk assessments.

The Framework stated the risk management strategy the Department had undertaken was based on the model of continuous identification, assessment, treatment, and monitoring. Each 'phase' of the model outlined the tasks to be completed and the outcome/deliverable to be obtained.

Although the IT Risk Management Framework had been in place since December 2009, the Department had only recently embarked on a project of mapping the Department's IT controls to the principles/controls documented in the National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA). The Department was in the process of identifying the various controls, risks, business owners, artifacts and if applicable, the compensating controls.

During the review period, the Department had not conducted any other risk assessments.

The Department had recently started conducting risk assessments over the IT environment.

Criteria: 3.2 - Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:

Criteria: A - Logical access security measures restrict access to information resources not deemed to be public.

Department's Control: Logical access to information is protected through system security software and application security. Access to resources is granted to authenticated users based on the user's identity. System options have been configured to protect system resources.

Test Performed: Reviewed security default settings, security profiles, operating system defaults and parameters, access to specific system libraries, programs and data, authentication servers, vendor website, and interviewed staff.



Test Results: System software integrated with Resource Access Control Facility (RACF) security software controlled logical access. Users must have a valid RACF ID and password before they could gain access to resources. Access rights were user specific and based on those rights, users were permitted or denied access to resources.

We reviewed a sample of access rights, noting access to system level data was restricted.

Additionally, we reviewed established security default settings, noting users were required to have an authenticated ID and password to access system resources. We also reviewed system options to ensure access to system libraries, programs and data were adequately secured, noting one ID had excessive powerful access privileges.

Authentication servers were utilized to provide authorized access to the firewalls, routers, and switches.

One ID had excessive powerful access privileges.

Criteria: B - Identification and authentication of users.

Department's Control: Users establish their identity and authentication to systems and applications through the use of user IDs and passwords. Unique user IDs are assigned to individual users. The sharing of individual IDs is prohibited. Password configurations have been established.

Test Performed: Reviewed security reports, security profiles, access to specific special purpose IDs, authentication servers, RACF, account parameters, and interviewed staff.

Test Results: Users were required to have a valid RACF ID and password before gaining access to mainframe resources.

We reviewed 107 users, noting each was assigned a unique ID. However, we noted eight active special purpose IDs (i.e. functional area – Command Center Consoles) were not uniquely assigned, and two IDs assigned to a retired staff member were still active.

In addition, we reviewed RACF reports and screens, noting users were identified and authenticated.

Passwords were complex and required specific syntax. Security configuration parameters forced passwords to be changed in defined intervals. Access was automatically revoked after a period of inactivity. Additionally, security configuration parameters forced IDs to be disabled after a defined number of unsuccessful login attempts.

The Network Services and LAN Services authentication servers utilized an administrative architecture in which groups were established with specific levels of administrative privileges for the individual's needs.

Upon review of the established parameters, we noted parameters had been established which required passwords to utilize specific syntax, forced passwords to be changed in defined intervals, maintained a history of previous passwords utilized, and disabled accounts after a defined number of unsuccessful login attempts.

Special purpose IDs were not always specifically assigned and two IDs assigned to a retired staff member were still active.

Criteria: C - Registration and authorization of new users.

Department's Control: Network Services required manager review and approval of new access rights. LAN Services utilized the LAN Services Access Authorization in order for staff to obtain access rights. Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form and submit via a Remedy Enterprise Service Request. The Mainframe Application Access Request Form indicates the access required and proper approval. The ability to create and modify user access rights is limited to authorized staff.

Test Performed: Reviewed standards, authorization request forms, personnel listings, Mainframe Security Procedures, Mainframe Application Access Form, new hire listing, and interviewed staff.

Test Results: The Department had not developed procedures related to the registration and authorization of users; however, divisions within the Department had developed specific procedures.

Network Services was notified by Personnel when a new individual began employment. Once notified, the Network Services Management would decide the appropriate access privileges to be granted to the individual. Documentation of the request and approvals was not required to be maintained.

To ensure proper access was assigned to the LAN Services technicians, LAN Services had developed and implemented the LAN Equipment Access Rights Standard (dated November 23, 2010).

The Standard required supervisors to complete the LAN Services Access Rights Authorization (Form) for new individuals to obtain access.

Upon review of personnel listings, detailing new hires and transfers, we noted no individuals had been hired or transferred into the Network Services or LAN Services Teams.

The Mainframe Security Procedures stated in order to obtain a RACF ID, the Department or proxy agency user was required to complete the Mainframe Application Access Request Form. However, the Procedures had not been updated to reflect the process of submitting the Form via a Remedy Enterprise Service Request to the Help Desk.

The Mainframe Application Access Form indicated the required access and was to be approved by the user's supervisor.

During the review period, the Department had two new hires which required the completion of the Mainframe Application Access Request Form. Our review of the Forms indicated no exceptions.

Procedures related to the registration and authorization of users had not been developed. In addition, documentation of access requests for Network Services was not maintained.

Criteria: D - The process to make changes and updates to user profiles.

Department's Control: Network Services is notified by Personnel of changes in an individual's employment status and makes changes to user's access rights accordingly. Changes to LAN Services staff access rights are made based on the approved LAN Services Access Rights Authorization. Changes, updates, and password resets to Department and proxy agency user profiles are completed by the Department's RACF Coordinator and/or the RACF Security Administrator. Changes are made based on the approved Mainframe Application Access Request Form submitted via a Remedy Enterprise Service Request. Bi-monthly the Department's RACF Coordinator receives a separation report documenting separations from all agencies. The Department's RACF Coordinator will review and revokes the user's ID. Bi-annually, the Department's RACF Coordinator will send all agencies a listing of their users, requesting the agency to review for accuracy, note any modifications, and return to the Department.

Test Performed: Reviewed standards, authorization request forms, personnel listings, Mainframe Security Procedures, Mainframe Access Request Forms, separation listing, violation reports, emails, DS Monitor Report, access associated with high-level access privileges, and interviewed staff.

Test Results: The Department had not developed policies related to the changing and updating of user profiles; however, divisions within the Department had developed specific procedures. Additionally, policies or procedures requiring the periodic review of access rights did not exist.

Network Services was notified by Personnel of changes in an individual's employment. Once notified, Network Services would make necessary adjustments to the individual's access privileges. Documentation of the request and approvals was not required to be maintained.

To ensure proper access was assigned to the LAN Service technicians, LAN Services had developed and implemented the LAN Equipment Access Rights Standard (dated November 23, 2010).

The Standard required supervisors to complete the LAN Services Access Rights Authorization (Form) for existing individuals whose access rights needed to be removed.

Upon review of personnel listings, detailing individual separations and transfers, we noted no individuals had left the Network Services Team and two individuals had left the LAN Services Team. We reviewed the Forms for the two individuals, noting no exceptions.

In the event an individual's RACF access required modification, the Mainframe Access Request Form was to be completed and submitted to the Help Desk via a Remedy Enterprise Service Request (ESR). Once the Help Desk received the ESR, it was reviewed and a change ticket was created, along with the ESR and the Mainframe Access Request Form being attached. The change ticket was then assigned to the applicable Team for completion.

Upon receipt of the change ticket, the RACF Security Administrator or RACF Coordinator would make the appropriate updates, inform the individual or the individual's supervisor, if applicable and close the change ticket.

We noted ten individuals who had RACF IDs and had separated from the Department. We requested the Mainframe Access Request Form documenting the revocation of the IDs for the ten individuals; two Forms could not be located. Our review of the remaining eight Forms indicated no exceptions.

The Mainframe Security Procedures stated twice a month, the RACF Coordinator was to receive a separation report documenting separations from all agencies. The RACF Coordinator was to revoke the separated user's accounts. According to the RACF Coordinator, he received the separation reports and revoked the applicable accounts; however, documentation was not maintained.

On June 16, 2011 the Department's Deputy Director issued a memo to all State agencies implementing a new process for the resetting of RACF passwords. Effectively immediately, the user was to send an email to the Help Desk stating:

- Full Name,
- Agency,
- RACF ID, and
- Telephone number.

Upon receipt, the Help Desk would verify the information and phone the individual with a temporary password. The temporary password was not to be left on voice mail, provided to another individual or emailed.

During an interview with the Department's RACF Coordinator on March 14, 2012, it was stated he was not aware of the new process for resetting RACF and had not received the memo. The Department's RACF Coordinator indicated he received telephone calls and direct emails requesting RACF password resets.

In the event an individual would telephone the Department's RACF Coordinator, he would reset the password at that time. If the individual would send an email, he would respond to the email with the temporary password.

Upon discussion with Department management, they notified the Department's RACF Coordinator on April 13, 2012 of the Department's process for resetting RACF passwords.

In order to ensure the Department's RACF Coordinator was complying with the new process, we reviewed the Violation Reports for the weeks of April 27 and May 4, 2012, noting the RACF password resets. During these two weeks, there were 19 resets which required an email from the user; our review indicated two resets did not have the corresponding email.

On a bi-annual basis the Department's RACF Coordinator was to send agencies a listing of their users for verification of appropriateness. The agencies were to review, note any modifications and return the listing to the Department's RACF Coordinator. On January 31, 2012, the Department's RACF Coordinator sent out the listings to the agencies requesting review.

The ability to change a user profile in RACF was limited to specific staff with special access rights. In addition, the capability to update user profiles (access rights to resources designated to a specific agency) was delegated to the RACF Coordinator and the RACF Security Administrator.

We reviewed the DS Monitor's Selected User Attribute Report noting access to high-level access privileges were restricted to security software administration staff. However, we noted one staff member with excessive high level access privileges. The RACF Security Administrator stated they performed updates to IDs for technical staff when requested.

We noted the RACF Coordinator performed updates to IDs for non-technical staff as well as specific (proxy) agencies. The RACF Security Administrator indicated the RACF Coordinator had access to the proxy agencies default security group and special access permissions for making updates to proxy agencies user profiles. We reviewed the DS Monitor's Selected User Attribute Report and access to specific default user groups and confirmed the RACF Coordinator had access for making updates to proxy agencies user profiles.

Procedures related to the changing and updating of user profiles had not been developed. In addition, the Department did not follow the documented process for resetting RACF passwords and documentation of changes in access rights for Network Services was not maintained. Additionally, one staff member had excessive high level access privileges.

Criteria: E - Distribution of output restricted to authorized users.

Department's Control: The distribution of output is restricted to authorized users via logical and physical security barriers. Distribution of digital output is restricted to authorized users through the management of system software tools or the online viewing software. Distribution of hardcopy output is restricted through physical and manual controls. Hardcopy output is printed at a secure facility with security guards. Upon request for pick up, the individual must identify themselves and be on the authorization listing.

Test Performed: Reviewed Report Distribution Logs, observed pickup process, toured facility, and interviewed staff.

Test Results: The Department of Revenue maintained the print shop utilized by agencies. The print shop was secured by proximity card readers, which required unique access codes. In addition, security guards staffed the facility 24/7.

The Department of Central Management Services, Department of Healthcare and Family Services and the Department of Human Services print jobs were maintained in the secure print shops until they were picked up. The print jobs were picked up at the loading dock each morning by each agency's messenger. All other print jobs were taken to the Report Distribution Room. The individual picking up the reports must provide identification and sign the Report Distribution Log. Department of Revenue staff would then check the individual against an authorization listing before allowing them to take the reports.

On March 2, 2012, we observed the pickup process, noting no exceptions.

Additionally, we reviewed 25 individuals from the Report Distribution Logs for the weeks of October 24, 2011, November 14, 2011, December 12, 2011, and January 17, 2012 to determine if the individuals who picked up reports were authorized, noting no exceptions.

In addition to obtaining hardcopy reports, agencies may view certain reports via an online reporting tool. The reporting tool was secured via security software, which allowed only authorized individuals to view reports. It was the responsibility of each agency to establish appropriate access rights for their staff.

No deviation noted.

Criteria: F - Restriction of access to offline storage, backup data, systems, and media.

Department's Control: Access to offline storage, backup data, system and media is limited to authorized staff via physical and logical access controls.

Test Performed: Reviewed security profiles, access to DASD and system backup resources, and interviewed staff.

Test Results: The card key system was utilized to control and restrict access to the Central Computer Facility (CCF) and Communications Building. Proximity card readers were installed on the building's exterior doors and strategically throughout the interior of each building.

Resource Access Control Facility (RACF) security software restricted access to offline storage, backup data, systems, and media. To access systems and resources, users were required to have a valid RACF user ID and password.

In order to create, modify or delete a RACF ID, a Mainframe Application Access Request Form was to be completed and submitted via an Enterprise Service Request (ESR). The ESR was then assigned to the RACF Security Administrator or RACF Coordinators for the granting of access.

During the review period, we noted one new employee had been hired to Enterprise Storage and Backup Team. We reviewed the Mainframe Access Request Form, noting no exceptions.

We reviewed a sample of access rights to these resources, noting no exceptions. Department management indicated periodic reviews of access rights were conducted; however, documentation was not maintained.

No deviation noted.

Criteria: G - Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).

Department's Control: Operating system configuration defaults are restricted to authorized personnel through logical access controls. Utility programs that can read, add, change or delete data or programs are restricted to authorized personnel. Master passwords are maintained in an encrypted database and also maintained in a secure safe. Authentication servers are utilized to control access, log access attempts, and alert management.

Test Performed: Reviewed system defaults, DS Monitor and CA-Examine reports, system consoles, supervisory calls, system exits, access over master passwords, access restrictions to powerful utilities, SMF recordings, access over SMF records, assessed access to APF-authorized libraries, authentication servers, access rights, device configurations, and interviewed staff.

Test Results: System software integrated with Resource Access Control Facility security software controlled logical access. Users must have a valid RACF ID and password before they could gain access to resources.

We reviewed the DS Monitor's Selected User Attribute Report noting access to high-level access privileges were restricted to security software administration staff. The RACF Security Administrator stated they performed updates to IDs for technical staff when requested.

Based on our review of the DS Monitor reports, we noted the Department encrypted the password database.

We confirmed a copy of the master password was maintained in a secured safe.

Authentication servers were utilized to provide authorized access to the firewalls, routers, and switches maintained by Network Services and LAN Services. We reviewed firewall and router configurations for the IP addresses of defined authentication servers and compared those IP addresses to those of the authentication servers in production.

Upon review of the firewall and router configuration files for Network Services, we noted all devices, except one, reviewed (5 firewalls and 109 routers) used all three of the Network Services authentication servers.

Additionally, we reviewed the users which had access to all firewalls, routers, and switches controlled by the three Network Services authentication servers, noting accounts with powerful access rights appeared to be appropriately assigned and controlled.

Upon review of the firewall and router configuration files for LAN Services, we noted all devices reviewed (47 firewalls and 17 routers) used both of the LAN Services authentication servers.

Additionally, we reviewed the user which had access to all firewalls, routers, and switches controlled by the two LAN Services authentication servers, noting accounts with powerful access rights appeared to be appropriately assigned and controlled, with two exceptions. We identified two accounts assigned to individuals no longer requiring access. Upon notification, management removed the two accounts noted.

Two accounts assigned to staff that no longer needed powerful access were identified.

Criteria: 3.3 - Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.

Department's Control: Physical access controls restrict access to authorized individuals via card key systems. Card keys are utilized to restrict access to the CCF and Communications Building. In order to obtain a card key, an ID Badge Request Form is to be completed, approval must be obtained from an authorized manager, and presentation of a valid ID. Visitors are required to sign in and out, in addition to being escorted. The CCF and the Communications Building are guarded by security guards. Video surveillance is utilized to monitor the CCF and the Communications Building. Procedures exist for the identification and escalation of physical security breaches. Physical access controls are in place to restrict access to the offsite storage location. Access to the offsite media is limited to authorized Department personnel.

Test Performed: Toured facilities, reviewed ID Badge Request Forms, Building Admittance Registers, card key system, access rights, key inventories, Site Specific Post Orders, Special Occurrence Reports, and interviewed staff.

Test Results: The card key system was utilized to control and restrict access to the CCF and Communications Building. Proximity card readers were installed on the building's exterior doors and strategically throughout the interior of each building.

In addition to other sensitive areas at the CCF, the card key system controlled and restricted access to the data center hosting the tape library, tape cleaning room, Operations Center, Public Key Infrastructure room, and telecommunications room.

In addition to other sensitive areas at the Communications Building, the card key system controlled and restricted access to the ICN network room, server and telecommunications rooms, Network Control Center (NCC), and Technical Safeguards lab.



In order to obtain a card key, an ID Badge Request Form was to be completed. The ID Badge Request Form was to be approved by an authorized manager and the employee was to present a valid ID.

During the review period, the Department had nine new employees, which requested a card key. We requested the completed ID Badge Request Form for the nine new employees, noting one Form could not be located and two Forms were not properly completed.

Upon leaving employment, Human Resources (HR) would email the Bureau of Property Management, who would then deactivate the card key badge. On the last day of employment, the employee's supervisor was to collect the card key badge and submit to HR. HR would then submit to the Bureau of Property Management for destruction.

Additionally, we reviewed 42 individuals with access to the CCF, noting six no longer required access. Upon notification, the Department removed the access rights for these six individuals. The card key system also had an absentee limit, whereby access rights were automatically revoked.

Individuals requesting a temporary badge were required to sign the Building Admittance Register prior to receiving the temporary badge from the security guard. We reviewed 83 individuals who had signed the Building Admittance Register for the CCF or the Communications Building and compared them to the access privileges defined in the card key system, noting no exceptions.

The Department had entered into a contract with a security firm to provide security guard services to select state facilities, including the CCF and Communications Building. The contract required at least one guard be on duty 24/7 at both locations and outlined their duties and responsibilities related to patrolling, and incident response/reporting.

In addition to the card keys, specific employees were also provided real property keys. The real property keys allowed access to specific doors within each facility. We reviewed the listing of real property keys for the CCF and Communications Building, noting:

- 63 of the 274 keys issued for the CCF could not be accounted for,
- 32 of the 207 keys issued for the Communications Building could not be accounted for,
- 13 of the 20 Grand Master keys for the CCF were indicated as lost or not found, and
- 3 of the 17 Grand Master keys for the Communications Building were indicated as lost or not found.

Additionally, video cameras were strategically placed throughout the interior and surrounding the exterior of the CCF and the Communications Building. Video feeds were monitored at the consoles located at the security guard desks. We viewed the digital video feeds, noting cameras were positioned to allow for clear unobstructed views and images were clear.

The guards at the CCF and the Communications Building maintained Site Specific Post Orders. The Orders provided general guidance and instructions related to the security guard's duties. In addition, the Orders provided guidance in responding to various types of "emergencies/threats."

Upon notification of an emergency/threat, the security guards were to contact the appropriate authorities and Department management. In addition, the security guards were to complete a Special Occurrence Report and submit it to the Facility Manager.

During the review period, there were three Special Occurrence Reports completed. The Reports indicated the security issues and the resolutions.

Offsite media was stored at a secure facility. Access to the facility was restricted to facility staff and authorized Department staff. We reviewed the listing of Department staff with access, noting no exceptions.

The Department did not ensure the ID Badge Request Form was properly completed and maintained. Additionally, the Department did not have adequate controls to ensure the timely deactivation of card key access rights or track and maintain real property keys.

Criteria: 3.4 - Procedures exist to protect against unauthorized access to system resources.

Department's Control: Access to system resources is restricted to authorized personnel through security software. Access to high-level access privileges is limited to security administration personnel. Firewalls and routers are used and configured to prevent unauthorized access.

Test Performed: Reviewed security defaults, security profiles, DS Monitor and CA-Examine reports, device configurations, hardware listing, vendor website, and interviewed staff.

Test Results: Access to system resources was restricted to authorized personnel. We reviewed the security default settings and confirmed access to system resources required an authenticated ID and password using complex password configuration requirements. We also reviewed the DS Monitor reports to review access rights to system-level libraries and high-level privileges. We noted two staff members with excessive access privileges.

The Department maintained the State of Illinois Statewide Network. Network Services (Network Operations and Enterprise Network Support) and LAN Services were tasked with maintaining the State's primary network consisting of firewalls, routers and switches.

We reviewed configurations, which contained software revision levels and fully documented high-level rule base descriptions, for a sample of devices (52 firewalls and 126 routers) maintained by Network Services and LAN Services, noting devices were configured to utilize authentication servers, logging servers and contained banners prohibiting unauthorized access and warning of prosecution. In addition, devices contained Access Control Lists (ACLs) to deny and permit specific types of network traffic.

Two staff members had excessive access privileges.

Criteria: 3.5 - Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.

Department's Control: The ability to install, modify, and replace operating systems is limited to authorized staff. Access to sensitive system functions is restricted to authorized staff. The Security and Compliance Solutions Team participates in user groups and subscribes to services related to computer viruses.

Test Performed: Reviewed access to system libraries and resources, security profiles, DS Monitor and CA-Examine Reports, emails, and interviewed staff.

Test Results: Users must have a valid RACF ID and password before they would gain access to resources.

We reviewed a sample of access rights to system configurations, powerful system privileges, and powerful utilities, noting one ID had excessive powerful access privileges. Additionally, we reviewed system defaults, access to system libraries including authorized libraries, security over established consoles and system monitoring, noting no exceptions.

The Department was a member of the Multi-State Information Sharing and Analysis Center, which provided members notifications related to security issues. We reviewed the notifications, noting they were received on an as needed basis and were prioritized based on criticality.

One ID had excessive powerful access privileges.

Criteria: 3.6 - Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.

Department's Control: The Department utilizes encryption technologies and access gateways for the transmission of sensitive or confidential information.

Test Performed: Reviewed standards, web portal, Department website, and interviewed staff.

Test Results: Network Services maintained 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, managed and maintained by Network Services, was utilized by the VPN solution.

To assist in managing and maintaining the Enterprise VPN solution, Network Services had developed the following standards:

- CMS Enterprise Virtual Private Network (VPN) Standard, and
- Enterprise VPN – Individual Remote Access Using SSL.

The CMS Enterprise VPN Standard defined the two types of VPNs currently available (individual remote access and site-to-site), as well as the type of encryption supported for the VPNs.

The Individual Remote Access Standard defined 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 were current on security and antivirus patches.

Upon review of the web portal utilized to login to the Enterprise VPN, we noted the existence of the security banner outlined in the Individual Remote Access Standard. Additionally, upon review of the web portal, we noted the security of authentication and communications to and from the web portal were the same as defined within the Individual Remote Access Standard.

Additionally, LAN Services maintained additional VPN technologies for eight agencies; however, we noted the technologies were aging. LAN Services had a project underway to migrate these VPNs to the Enterprise VPN Solution managed and maintained by Network Services. Department management indicated they would like to have the project completed within the next 12 months.

The State of Illinois Digital Signature Project provided a comprehensive system for public-key encryption and digital signature services (public-key infrastructure (PKI)). Public-key technology provided stronger levels of identification, privacy (encryption), verification, and security management capabilities.

No deviation noted.

### **Criteria related to execution and incident management used to achieve objectives**

Criteria: 3.7 - Procedures exist to identify, report, and act upon system security breaches and other incidents.

Department's Control: The Department has tools in place to identify, log, and report security breaches and other incidents. The Department's website provides users instructions for communicating security issues to the CMS Service Desk. The Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provided guidance to users for the reporting of lost or stolen assets.

Test Performed: Reviewed spreadsheets, device configurations, SolarWinds, vendor website, authentication servers, Department's website, policies, procedures, Critical Incident Response Team (CIRT) Reports, Remedy tickets, and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated anyone suspecting a security breach, including lost or broken IT resource assets were to report the incident to their immediate supervisor. However, the Policy did not document the actions to be taken by the supervisor.

Additionally, the Department's website instructed users to contact the Customer Service Center (Help Desk) regarding security issues. However, no policies or procedures had been developed

to ensure Help Desk staff assigned suspected breaches or security incidents to appropriate managers.

According to the Critical Incident Response Procedures, if the Major Outage Response Team and/or the Department's Infrastructure Services Team determined an incident had occurred, they were to determine the extent of the incident and if applicable, notify the Critical Incident Response Team. In the event it was determined the incident was considered minor, the Department's Help Desk was to be notified. However, our review of the Procedures indicated it did not document the process for identifying security breaches and other incidents, tracking or logging of the incident and the process which the Help Desk was to follow for minor incidents.

In addition, the Critical Incident Response Procedures stated for each event a CIRT Report was to be completed, which documented the specifics of the event, devices affected, and the resolution the Critical Incident Response Team took. We reviewed 18 CIRT Reports, noting no exceptions.

The Enterprise Desktop/Laptop Policy and Mobile Device Security Policy stated users were to inform the Department's Help Desk of all lost or stolen assets.

According to the Department, there were five laptops which were reported lost or stolen during the review period. Upon further review, we noted four of the laptops were not protected with encryption as required by the Laptop Data Encryption Policy.

In addition, we reviewed the CIRT Reports to determine if a Report had been completed for the lost/stolen laptops, noting they had not.

Network Services had configured three servers to function as the primary logging servers for the firewalls, routers, and switches it maintained. To confirm, during our review of the configuration files for selected devices (5 firewalls and 109 routers), we identified the IP addresses of the defined logging servers in the configuration files. We noted all devices reviewed, except one, utilized logging servers. However, we did note seven Network Operations devices which did not utilize all three logging servers. In addition, we noted devices were configured to utilize several additional logging servers in addition to the three primary logging servers that were utilized.

According to Department staff, log files on the logging servers utilized by Network Services were not typically reviewed in a proactive manner for potential incidents. Typically, log files located on these servers were utilized for error identification and resolution purposes.

LAN Services had configured two servers to function as the primary logging servers for the firewalls, routers, and switches it maintained. To confirm, during our review of the configuration files for selected devices (47 firewalls and 17 routers), we identified the IP addresses of the defined logging servers in the configuration files. We noted all devices reviewed utilized the two logging servers utilized by LAN Services. In addition, we noted two additional IP addresses which had been designated as logging servers. Upon follow-up with Department management, we noted the IPs were no longer active.

To monitor the log files for potential issues, LAN Services had assigned an individual the responsibility of proactively reviewing logs daily for select devices. These reviews, as well as any issues noted, were tracked in a spreadsheet. Any issues identified were referred to the LAN Services Data Center Team for further review.

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

According to Department staff, all Network Services devices were connected to NPM. For each of the Network Services devices (5 firewalls and 109 routers) we reviewed configurations for, we also reviewed NPM to ensure connectivity of each of the devices to SolarWinds; noting all devices, except one, were connected to NPM.

According to Department staff, all LAN Services devices were connected to NPM. For each of the LAN Services devices (47 firewalls and 17 routers) we reviewed configurations for, we also reviewed NPM to ensure connectivity of each of the devices to SolarWinds; noting all devices were connected to NPM.

In addition Network Services and LAN Services had implemented controls to allow them to monitor failed access attempts to networking devices.

According to Department management, in the event a breach was identified, Network Services and LAN Services would utilize the Data Breach Notification Policy and the Action Plan for Notification of a Security Breach posted on the Department's website. In addition, a Remedy ticket would be opened and if necessary the Technical Safeguards Team would be alerted.

The procedures did not document a process for identifying incidents, or the complete process for reporting and acting upon security breaches or incidents. In addition, discrepancies in the assignment of logging servers existed.

### **Criteria related to the system components used to achieve the objectives**

Criteria: 3.8 - Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.

Department's Control: 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 Business Reference Model is periodically updated by the applicable agency.

Test Performed: Reviewed Policy, Department's data classification, and interviewed staff.

Test Results: The Business Reference Model collected and stored information related to application and data processing services provided based on the Data Classification and Protection Policy. The Data Classification and Protection Policy was developed to inform "data

owners and data users the data classification and protection schema used by CMS/BCCS for protecting data.”

The Policy outlined three categories in which data was to be classified:

- Public,
- Official Use Only, and
- Confidential.

The Data Classification and Protection Policy stated it was the responsibility of the data owner to determine the appropriate classification over their data and to ensure the appropriate security and protection protocols were in place.

In March 2011, the Department undertook a project to begin classifying their data in accordance with the Data Classification and Protection Policy.

As of March 2012, the Department had determined they were the data owners for 176 applications. Our review indicated:

- 38 had been classified as confidential,
- 36 had been classified as Official Use Only,
- 11 had been classified as Public, and
- 91 had not been classified.

The Department had not completed the classification of its data.

Criteria: 3.9 - Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.

Department’s Control: Department staff are assigned the responsibility for monitoring and ensuring compliance with security policies.

Test Performed: Reviewed policies and interviewed staff.

Test Results: According to the Department’s security policies posted on their website, the Department and security personnel were responsible for the monitoring, auditing, tracking, and for the validation of compliance with the policies and procedures. Additionally, they were responsible for investigating violations of laws, policies, and procedures.

The policies did not define who the security personnel were and we were unable to determine who, within the Department was responsible. In addition, according to the Chief Information Security Officer; the designated personnel referenced in the policies had not been defined or formally assigned.

The Department had not clearly defined and communicated security personnel assignments.

Criteria: 3.10 - Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.

Department's Control: The IT Governance Policy governs the acquisition of systems and technology. Additionally, as part of the Governance process, agencies are to classify the data and systems in accordance with the Data Classification and Protection Policy. The Remedy Change Management Guide guides the development, implementation and maintenance of systems. Standards provide guidance on the configuration and deployment of network devices. Authentication servers are utilized to control access to networking devices. Network diagrams are maintained.

Test Performed: Reviewed IT Governance Policy, IT Governance Gates (templates), IT Guiding Principles, charters, Remedy Change Management Guide, standards, authentication servers, network diagrams, and interviewed staff.

Test Results: To help achieve the acquisition and management of systems and technology, the Department developed the IT Governance Policy, IT Guiding Principles, and the IT Governance Gates, which were published on the Department's website.

IT Governance Policy stated "ITG applies to business-sponsored IT projects that satisfy at least one of the following criteria:

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

The Project Charter, Business Requirements, and Technical Requirements Templates solicit information related to the design, acquisition, implementation, configuration, system availability/recovery requirements, and security requirements.

All projects were to follow the IT Governance process. Any exceptions required a waiver from the State's Chief Information Officer (CIO). During the review period, there were no exceptions that required a waiver

As part of the IT Governance process, the agencies were required to assess availability, accessibility, and data classification requirements.

We reviewed 25 charters to determine if the charters contained the required documentation and were appropriately approved, noting no exceptions.

The Remedy Change Management Guide was developed to provide corresponding procedures to the Change Management Policy. The Guide provided guidance on documenting changes and entering/tracking changes in the Remedy Action Request System. Additionally, the Guide



defined the authorization and approval processes, roles and responsibilities, emergency changes, and user involvement over changes.

All changes to the infrastructure were required to follow the Guide. Additionally, the Guide stated emergency changes were to be reviewed and documented.

To assist in the configuration and deployment of network infrastructure managed and maintained by Network Services and LAN Services, various standards and templates were maintained. However, we noted the standards and templates maintained by Network Services addressed routers at the core, distribution, and access levels and did not address the other routers and firewalls they maintained. Upon review, we noted baseline configurations outlined in the documents provided for authentication servers, logging servers, and banners prohibiting unauthorized access and warning of prosecution.

To provide authorized access to configurations deployed on devices throughout the network, authentication servers were utilized by Network Services and LAN Services.

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

No deviation noted.

Criteria: 3.11 - Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.

Department's Control: The Department's position descriptions specify the position's qualifications and responsibilities. The State's hiring procedures are followed for the hiring of staff. New employees are required to have background checks. Annual performance evaluations are completed. Staff is provided training based on their position's requirements. The Department conducts cross training for key positions.

Test Performed: Reviewed position descriptions, hiring procedures, background checks, performance evaluations, training records, and interviewed staff.

Test Results: The Department had established position descriptions for their positions. The position description outlined the position's responsibilities and requirements. The Personnel Code (20 ILCS 415) and the State of Illinois Personnel Rules dictated the hiring process for the Department.

New employees were required to have a background check completed prior to start of employment. We confirmed the background checks for the ten employees hired during the review period had been performed, noting no exceptions.

Employees were to receive a performance evaluation on an annual basis to provide timely feedback of their job performance. We reviewed 388 employees to determine if their annual

evaluation had been completed on a timely basis noting, 190 (49%) had not received an evaluation by the prescribed date.

Employees were to receive mandatory training upon hiring: ethics, Family Medical Leave Act (FMLA), Health Insurance Portability and Accountability Act (HIPAA), and sexual harassment. In addition, employees were to continue to receive job specific training.

During the review period, the Department hired ten new employees. We reviewed their training files, noting they had received the mandatory training upon employment. Additionally, we reviewed 92 employee training records, noting 25 employees had received additional training.

According to Department management, cross training would be completed as required for the specific job.

Performance evaluations were not always completed by the prescribed date.

### **Change management-related criteria applicable to the system's security**

Criteria: 3.12 - Procedures exist to maintain system components, including configurations consistent with the defined system security policies.

Department's Control: The Remedy Change Management Guide provides guidance in maintaining system components, including system configurations. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Standards provide guidance on the configuration and deployment of network devices. Tools are in place to assist in the deployment of and reporting on configurations.

Test Performed: Reviewed Change Management Guide, Requests for Change (RFC), CAC meeting minutes, standards, templates, SolarWinds, vendor website, and interviewed staff.

Test Results: The Remedy Change Management Guide provided guidance for maintaining system components, including system configurations. The Guide provided direction for the categorization, prioritization, and emergency changes.

We reviewed 50 RFCs to ensure they had been classified and prioritized, noting no exceptions. In addition, we reviewed nine emergency RFCs, noting they had been documented and approved.

Requestors were kept informed of their requests through the Change Advisory Committee documentation and the CAC meeting minutes. We reviewed the reports and meeting minutes from the ECM SharePoint site for July 2011 – January 2012, noting information related to changes.

To assist in the configuration and deployment of network infrastructure managed and maintained by Network Services and LAN Services, various standards and templates were maintained. However, we noted the standards and templates maintained by Network Services addressed

routers at the core, distribution, and access levels and did not address the other routers and firewalls they maintained. Upon review, we noted baseline configurations outlined in the documents provided for authentication servers, logging servers, and banners prohibiting unauthorized access and warning of prosecution.

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

According to Department staff, all Network Services devices were connected to NCM. For each of the Network Services devices (5 firewalls and 109 routers) we reviewed configurations for, we also reviewed NCM to ensure connectivity of each of the devices to SolarWinds; noting all devices, except one, were connected to NCM.

According to Department staff, all LAN Services devices were connected to NCM. For each of the LAN Services devices (47 firewalls and 17 routers) we reviewed configurations for, we also reviewed NCM to ensure connectivity of each of the devices to SolarWinds; noting all devices were connected to NCM.

No deviation noted.

Criteria: 3.13 - Procedures exist to provide that only authorized, tested and documented changes are made to the systems.

Department's Control: The Remedy Change Management Guide provides guidance for the authorization and documentation requirements for changes to systems. Changes are prioritized and categorized. Changes are communicated to users via the Change Advisory Committee meeting minutes and reports, which are located on the ECM SharePoint site. High impact changes require backout, test, and implementation plans to be attached to the RFC for the use in the event of a disruption.

Test Performed: Reviewed Remedy Change Management Guide, Requests for Change (RFC), CAC meeting minutes, EMC SharePoint site, and interviewed staff.

Test Results: The Remedy Change Management Guide provided guidance for the authorization, prioritization, categorization and documentation requirements. In addition, the Guide stated backout, testing and implementation plans were required to be attached to the RFC for high impact changes. However, the Guide did not document the requirements or required documentation of the various plans. The Guide stated testing was the responsibility of the Shared Services Team.

During our review, we inquired with the managers of the Shared Services Teams of their documentation related to testing of changes. The managers indicated testing was to be conducted; however, documentation was lacking. Additionally, it was indicated procedures had not been developed to outline testing requirements or documentation requirements.

We reviewed 50 RFCs to ensure they had been properly authorized, prioritized and categorized, noting no exceptions. In addition, we reviewed 18 high impact RFCs, noting the backout, test, and implementation plans had been attached. However, we were unable to determine the adequacy of the documentation due to the lack of documented requirements in the Guide.

Changes were communicated to users through CAC meeting minutes and reports on the ECM SharePoint site. We reviewed the reports and meeting minutes from the ECM SharePoint site for July 2011 – January 2012, noting information related to changes.

The Department had not included requirements over the backout, testing, and implementation plans in the Guide.

Criteria: 3.14 - Procedures exist to provide that emergency changes are documented and authorized timely.

Department's Control: Emergency changes are required to complete the standard documentation outlined in the Change Management Policy and the Remedy Change Management Guide. Emergency changes are reviewed by the technical and business approver post implementation. Emergency changes are communicated to users post implementation via the CAC meeting.

Test Performed: Reviewed emergency Requests for Change (RFC), CAC meeting minutes, Change Management Policy, Remedy Change Management Guide, and interviewed staff.

Test Results: According to the Change Management Policy, an emergency was defined as “a change that does not present notification to the formal process in advance of implementation. Emergency changes will only be acceptable in the event of a system failure or the discovery of security vulnerability.” The Policy also stated “all emergency changes will be reviewed and documented.”

The Change Management Guide defined emergency changes as unscheduled changes. Emergency changes were only acceptable in the event of a system failure or the discovery of security vulnerability. Emergency changes were to follow all change management processes except they may be implemented in advance of approval in order to correct the failure in a timely manner.

We reviewed nine emergency RFCs, noting the documentation and proper approvals were obtained. However, we did note the Policy and the Guide did not include the documentation requirements of the Post Implementation Review; therefore, we were unable to determine the adequacy of the documentation.

In addition, we reviewed the CAC meeting minutes to ensure the nine emergency RFCs had been included for discussion, noting no exceptions.

The Policy and the Guide did not document the requirements for Post Implementation Reviews.

**4.0 - Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system security policies.**

Criteria: 4.1 - The entity's system security is periodically reviewed and compared with the defined system security policies.

Department's Control: The Department utilizes various tools to review and assess the infrastructure and vulnerabilities.

Test Performed: Reviewed Mainframe Security Procedures, violation reports, monitoring reports, standards, templates, device configurations, network diagrams, reports, authentication servers, spreadsheets, vulnerability assessments, SolarWinds, and interviewed staff.

Test Results: The Department utilized various tools to review and assess the infrastructure, system capacity and performance. The Department reviewed performance within their respective functional areas utilizing various tools.

The Department's System Software Support staff maintained a system configuration for the four mainframe computers and the alternate data center. The configuration identified the logical partitions, the location, mode, operating system and version, memory allocation, primary function, environment, and the primary user agencies assigned to each logical system. To assist the Department in assuring system availability and security performance, the Department's security administration staff maintained security software, security authorization lists, and periodically reviewed security violation reports.

To assist with assuring system capacity and availability of system resources were reasonable, the Department's System Software Support staff monitored system capacity and system downtime using available software tools including Resource Measurement Facility (RMF) for monitoring system capacity and Tivoli Directory Server (TDS) for monitoring system availability. An excel spreadsheet containing the history of system capacity measures for each logical system within each computer was maintained. With regards to system availability, TDS reports were maintained and emailed to System Support staff and Department management each Monday indicating the availability of each system. A summary of downtime by system was also maintained and forwarded to management for review.

To assist in the configuration and deployment of network infrastructure managed and maintained by Network Services and LAN Services, various standards and templates were maintained. However, we noted the standards and templates maintained by Network Services addressed routers at the core, distribution, and access levels and did not address the other routers and firewalls they maintained. Upon review, we noted baseline configurations outlined in the documents provided for authentication servers, logging servers, and banners prohibiting unauthorized access and warning of prosecution.

Department management indicated periodic reviews of configurations were performed; however, documentation of these reviews was not maintained. Upon review of the configurations for compliance with the standards and templates, we noted all devices reviewed, which the standards

and templates applied to, utilized authentication servers, logging servers, and banners as outlined in documents.

Additionally, to keep the network aligned with Cisco's best practices and recommendations, Cisco periodically performed reviews and provided Network Services with a report. The last report, titled Best Practices Configuration Analysis Report, was prepared and provided to Network Services in December 2011.

Upon review of the Report and discussion with Department staff, the Report addressed only the segment of the network managed and maintained by Network Services Network Operations Team. The Report outlined two devices (of 150 reviewed) with High Risk Security exceptions. The Report also made recommendations regarding hardware and software upgrade needs; as well as, configuration enhancements to increase network security, efficiency, and redundancy.

According to Department management, due to other ongoing projects, resources have not been available to permit Network Services to review and take corrective actions; however, as resources permit the report would be reviewed and evaluated.

Authentication servers were utilized to provide authorized access to the firewalls, routers, and switches maintained by Network Services and LAN Services.

Department management indicated user access defined in the Network Services authentication servers was periodically reviewed; however, documentation of the reviews was not maintained.

The LAN Equipment Access Rights Standard indicated quarterly reviews of access rights were to be performed by LAN Services for networking devices they maintained. Department management indicated user access defined in the LAN Services authentication servers was periodically reviewed. Although documentation of the reviews was not maintained, if the review resulted in access rights which required modification/revocation, an Access Request Form was to be completed.

Network Services had configured three servers to function as the primary logging servers for the firewalls, routers, and switches it maintained. According to Department staff, we noted log files on the logging servers utilized by Network Services were not typically reviewed in a proactive manner for potential incidents. Typically, log files located on these servers were utilized for error identification and resolution purposes.

LAN Services had configured two servers to function as the primary logging servers for the firewalls, routers, and switches it maintained. To monitor the log files for potential issues, LAN Services had assigned an individual the responsibility of proactively reviewing logs daily for select devices. These reviews, as well as any issues noted, were tracked in a spreadsheet. Any issues identified were referred to LAN Services Data Center Team for further review.

In addition Network Services and LAN Services had implemented controls to allow them to monitor failed access attempts to networking devices.

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

LAN Services also placed reliance on vulnerability assessment work performed by the Technical Safeguard Team. As Technical Safeguards performed assessments for the various agencies supported by the Department, they would identify weaknesses such as open ports, open snmp strings, weak passwords, etc. Once notified by Technical Safeguards, LAN Services would take action as necessary.

Reports detailing the networks alignment with Cisco's best practices and recommendations were not reviewed to determine if corrective actions should be taken.

Criteria: 4.2 - There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.

Department's Control: Logs are analyzed either manually or by automated tools to identify trends that may have the potential to impact the Department's ability to achieve system security objectives. Security issues are addressed with management at various meetings.

Test Performed: Reviewed Mainframe Security Procedures, violation reports, monitoring reports, SolarWinds, and interviewed staff.

Test Results: The Department utilized various tools to review and assess the infrastructure, system capacity and performance. The Department reviewed performance within their respective functional areas utilizing various tools. Although, the Department had established and maintained various reports for monitoring purposes, they did not formally document their reviews.

A technical staff member outlined methods used to identify security issues during interviews. However, the methods and outcomes were not documented.

In addition, security issues were to be addressed at the monthly management meetings. We reviewed the meeting agendas, noting security issues were discussed.

The Department utilized the Resource Measurement Facility software for monitoring system capacity. Monitoring reports were reviewed for statistical performance and capacity statuses.

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

LAN Services also placed reliance on vulnerability assessment work performed by the Technical Safeguard Team. As Technical Safeguards performed assessments for the various agencies supported by the Department, they would identify weaknesses such as open ports, open snmp

strings, weak passwords, etc. Once notified by Technical Safeguards, LAN Services would take action as necessary.

The methods used to identify security issues and the outcomes of the reviews were not documented.

Criteria: 4.3 - Environmental, regulatory, and technological changes are monitored and their effect on system security is assessed on a timely basis and policies are updated for that assessment.

Department's Control: Department management considers technological developments, and laws and regulations during the planning process. Management conducts meetings with user agencies to determine their future needs.

Test Performed: Reviewed Strategic Priority Initiatives Summary, meeting agendas, and interviewed staff.

Test Results: The Strategic Priority Initiatives Summary documented projects which the Department had identified in order to allow them to stay current on technology changes, regulatory and environmental requirements. The Department had outlined 38 projects which were key to strategic objectives. Each project documented specifics, such as, business drivers (security, privacy), technology drivers (new hardware/software, DR/backup), the ranking/prioritization, desired outcomes, metrics (reductions, system availability/uptime) and timeframe for completion.

The Summary was developed based on input from all levels of management within the Department.

The Department had conducted meeting with agencies to determine their future technological needs.

No deviation noted.



## **TRUST SERVICES - AVAILABILITY PRINCIPLE, CRITERIA, RELATED CONTROLS AND TEST OF CONTROLS**

The system is available for operation and use as committed or agreed.

### **1.0 – Policies: The entity defines and documents its policies for the availability of its system.**

Criteria: 1.1 - The entity's system availability and related security policies are established and periodically reviewed and approved by a designated individual or group.

Department's Control: The security policies addressing logical and physical security are reviewed and approved by the Department's Director, Deputy Director, Deputy General Counsel and the Chief Information Security Officer. The Department has implemented security policies, which are posted on the Department's website.

Test Performed: Reviewed policies, Department's website, position description, and interviewed staff.

Test Results: According to the Chief Information Security Officer's position description, he was responsible for "policy development, planning, implementation and administration." Additionally, the Chief Information Security Officer was responsible for the development of "confidential comprehensive IT security plans and procedures."

The following policies, including but not limited to, were posted on the Department's website.

- Data Classification and Protection Policy, revised January 3, 2012
- General Security for Statewide IT Resources Policy, revised January 1, 2010
- General Security for Statewide Network Resources Policy, revised January 1, 2010
- IT Resource Access Policy, effective December 1, 2007
- Laptop Data Encryption Policy, revised January 1, 2010
- Statewide CMS/BCCS Facility Access Policy, revised January 1, 2010
- Change Management Policy, revised January 3, 2012
- Data Breach Notification Policy, revised January 1, 2010
- Action Plan for Notification of a Security Breach, effective August 31, 2007
- Electronically Stored Information Retention Policy, effective February 15, 2009
- IT Governance Policy, revised January 3, 2012
- Mobile Device Security Policy, effective October 1, 2009
- IT Recovery Policy, effective October 1, 2009

The General Security for Statewide IT Resources Policy along with the IT Recovery Policy and the associated IT Recovery Methodology addressed system availability.

The Department had implemented policies, which addressed logical and physical security. We reviewed the policies, noting they were reviewed and approved by the Department's Director, Deputy Director, Deputy General Counsel, and the Chief Information Security Officer.

During our review of the policies, we noted there was no formal policy requirement for periodic or routine reviews; however, four policies were updated during the review period.

A formal requirement to ensure periodic reviews of policies did not exist.

Criteria: 1.2 - The entity's system availability and related security policies include, but may not be limited to, the following matters:

Criteria: A - Identifying and documenting the system availability and related security requirements of authorized users.

Department's Control: The security policies identify and document the general security and availability requirements.

Test Performed: Reviewed policies and interviewed staff.

Test Results: The IT Governance Policy and associated documents required system and application availability requirements to be outlined. In addition, the IT Recovery Policy addressed system availability in the event of a disruption of normal operations.

The General Security For Statewide IT Resources Policy defined the general security measures specific to the IT resources managed by the Department. The Policy outlined security measures related to validating a user's identity prior to use of resources, general controls over confidential and sensitive information, and security awareness training requirements. The Policy also stated in the event of any actual or suspected security breaches the individual was to report the issue to their immediate supervisor.

The General Security For Statewide Network Resources Policy defined the general security measures specific to the network environment managed by the Department. The Policy outlined the general standards for firewall/intrusion detection devices, wireless LANs, content filtering, vulnerability assessments, remote access, WAN, internet services, and off-net services.

The IT Resource Access Policy documented the general requirements in order to obtain physical and/or logical access to Department resources and facilities. In order to obtain access, an individual's identity was required to be validated, background check completed, and a business justification provided. Individuals requiring access to resources were to be provided a badge, digital certificate, and a user ID. Upon separation, access was to be revoked and all badges were to be returned to the Department.

The Statewide CMS/BCCS Facility Access Policy defined the requirements for the granting and revocation of an individual's physical access privileges to the Department's facilities. The Policy stated in order to obtain unescorted access to a Department facility, an individual was required to have a background check completed. In addition, an individual's identity was to be validated.

Additionally, the Statewide CMS/BCCS Facility Access Policy stated upon determination physical access was no longer required; the individual was required to return the access badge. The Laptop Data Encryption Policy stated all newly issued and redeployed laptops were required to be equipped with full-disk encryption.

The Data Classification and Protection Policy stated data was to be classified into one of three categories; Public, Official Use Only, and Confidential. It was the responsibility of the data owner to determine the classification and to ensure appropriate security and protection protocols had been implemented.

The Mobile Device Security Policy defined the general security precautions; passwords, encryption, screen locking and timeout, to be taken with mobile devices. The Policy stated in the event a device was lost or stolen, the user was to report the incident to the Department's Help Desk.

No deviation noted.

Criteria: B - Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements.

Department's Control: The Data Classification and Protection Policy documents the data classification schema used to value and classify information generated, accessed, transmitted or stored. The IT Resource Access Policy documents the requirements for obtaining access to resources. The Electronically Stored Information Retention Policy documents the retention requirements for electronic information. The General Security For Statewide IT Resource Policy documents the destruction requirements.

Test Performed: Reviewed policies and interviewed staff.

Test Results: The Data Classification and Protection Policy was developed to inform "data owners and data users of the data classification and protection schema used by CMS/BCCS for protecting data." The Policy stated it was "applicable to all structured and unstructured data generated, accessed, transmitted, or stored on systems and networks managed by CMS/BCCS."

The Policy stated data was to be classified into one of three categories:

- Public,
- Official Use Only, and
- Confidential.

The Policy stated it was the responsibility of the data owner to determine the appropriate classification over their data and to ensure the appropriate security and protection protocols were in place. Additionally, the data owner was responsible for ensuring the proper sharing of information based on its classification.

According to the IT Resource Access Policy in order to obtain access to resources, a user was required to have a background check completed, their identity validated, and a business justification for access.

The Electronically Stored Information Retention Policy stated agencies were required to maintain records for the minimum period of time as outlined in the State Records Act (5 ILCS 160). In addition, agencies were required to obtain approval from the State Records Commission prior to the destruction of records.

According to the General Security For Statewide IT Resource Policy disclosure of confidential or sensitive information was to be restricted to authorized individuals. Additionally, the destruction of confidential and sensitive information was to be conducted in accordance with agency specific procedures.

No deviation noted.

Criteria: C - Assessing risks on a periodic basis.

Department's Control: The IT Risk Assessment Policy documents the requirements for assessing risk.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: The IT Risk Assessment Policy stated the Department, along with the Business Owners, would conduct periodic risk assessments for "identifying threats and vulnerabilities and assessing the impact." Additionally, risk assessments could include new systems, major modifications, application servers, networks, and processes by which the systems were administered.

The Policy also stated the Department would establish risk assessment criteria and classifications. In addition, the Department would appropriately address and remediate the risk identified in risk assessments.

No deviation noted.

Criteria: D - Preventing unauthorized access.

Department's Control: The IT Resource Access Policy documents controls for preventing unauthorized access.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: According to the IT Resource Access Policy, in order to ensure access was controlled, individuals requiring access to protected IT resources were to be "issued physical badges, and/or digital certificate, and/or an user ID."

No deviation noted.

Criteria: E - Adding new users, modifying the access levels of existing users, and removing users who no longer need access.

Department's Control: The IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the Statewide CMS/BCCS Facility Access Policy documents the requirements for granting, assigning and revoking user access.

Test Performed: Reviewed policies and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated an individual's identity was to be validated prior to obtaining access to resources. Additionally, once it was determined an individual no longer required access, the individual was to return the IT resources and notify the appropriate parties.

In accordance with the IT Resource Access Policy, prior to obtaining access to Department resources, an individual was to have a completed background check and their identity verified. In addition, upon determination access was no longer required, the individual's rights were to be removed.

The IT Resource Access Policy stated prior to obtaining administrative access to Department resources; supervisory approval must be obtained.

However, the policies did not address the requirements for requesting and obtaining access; including but not limited to documentation, tracking, and approvals, periodic review of access rights and the process for revoking access.

The policies did not address the requirements for requesting, obtaining, modifying, removing, approving, or the periodic review of access rights.

Criteria: F - Assigning responsibility and accountability for system availability and related security.

Department's Control: The IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the General Security For Statewide Network Resource Policy document the responsibilities and accountability of system security.

Test Performed: Reviewed policies and interviewed staff.

Test Results: Each of the policies, noted above, contained the following general statements regarding responsibilities:

- It was the responsibility of the users to understand the applicable policy and to follow the corresponding procedures.
- The Resource Custodians were responsible for understanding and adhering to the policies and for granting, reviewing, and removal of access to resources.

- The Department and security personnel were responsible for the monitoring, auditing, tracking, and for the validation of compliance with the policies and procedures. Additionally, they were responsible for investigating violations of laws, policies, and procedures.

The General Security For Statewide IT Resources Policy outlined general security measures over the usage of State resources in which users were responsible for; general provisions over resource use, credential rules, and inappropriate activities.

The General Security For Statewide Network Resources Policy stated it was a violation for users to circumvent the security measures put in place by the Department.

The IT Governance Policy stated the Chief Information Officer (CIO) of the State of Illinois, together with the Department of Central Management Services, Bureau of Communication and Computer Services (CMS/BCCS), established and oversaw the application of the State's Information Technology Governance.

The General Security for Statewide IT Resources Policy along with the IT Recovery Policy and the associated IT Recovery Methodology addressed system availability.

No deviation noted.

Criteria: G - Assigning responsibility and accountability for system changes and maintenance.

Department's Control: The Change Management Policy documents the responsibility and accountability of Department staff for system changes and maintenance.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: The Change Management Policy stated it was the responsibility of the Department and supported agency staff to familiarize themselves with the policy and the corresponding change management process.

The Policy stated all changes to the production IT environment would be subject to the change management process. The requests for changes would be reviewed and would ensure the appropriate communication to users had occurred.

No deviation noted.

Criteria: H - Testing, evaluating, and authorizing system components before implementation.

Department's Control: The Change Management Policy documents the process in which infrastructure changes are to follow.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: The Change Management Policy stated all changes to the production IT infrastructure were to follow the change management process. All changes required a completed Request For Change and review by the Change Advisory Committee.

The Policy did not address the requirements over testing and authorization of system components prior to implementation.

Requirements over testing and authorization of changes were not documented in policies.

Criteria: I - Addressing how complaints and requests relating to system availability and related security issues are resolved.

Department's Control: The General Security For Statewide IT Resources Policy states users are responsible for disclosing any actions or behaviors involving a State IT resource and report on actual or suspected breaches.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated all security issue complaints and requests were to be directed to the individual's immediate supervisor. However, we noted the Policy did not address the actions in which the supervisor was to take once a complaint or request was received.

The Policy did not address the entire process for reporting and resolving security or availability issues.

Criteria: J - Identifying and mitigating system availability and related security breaches and other incidents.

Department's Control: The General Security For Statewide IT Resources Policy and the Action Plan For Notification of a Security Breach documents the identification and notification of security breaches and other incidents.

Test Performed: Reviewed policies and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated if an event of misuse, theft, or abuse of information was identified, the individual was to report the event to their supervisor. However, we noted the Policy did not address the actions the supervisor was to take once a complaint or request was received. In addition, the Policy did not address the process for the identification of breaches or other incidents.

However, in the event a breach of personal information was determined, the Action Plan For Notification of a Security Breach documented the required actions to be taken. Upon determination of such a breach, the individuals were to be notified in accordance with the Personal Information Protection Act (815 ILCS 530).

The General Security For Statewide IT Resources Policy did not address the entire process for identifying, reporting, and mitigating security issues and availability issues.

Criteria: K - Providing for training and other resources to support its system availability and related security policies.

Department's Control: The General Security For Statewide IT Resources Policy documents the training requirements for Department staff.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated CMS/BCCS will provide security for CMS/BCCS managed IT resources to ensure the confidentiality, integrity and availability of State of Illinois operations. The Policy also stated new employees were to certify their participation in new employee orientation which addressed security awareness. Additionally, current employees were to certify annually that they had completed the security awareness training.

No deviation noted.

Criteria: L- Providing for the handling of exceptions and situations not specifically addressed in its system availability and related security policies.

Department's Control: The General Security For Statewide IT Resources Policy and the General Security For Network Resources Policy indicates it is the responsibility of the users to inform the Department, in writing of any exceptions or special use requirements.

Test Performed: Reviewed policies and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy and the General Security For Network Resources Policy stated users were to inform the Department, in writing, of any exceptions to the policies. Exceptions were granted upon approval of the Chief Information Security Officer.

No deviation noted.

Criteria: M - Providing for the identification of and consistency with, applicable laws and regulations defined commitments, service-level agreements, and other contractual requirements.

Department's Control: The IT Governance Policy documents the Department and the agencies responsibilities for identifying applicable laws, regulations, and other requirements as part of the new IT projects requirements.

Test Performed: Reviewed statute, Policy and interviewed staff.



Test Results: The Department carries out statutory responsibilities relating to data processing and telecommunication services (20 ILCS 405/405-10; 20 ILCS 405/405-20; 20 ILCS 405/405-250; 20 ILCS 405/405-255; 20 ILCS 405/405-260; 20 ILCS 405/405-270 and 20 ILCS 405/405-410). The Department was mandated to manage or delegate the management of the procurement, retention, installation, maintenance, and operation of all electronic data processing equipment used by State agencies to achieve maximum economy consistent with development of adequate and timely information in a form suitable for management analysis, in a manner that provides for adequate security protection and back-up facilities for that equipment.

According to the IT Governance Policy, the Department and agencies were responsible for identifying and ensuring compliance with applicable laws, regulations and applicable requirements as part of the IT Governance process.

The IT Governance Policy only addressed provisions of compliance with laws and regulations for new developments; it did not address provisions for existing systems. Additionally, the Policy did not document requirements for the identification of defined commitments, service-level agreements, and other contractual agreements.

Beyond statutory provisions, the Department did not have documented customer commitments or other agreements outlining requirements.

The Policy did not document the process for ensuring existing systems were in compliance with applicable laws and regulations. Additionally, the Policy did not document requirements for the identification of defined commitments, service-level agreements, and other contractual agreements.

Criteria: N - Recovering and continuing service in accordance with documented customer commitments or other agreements.

Department's Control: The CMS/BCCS Recovery Activation Plan and the Recovery Methodology document the Department's responsibilities related to recovery and continuous services.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: The IT Recovery Policy stated the Department would provide the IT infrastructure for recovery in the event of a disruption to normal operations. The agencies were responsible for conducting a business impact analysis, determining the criticality of their applications, recovery time objectives, communicating such to the Department, and participating in annual exercises.

Beyond statutory provisions, the Department did not have documented customer commitments or other agreements outlining requirements.

Criteria: O - Monitoring system capacity to achieve customer commitments or other agreements regarding availability.

Department's Control: The IT Governance Policy and associated documents outlined requirements for applications.

Test Performed: Reviewed policy, statutes, and interviewed staff.

Test Results: The IT Governance Policy and associated documents outlined requirements for system capacity. The Technical Requirements Template requested information on number of users and transaction, storage requirements, performance requirements, interfaces, availability requirements for applications. However, monitoring system capacity was not specifically addressed in the Policy.

Beyond statutory provisions, the Department did not have documented customer commitments or other agreements.

The Department had not implemented a policy regarding the monitoring of system capacity.

Criteria: 1.3 - Responsibility and accountability for developing and maintaining the entity's system availability and related security policies, and changes and updates to those policies, are assigned.

Department's Control: The Chief Information Security Officer has primary responsibility and accountability for the development and maintenance of the security policies.

Test Performed: Reviewed position description and interviewed staff.

Test Results: The Chief Information Security Officer was responsible for "policy development, planning, implementation and administration." Additionally, the Chief Information Security Officer was responsible for the development of "confidential comprehensive IT security plans and procedures."

In addition, the position description for the Data Center Manager included ensuring the availability of mainframe services as an essential function.

No deviation noted.

**2.0 – Communications: The entity communicates the defined system availability policies to responsible parties and authorized users.**

Criteria: 2.1 - The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

Department's Control: The Department has published the Service Catalog on its website, which documents the services provided by the Department.

Test Performed: Reviewed Service Catalog and interviewed staff.

Test Results: The Department had published on its website a Service Catalog, which outlined the basic services to be provided to users. The Service Catalog outlined the following services:

- Application Services,
- Business Services,
- Computing Services,
- Network Services, and
- Telecommunication Services.

Each service outlined the standard service provided; however, the Catalog stated specific services may be provided upon request. Additionally, the Catalog documented the hours of availability for each service, help desk contact, and the availability of disaster recovery, security, and change management.

No deviation noted.

Criteria: 2.2 - The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.

Department's Control: The Department's security commitments and obligations are outlined in the Service Catalog, which is posted on the Department's website. The security obligations of Department staff are communicated via the mandatory annual security awareness training, security policies, and periodic emails. New Department staff are required to sign a statement signifying that they have read, understand, and will comply with the security policies. Department staff reconfirm their compliance with the security policies through the annual security training. Contractors are required to take the annual security awareness training and certify they will comply with all security policies. The security obligations of users are communicated in several different fashions; policies published on the web, emails, and security notices on the website.

Test Performed: Reviewed Service Catalog, communications to users and staff, security awareness training, security policies, security policy acknowledgements, security training, Department website, and interviewed staff.

Test Results: The Department's Service Catalog, which was posted on their website, stated standard security measures would be provided with services, in addition to the availability of specific systems. If the user agency required non-standard services, such a request could be made to the Department.

According to the General Security For Statewide IT Resources Policy, new Department "employees are required to participate in employee orientation which included certifying that they have completed any required security awareness training and agreed to comply with the General Security for Statewide IT Resources Policy."

During the review period, the Department had ten new employees. We requested and reviewed the policy acknowledgment forms for them, noting no exceptions.

Additionally, the General Security For Statewide IT Resources Policy stated “current employees shall, at each annual performance evaluation, certify that they have completed any required security awareness training and agree to comply with this General Security for Statewide IT Resources.”

In February 2012, the Department conducted security awareness training for all Department staff and contractors. The security awareness training addressed various security topics. Additionally, at the conclusion of the training, the staff and contractors were required to certify they would comply “with all CMS Security Policies and failure to comply could result in discipline.”

We requested and reviewed a listing of all Department staff and contractors to ensure each had completed the security awareness training, noting eight individuals had not.

During the review period the Department sent emails to Department staff and user agencies indicating security threats, security awareness, and the announcement of the new process for resetting of passwords. In addition, the Department had posted security policies and security bulletins on their website.

Eight individuals had not completed security awareness training.

Criteria: 2.3 - Responsibility and accountability for the entity's system availability and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.

Department's Control: The Chief Information Security Officer has primary responsibility and accountability for security policy changes and updates. Position descriptions have been defined and communicated to employees.

Test Performed: Reviewed position descriptions and interviewed staff.

Test Results: The Chief Information Security Officer was responsible for “policy development, planning, implementation and administration.” Additionally, the Chief Information Security Officer was responsible for the development of “confidential comprehensive IT security plans and procedures.”

Position descriptions, which define the requirements of the job were available upon request and were posted for open positions. Additionally, staff members were automatically notified when their position description was updated.

The IT Governance Policy stated the Chief Information Officer (CIO) of the State of Illinois, together with the Department of Central Management Services, Bureau of Communication and Computer Services (CMS/BCCS), established and oversaw the application of the State's Information Technology Governance.

In addition, the position description for the Data Center Manager included ensuring the availability of mainframe services as an essential function.

No deviation noted.

Criteria: 2.4 - The process for informing the entity about system availability issues and breaches of system security and for submitting complaints is communicated to authorized users.

Department's Control: The process for users to inform the Department of possible security issues and other incidents is posted on the Department's website. The General Security For IT Resources Access Policy documents the process for users to inform their supervisor of security incidents. The common system user manuals provide instructions for users to contact the CMS Service Desk to report issues.

Test Performed: Reviewed Department's website, Policy, procedures, user manuals and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated anyone suspecting a security breach, including lost or broken IT resource assets were to report the incident to their immediate supervisor.

In addition, the Department's website instructed users to contact the Customer Service Center (Help Desk) regarding security issues. However, procedures had not been developed to ensure Help Desk staff assigned suspected breaches, system availability issues, or security incidents to appropriate managers.

According to the Critical Incident Response Procedures, if the Major Outage Response Team and/or the Department's Infrastructure Services Team had determined an incident had occurred, they were to determine the extent and if applicable, the Critical Incident Response Team was to be notified. In the event it was determined the incident was considered minor, the Department's Help Desk was to handle.

The user manuals instructed users to contact the CMS Service Desk (Help Desk) to report issues (i.e. system availability) regarding the common system (Accounting Information System, Central Inventory System, Central Payroll System, and Central Time and Attendance System).

Procedures had not been developed to ensure suspected breaches, system availability issues, or security incidents were assigned to managers.

Criteria: 2.5 - Changes that may affect system availability and system security are communicated to management and users who will be affected.

Department's Control: Changes are communicated to users and management via the CAC meetings; in which the meeting minutes are posted on the ECM SharePoint site. Agencies have access to the ECM SharePoint site. Changes to the common systems are communicated to users via email or phone. Planned changes to the common systems are conducted during the scheduled maintenance window.

Test Performed: Reviewed ECM SharePoint site, CAC meeting minutes, and interviewed staff.

Test Results: Infrastructure changes were communicated to users through CAC meetings and reports on the ECM SharePoint site.

The ECM SharePoint site maintained various reports to inform the users:

- Change Advisory Committee Meeting Minutes,
- 30 Day Outage Report by Agency,
- Change Detail Report (Next 14 Days),
- Enterprise Change Schedule (Next 90 Days), and
- Overdue Change Report.

We reviewed the reports and meeting minutes from the ECM SharePoint site for July 2011 – January 2012, noting information related to changes.

Emails were sent to all agencies identifying the changes to be discussed at the upcoming CAC meeting and the email included a link to the SharePoint site.

System managers were to communicate common system changes to the users via email or phone; however, they were not required to maintain documentation of the communications. Additionally, planned changes were scheduled to be completed during the scheduled maintenance window.

According to Department management, there were no major changes to common systems during the review period.

No deviation noted.

**3.0 – Procedures: The entity placed in operation procedures to achieve its documented system availability objectives in accordance with its defined policies.**

Criteria: 3.1 - Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats.

Department's Control: A risk assessment is performed periodically. As security threats are identified, they are assessed.

Test Performed: Reviewed Framework, risk assessments, and interviewed staff.

Test Results: The Department had developed the IDCMS/BCCS Security and Compliance Solutions IT Risk Management Framework (Framework), dated December 15, 2009, to assist in conducting risk assessments.

The Framework stated the risk management strategy the Department had undertaken was based on the model of continuous identification, assessment, treatment, and monitoring. Each 'phase' of the model outlined the tasks to be completed and the outcome/deliverable to be obtained.

Although the IT Risk Management Framework had been in place since December 2009, the Department had only recently embarked on a project of mapping the Department's IT controls to the principles/controls documented in the National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA). The Department was in the process of identifying the various controls, risks, business owners, artifacts and if applicable, the compensating controls.

During the review period, the Department had not conducted any other risk assessments.

The Department had recently started conducting risk assessments over the IT environment.

Criteria: 3.2 - Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.

Department's Control: Procedures exist for the identification, documentation, escalation, resolution, and review of problems. The Department maintains measures to protect against environmental factors at the CCF and the Communications Building. The CCF and the Communications Building are protected against fire using both smoke detectors and a fire suppression system. Water detectors are installed within the raised floor areas. The CCF and the Communications Building are protected against a disruption in power supply to the processing environment by both uninterruptible power supplies and emergency power supplies. This equipment is tested periodically. Preventive maintenance agreements and scheduled maintenance procedures are in place for key system hardware components. Physical and logical security controls are implemented to reduce the opportunity for unauthorized actions that could impair system availability. Vendor agreements are in place for maintenance and support services associated with networking equipment. The network is configured in a redundant manner.

Test Performed: Reviewed DP Guide, toured facilities, reviewed contracts, inspection reports, card key system, video cameras, security software, agreements, hardware listing, vendor website, device configurations, and interviewed staff.

Test Results: The Department maintained the Data Processing (DP) Guide which contained information for commands, problems, troubleshooting, changes, and a description on how to take the mainframe systems down and bring them back up. The DP Guide was available on the SharePoint site.

The CCF and the Communications Building maintained measures to protect against environmental factors.

The CCF third floor computer room contained fire suppression and detection systems that were Underwriter Laboratory approved and utilized an environmental friendly agency; FM-200. Upon review, we noted the system was last inspected in February 2012.

The Communications Building contained a fire detection and suppression system throughout the entire facility. Upon review, we noted the system was last inspected May 2005.

In addition to the fire suppression and detection system, the Department maintained fire extinguishers throughout the CCF and the Communications Building. During our review, we noted the fire extinguishers were inspected in January and March 2012, respectively.

The Department had maintained a preventive maintenance contract for the fire extinguishers at the CCF and the Communications Building.

Water detectors were installed within the raised floor area of the CCF. In the event sensors become damp, an alarm would sound at the Command Center.

The CCF was equipped with a uninterruptible power supply (UPS) and in the event of a power failure, the UPS would engage immediately and draw power from the battery farm until the generators would engage. The Department maintained a preventive maintenance contract for routine inspection and maintenance of the CCF UPS. Upon review of the inspection reports, we noted the UPS was last tested in January 2012.

Additionally, the Department maintained a preventive maintenance contract for the CCF generators. We reviewed the maintenance reports, noting the generators were inspected in November 2011.

The Communications Building was equipped with a UPS and in the event of a power failure, the UPS would engage immediately and draw power from the battery farm until the generators would engage. The Department maintained a preventive maintenance contract for routine inspection and maintenance of the UPS. Upon review of the inspection reports, we noted the UPS was last tested in October 2011.

The Department maintained a preventive maintenance contract for the Communications Building generators. Upon review of the inspection reports, we noted the generators were last inspected in December 2011.

In addition to the above preventive maintenance agreements, the Department maintained maintenance agreements for the chiller at the CCF and the HVAC systems at the CCF and Communications Building. Upon review of the inspection reports, we noted the chiller was last inspected in February 2012. Additionally, we noted the HVAC systems were inspected on a monthly basis.

A card key system, video cameras, and security guards were utilized to control and restrict access to the CCF and Communications Building.

Resource Access Control Facility (RACF) security software was the primary logical mainframe security control to prevent unauthorized actions.

The Department maintained an agreement with AT&T for Cisco's SMARTnet services. SMARTnet services provided maintenance and support services for Cisco brand hardware and software, as well as product replacement, maintained by Network Services, Field Operations and LAN Services.



However, SMARTnet did not cover equipment which had reached End-of-Life.

We performed review work to determine devices which will have reached End-of-Life (EoL) status by the end of FY12; as well as, CY13.

Upon review, we noted approximately 1,654 Agency Access Routers were managed and maintained by Network Services Enterprise Network Support and Customer and Account Management Field Operations, of which approximately 1,187 (71.8%) devices will have reached EoL status by the end of FY12. Only another two (.1%) devices will reach EoL status by December 31, 2013.

Network Services did not deem the risk associated with running Agency Access devices which were EoL to be significant; as spare equipment was maintained to support hardware failures. Additionally, per Department management, enterprise wide plans for replacing EoL equipment did not exist; however, such equipment would be replaced when rolling out new services as a result of agency specific requests and/or projects.

Additionally, we noted LAN Services maintained approximately 2,164 networking devices, of which approximately 722 (33.4%) devices will have reached EoL status by the end of FY12. Approximately another 85 (3.9%) devices will reach EoL status by December 31, 2013.

Department management indicated, LAN Services was working on a purchase for approximately \$2.2 million in new networking equipment. Although no formal approvals had been obtained at the time of our review, if approved, the purchase would replace approximately 300 of the devices which have already reached or will reach EoL by the end of FY12.

The vendor's Product End-of-Life Policy indicated notice of a product's end-of-sale date is generally given six months prior to the end-of-sale date. Subsequently, hardware will be supported by the vendor for a period of five years from the end-of-sale date, at which time the product will reach its End-of-Life date. Once a product has been through the End of Product Life Cycle the product is considered obsolete and is not sold, manufactured, improved, repaired, maintained, or supported.

Additionally, to ensure continuous availability of the network, the Department had configured the network in a redundant manner. Where operationally feasible, the State's primary network was configured so if one agency site went down, agency traffic would be rerouted to another agency location to ensure connectivity. Some redundancy was also configured within the agency networks themselves.

Approximately 72% of Agency Access Routers (maintained by Enterprise Network Support and Field Operations) and 33% of networking devices (maintained by LAN Services) had reached End-of-Life. In addition, the fire detection and suppression system at the Communications Building was last tested in 2005.

Criteria: 3.3 - Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies.

Department's Control: The Department has implemented a comprehensive strategy for backup and restoration. Backup procedures for the Department are documented and include daily backups and a complete backup of the entire week's changes on a weekly basis. The Department is notified of successful or failed backups. Daily and weekly backups are stored offsite. The DCMS/BCCS Infrastructure Services Recovery Activation Plan is documented. The DCMS/BCCS Infrastructure Services Recovery Activation Plan documents the roles and responsibilities of personnel. The agencies document their application recovery classification in the Business Reference Module. Testing is conducted annually. Critical personnel hold current versions of the various disaster recovery documents. Current versions of the various documents are stored offsite.

Test Performed: Reviewed backup schedules, procedures, backup logs, Shift Reports, Remedy tickets, DCMS/BCCS Infrastructure Services Recovery Activation Plan, application listing, contracts, exercise documentation, hotbox inventory, and interviewed staff

Test Results: The Department utilized CA-Scheduler to control and schedule backups. All systems were scheduled within CA-Scheduler to be backed up on a routine daily and weekly basis. Once scheduled, the backups ran automatically utilizing a utility within CA-Scheduler to perform the backup dumps.

To document backup jobs scheduled in CA-Scheduler and assist with the verification that backups were successful, the Department maintained and reviewed the CA-Scheduler Verify Backups document. Based on our review, we noted Department staff monitored the completion of the backup process.

The Department did not periodically verify the reliability of backups generated; however, they believed the current process of monitoring backups, the proven capability to restore files when needed, and the successful use of backups to perform disaster recovery testing were sufficient.

We compared the daily and weekly backup schedules detailed in CA-Scheduler Verify Backups document to the daily and weekly schedules defined within CA-Scheduler, noting no exceptions.

In the event a backup did not run successfully, Automation would send a notification to the Command Center, who would in turn notify Enterprise Storage and Backup staff of such issues. The Department would research and rectify the problem, then manually run cleanup jobs until all issues were resolved. Additionally, Department staff notified the user agency, explained the problem, and requested the agency rectify the problem.

We reviewed a sample of daily and weekly backups to ensure they were successful, noting no exceptions. Additionally, we reviewed a sample of daily and weekly backup success/failure logs, noting the Department did not maintain documentation of the corrective action taken.

In addition, Enterprise Storage and Backup staff monitored CA-Scheduler daily for any issues related to the backups.

We reviewed three months of the Shift Reports, noting nine instances effecting backups. The Shift Report indicated the Remedy ticket associated with the issue. We then reviewed the Remedy ticket to ensure corrective action had taken place, noting no exceptions.

The daily backups were maintained onsite, and the weekly backups were rotated to the Regional Vault.

Network Services and LAN Services had implemented procedures to routinely backup configurations for firewalls, routers, and switches they managed and maintained

Network Services' firewall, router, and switch configurations were backed-up via two independent processes.

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

The second method of backing-up Network Services device configurations utilized SolarWinds NCM. SolarWinds NCM was configured to routinely backup configurations for all firewalls, routers, and switches managed and maintained by Network Services. NCM pulled the device configurations and placed them on a database server.

Once configurations were backed-up, NCM emailed reports to administrators notifying them of the devices that were both successfully and unsuccessfully backed-up during the cycle. We reviewed reports, for a two day period, detailing Network Services devices which were successfully and unsuccessfully backed-up. Upon review of the reports, we noted 6,272 devices were checked for backup purposes over the two day period and errors occurred while attempting to backup 70 (1.1%) of the devices.

LAN Services' firewall, router, and switch configurations were backed-up via SolarWinds NCM. SolarWinds NCM was configured to routinely backup configurations for all firewall, routers, and switches managed and maintained by LAN Services. NCM pulled the device configurations and placed them on a database server for the Department's Enterprise Storage and Backup team to backup and rotate off-site according to their defined methods and procedures.

Once configurations were backed-up, NCM emailed reports to administrators notifying them of the devices that were both successfully and unsuccessfully backed-up during the cycle. We reviewed the reports, for a five day period, detailing LAN Services devices which were successfully and unsuccessfully backed-up. Upon review, we noted the devices managed and maintained by the LAN Services Data Center team did not encounter any errors during the five day period. However, the devices maintained by the LAN Services Field Operations team did encounter an elevated number of errors during the five day period. During that period 10,736 devices were checked for backup purposes and errors occurred while attempting to backup 2,327 (21.7%) devices. Although errors occurred for devices representing multiple agencies, the

majority of the backup errors were generated by devices representing two user agencies. Upon following up with Department staff, we learned NCM required the device to utilize command prompt to allow it to pull the configuration from the devices. Although the agency devices were at one time configured to allow command prompt, many of the devices have since been reset and therefore have returned to their default menu driven functionality instead of the reconfigured command prompt functionality. Additionally, many of the agency devices were older devices and did not function properly with NCM.

The Department developed the State of Illinois, CMS/BCCS, Recovery Activation Plan (Plan) to provide “instructions and actions required when recovering CMS/BCCS computing facilities and services.” The Plan was limited to the “events affecting CMS/BCCS computing facilities and services” and had a “defined scope of mainframe category 1, stage 0 applications.”

The Plan outlined the task/responsibilities of the various recovery teams. The Plan provided guidance from assessing the damage to obtaining the recovery services provider services.

The Plan stated the first 72 hours of an outage would be limited to the restoration of Stage 0, Category One (Human Safety) applications; along with applications and services added at the time of disaster.

In order to determine the Stage 0, Category One applications which were to be recovered, user agencies were to classify their applicable applications within the Business Reference Model. We reviewed the critical applications in the Business Reference Model, noting four agencies had deemed 13 applications as Stage 0, Category One.

The Department had a contract with an out of state disaster recovery service provider to provide recovery services in the event of a major regional disaster with prolonged outages.

According to the contract, the vendor would be required to provide mainframe recovery services, resources, personnel, and other services in order to continue the required processing capabilities.

The contract was set expire on June 30, 2012; however, the Department had an option to renew if the alternate data center was not equipped and ready. According to Department staff, the Department will not be renewing the contract for recovery purposes at June 30, 2012. The Department will be conducting recovery operations at the alternate data center.

In September 2011, the Department conducted testing of its computing facility, mainframe services, and the disaster recovery plans at the disaster recovery service provider data processing facility.

Our review of exercise documentation indicated four agencies, including the Department, participated in the exercise and tested the recovery of thirteen Stage 0, Category One applications.

Our review of the testing documentation indicated the overall test “went off well”. The documentation indicated problems were encountered; however, problems were addressed as

testing progressed. The documentation consisted of application and system requirements, recovery scripts, and post-exercise reviews. However, our review of the detailed documentation noted several of the documents were incomplete.

The Activation Plan stated “All critical data backups, media, and recovery documentation must be stored at an official CMS vault location.” The Activation Plan contained a listing of documents (hardcopy and electronic) which were to be maintained offsite.

During our review, we reviewed the contents of the Department’s “hotbox” maintained at the Regional Vault. The “hotbox” contained recovery documentation as outlined in Activation Plan. Additionally, per discussion with the Recovery Services Manager, a CD of the recovery documentation was provided to the Recovery Management Team Chair, Co-Chair, and the Recovery Services Manager. The individuals maintained the CD at their respective residence.

Errors occurred which prohibited the successful backup of configurations for LAN Services networking devices. Additionally, the Department did not maintain documentation of the corrective action taken on failed backups.

Criteria: 3.4 - Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies.

Department’s Control: Backups are performed in accordance with the Department’s defined backup strategy. An inventory of available backups and the physical location of the backups are maintained. Backup systems and data are stored offsite at the facilities of a third-party service provider. The Department performs an annual verification of media stored at the offsite storage facility.

Test Performed: Reviewed backup logs, procedures, inventory reports, and interviewed staff.

Test Results: The Department utilized CA-Scheduler to control and schedule backups. All systems were scheduled within CA-Scheduler to be backed up on a routine daily and weekly basis. Once scheduled, the backups ran automatically utilizing a utility within CA-Scheduler to perform the backup dumps.

To document backup jobs scheduled in CA-Scheduler and assist with the verification that backups were successful, the Department maintained and reviewed the CA-Scheduler Verify Backups document. Based on our review, we noted Department staff monitored the completion of the backup process.

Automated software was utilized to control and track media. Reports were utilized to inventory media in order to maintain current inventories.

The Department did not periodically verify the reliability of backups generated; however, they believed the current process of monitoring backups, the proven capability to restore files when needed, and the successful use of backups to perform disaster recovery testing were sufficient.

The Department utilized various reports for inventorying tape media. The Department conducted inventories in June and November 2011 and May 2012 of tapes located at the CCF and the offsite storage facility. According to the May 2012 inventory, there were 37 discrepancies noted. The Department has subsequently conducted additional investigation, resulting in one remaining discrepancy.

In addition, we reviewed 48 tapes, which were to be located at the CCF or the Regional Vault noting all tapes were located appropriately and had a unique tracking alpha numeric identification number.

One discrepancy was noted during the May 2012 tape media inventory.

### **Security-related criteria relevant to the system's availability**

Criteria: 3.5 - Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:

Criteria: A - Logical access security measures to restrict access to information resources not deemed to be public.

Department's Control: Logical access to information is protected through system security software and application security. Access to resources is granted to authenticated users based on the user's identity. System options have been configured to protect system resources.

Test Performed: Reviewed security default settings, security profiles, operating system defaults and parameters, access to specific system libraries, programs and data, authentication servers, vendor website, and interviewed staff.

Test Results: System software integrated with Resource Access Control Facility (RACF) security software controlled logical access. Users must have a valid RACF ID and password before they could gain access to resources. Access rights were user specific and based on those rights, users were permitted or denied access to resources.

We reviewed a sample of access rights, noting access to system level data was restricted.

Additionally, we reviewed established security default settings, noting users were required to have an authenticated ID and password to access system resources. We also reviewed system options to ensure access to system libraries, programs and data were adequately secured, noting one ID had excessive powerful access privileges.

Authentication servers were utilized to provide authorized access to the firewalls, routers, and switches.

One ID had excessive powerful access privileges.

Criteria: B - Identification and authentication of users.

Department's Control: Users establish their identity and authentication to systems and applications through the use of user IDs and passwords. Unique user IDs are assigned to individual users. The sharing of individual IDs is prohibited. Password configurations have been established.

Test Performed: Reviewed security reports, security profiles, access to specific special purpose IDs, authentication servers, RACF, account parameters, and interviewed staff.

Test Results: Users were required to have a valid RACF ID and password before gaining access to mainframe resources.

We reviewed 107 users, noting eight active special purpose IDs (i.e. functional area – Command Center Consoles) were not uniquely assigned, and two IDs assigned to a retired staff member were still active.

In addition, we reviewed RACF reports and screens, noting users were identified and authenticated.

Passwords were complex and required specific syntax. Security configuration parameters forced passwords to be changed in defined intervals. Access was automatically revoked after a period of inactivity. Additionally, security configuration parameters forced IDs to be disabled after a defined number of unsuccessful login attempts.

The Network Services and LAN Services authentication servers utilized an administrative architecture in which groups were established with specific levels of administrative privileges for the individual's needs.

Upon review of the established parameters, we noted parameters had been established which required passwords to utilize specific syntax, forced passwords to be changed in defined intervals, maintained a history of previous passwords utilized, and disabled accounts after a defined number of unsuccessful login attempts.

Special purpose IDs were not always specifically assigned and IDs assigned to a retired staff member were still active.

Criteria: C - Registration and authorization of new users.

Department's Control: Network Services required manager review and approval of new access rights. LAN Services utilized the LAN Services Access Authorization in order for staff to obtain access rights. Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form and submit via a Remedy Enterprise Service Request. The Mainframe Application Access Request Form indicates the access required and proper approval. The ability to create and modify user access rights is limited to authorized staff.

Test Performed: Reviewed standards, authorization request forms, personnel listings, Mainframe Security Procedures, Mainframe Application Access Form, new hire listing, and interviewed staff.

Test Results: The Department had not developed procedures related to the registration and authorization of users; however, divisions within the Department had developed specific procedures.

Network Services was notified by Personnel when a new individual began employment. Once notified, the Network Services Management would decide the appropriate access privileges to be granted to the individual. Documentation of the request and approvals was not required to be maintained.

To ensure proper access was assigned to the LAN Services technicians, LAN Services had developed and implemented the LAN Equipment Access Rights Standard (dated November 23, 2010).

The Standard required supervisors to complete the LAN Services Access Rights Authorization (Form) for new individuals to obtain access.

Upon review of personnel listings, detailing new hires and transfers, we noted no individuals had been hired or transferred into the Network Services or LAN Services Teams.

The Mainframe Security Procedures stated in order to obtain a RACF ID, the Department or proxy agency user was required to complete the Mainframe Application Access Request Form. However, the Procedures had not been updated to reflect the process of submitting the Form via a Remedy Enterprise Service Request to the Help Desk.

The Mainframe Application Access Form indicated the required access and was to be approved by the user's supervisor.

During the review period, the Department had two new hires which required the completion of the Mainframe Application Access Request Form. Our review of the Forms indicated no exceptions.

Procedures related to the registration and authorization of users had not been developed. In addition, documentation of access requests for Network Services was not maintained.

Criteria: D - The process to make changes and updates to user profiles.

Department's Control: Network Services is notified by Personnel of changes in an individual's employment status and makes changes to user's access rights accordingly. Changes to LAN Services staff access rights are made based on the approved LAN Services Access Rights Authorization. Changes, updates, and password resets to Department and proxy agency user profiles are completed by the Department's RACF Coordinator and/or the RACF Security Administrator. Changes are made based on the approved Mainframe Application Access Request



Form submitted via a Remedy Enterprise Service Request. Bi-monthly the Department's RACF Coordinator receives a separation report documenting separations from all agencies. The Department's RACF Coordinator will review and revoke the user's ID. Bi-annually, the Department's RACF Coordinator will send all agencies a listing of their users, requesting the agency to review for accuracy, note any modifications, and return to the Department.

Test Performed: Reviewed standards, authorization request forms, personnel listings, Mainframe Security Procedures, Mainframe Access Request Forms, separation listing, violation reports, emails, DS Monitor Report, access associated with high-level access privileges, and interviewed staff.

Test Results: The Department had not developed policies related to the changing and updating of user profiles; however, divisions within the Department had developed specific procedures. Additionally, policies or procedures requiring the periodic review of access rights did not exist.

Network Services was notified by Personnel of changes in an individual's employment. Once notified, Network Services would make necessary adjustments to the individual's access privileges. Documentation of the request and approvals was not required to be maintained.

To ensure proper access was assigned to the LAN Service technicians, LAN Services had developed and implemented the LAN Equipment Access Rights Standard (dated November 23, 2010).

The Standard required supervisors to complete the LAN Services Access Rights Authorization (Form) for existing individuals whose access rights needed to be removed.

Upon review of personnel listings, detailing individual separations and transfers, we noted no individuals had left the Network Services Team and two individuals had left the LAN Services Team. We reviewed the Forms for the two individuals, noting no exceptions.

In the event an individual's RACF access required modification, the Mainframe Application Access Request Form was to be completed and submitted to the Help Desk via a Remedy Enterprise Service Request (ESR). Once the Help Desk received the ESR, it was reviewed and a change ticket was created, along with the ESR and the Mainframe Access Request Form being attached. The Change Ticket was then assigned to the applicable Team for completion.

Upon receipt of the change ticket, the RACF Security Administrator or RACF Coordinator would make the appropriate updates, inform the individual or the individual's supervisor, if applicable and close the change ticket.

We noted ten individuals who had RACF IDs and had separated from the Department. We requested the Mainframe Access Request Form documenting the revocation of the IDs for the ten individuals; two Forms could not be located. Our review of the remaining eight Forms indicated no exceptions.

The Mainframe Security Procedures stated twice a month, the RACF Coordinator was to receive a separation report documenting separations from all agencies. The RACF Coordinator was to revoke the separated user's accounts. According to the RACF Coordinator, he received the separation reports and revoked the applicable accounts; however, documentation was not maintained.

On June 16, 2011 the Department's Deputy Director issued a memo to all State agencies implementing a new process for the resetting of RACF passwords. Effectively immediately, the user was to send an email to the Help Desk stating:

- Full Name,
- Agency,
- RACF ID, and
- Telephone number.

Upon receipt, the Help Desk would verify the information and phone the individual with a temporary password. The temporary password was not to be left on voice mail, provided to another individual or emailed.

During an interview with the Department's RACF Coordinator on March 14, 2012, it was stated he was not aware of the new process for resetting RACF and had not received the memo. The Department's RACF Coordinator indicated he received telephone calls and direct emails requesting RACF password resets.

In the event an individual would telephone the Department's RACF Coordinator, he would reset the password at that time. If the individual would send an email, he would respond to the email with the temporary password.

Upon discussion with Department management, they notified the Department's RACF Coordinator on April 13, 2012 of the Department's process for resetting RACF passwords.

In order to ensure the Department's RACF Coordinator was complying with the new process, we reviewed the Violation Reports for the weeks of April 27 and May 4, 2012, noting the RACF password resets. During these two weeks, there were 19 resets which required an email from the user; our review indicated two resets did not have the corresponding email.

On a bi-annual basis the Department's RACF Coordinator was to send agencies a listing of their users for verification of appropriateness. The agencies were to review, note any modifications and return the listing to the Department's RACF Coordinator. On January 31, 2012, the Department's RACF Coordinator sent out the listings to the agencies requesting review.

The ability to change a user profile in RACF was limited to specific staff with special access rights. In addition, the capability to update user profiles (access rights to resources designated to a specific agency) was delegated to the RACF Coordinator and the RACF Security Administrator.

We reviewed the DS Monitor's Selected User Attribute Report noting access to high-level access privileges were restricted to security software administration staff. However, we noted one staff member with excessive high level access privileges. The RACF Security Administrator stated they performed updates to IDs for technical staff when requested.

We noted the RACF Coordinator performed updates to IDs for non-technical staff as well as specific (proxy) agencies. The RACF Security Administrator indicated the RACF Coordinator had access to the proxy agencies default security group and special access permissions for making updates to proxy agencies user profiles. We reviewed the DS Monitor's Selected User Attribute Report and access to specific default user groups and confirmed the RACF Coordinator had access for making updates to proxy agencies user profiles.

Procedures related to the changing and updating of user profiles had not been developed. In addition, the Department did not follow the documented process for resetting RACF passwords and documentation of changes in access rights for Network Services was not maintained. Additionally, one staff member had excessive high level access privileges.

Criteria: E - Restriction of access to offline storage, backup data, systems and media.

Department's Control: Access to offline storage, backup data, system and media is limited to authorized staff via physical and logical access controls.

Test Performed: Reviewed security profiles, access to DASD and system backup resources, and interviewed staff.

Test Results: The card key system was utilized to control and restrict access to the Central Computer Facility (CCF) and Communications Building. Proximity card readers were installed on the building's exterior doors and strategically throughout the interior of each building.

Resource Access Control Facility (RACF) security software restricted access to offline storage, backup data, systems, and media. To access systems and resources, users were required to have a valid RACF user ID and password.

In order to create, modify or delete a RACF ID, a Mainframe Application Access Request Form was to be completed and submitted via an Enterprise Service Request (ESR). The ESR was then assigned to the RACF Security Administrator or RACF Coordinator for the granting of access.

During the review period, we noted one new employee had been hired to Enterprise Storage and Backup Team. We reviewed the Mainframe Access Request Form, noting no exceptions.

We reviewed a sample of access rights to these resources, noting no exceptions. Department management indicated periodic reviews of access rights were conducted; however, documentation was not maintained.

No deviation noted.

Criteria: F - Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).

Department's Control: Operating system configuration defaults are restricted to authorized personnel through logical access controls. Utility programs that can read, add, change or delete data or programs are restricted to authorized personnel. Master passwords are maintained in an encrypted database and also maintained in a secure safe. Authentication servers are utilized to control access, log access attempts, and alert management.

Test Performed: Reviewed system defaults, DS Monitor and CA-Examine reports, system consoles, supervisory calls, system exits, access over master passwords, access restrictions to powerful utilities, SMF recordings, access over SMF records, assessed access to APF-authorized libraries, authentication servers, access rights, device configurations, and interviewed staff.

Test Results: System software integrated with Resource Access Control Facility security software controls logical access. Users must have a valid RACF ID and password before they could gain access to resources.

We reviewed the DS Monitor's Selected User Attribute Report noting access to high-level access privileges were restricted to security software administration staff. The RACF Security Administrator stated they performed updates to IDs for technical staff when requested.

Based on our review of DS Monitor reports, we noted the Department encrypted the password database.

We confirmed a copy of the master password was maintained in a secured safe.

Authentication servers were utilized to provide authorized access to the firewalls, routers, and switches maintained by Network Services and LAN Services. We reviewed firewall and router configurations for the IP addresses of defined authentication servers and compared those IP addresses to those of the authentication servers in production.

Upon review of the firewall and router configuration files for Network Services, we noted all devices, except one, reviewed (5 firewalls and 109 routers) used all three of the Network Services authentication servers.

Additionally, we reviewed the users which had access to all firewalls, routers, and switches controlled by the three Network Services authentication servers, noting accounts with powerful access rights appeared to be appropriately assigned and controlled.

Upon review of the firewall and router configuration files for LAN Services, we noted all devices reviewed (47 firewalls and 17 routers) used both of the LAN Services authentication servers.

Additionally, we reviewed the user which had access to all firewalls, routers, and switches controlled by the two LAN Services authentication servers, noting accounts with powerful access

rights appeared to be appropriately assigned and controlled, with two exceptions. We identified two accounts assigned to individuals no longer requiring access. Upon notification, management removed the two accounts noted.

Two accounts assigned to staff that no longer needed powerful access were identified in our testing.

Criteria: 3.6 - Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.

Department's Control: Physical access controls restrict access to authorized individuals via card key systems. Card keys are utilized to restrict access to the CCF and Communications Building. In order to obtain a card key, an ID Badge Request Form is to be completed, approval must be obtained from an authorized manager, and presentation of a valid ID. Visitors are required to sign in and out, in addition to being escorted. The CCF and the Communications Building are guarded by security guards. Video surveillance is utilized to monitor the CCF and the Communications Building. Procedures exist for the identification and escalation of physical security breaches. Physical access controls are in place to restrict access to the offsite storage location. Access to the offsite media is limited to authorized Department personnel.

Test Performed: Toured facilities, reviewed ID Badge Request Forms, Building Admittance Registers, card key system, access rights, key inventories, Site Specific Post Orders, Special Occurrence Reports, and interviewed staff.

Test Results: The card key system was utilized to control and restrict access to the CCF and Communications Building. Proximity card readers were installed on the building's exterior doors and strategically throughout the interior of each building.

In addition to other sensitive areas at the CCF, the card key system controlled and restricted access to the data center hosting the tape library, tape cleaning room, Operations Center, Public Key Infrastructure room, and telecommunications room.

In addition to other sensitive areas at the Communications Building, the card key system controlled and restricted access to the ICN network room, server and telecommunications rooms, Network Control Center (NCC), and Technical Safeguards lab.

In order to obtain a card key, an ID Badge Request Form was to be completed. The ID Badge Request Form was to be approved by an authorized manager and the employee was to present a valid ID.

During the review period, the Department had nine new employees, which requested a card key. We requested the completed ID Badge Request Form for the nine new employees, noting one Form could not be located and two Forms were not properly completed.

Upon leaving employment, Human Resources (HR) would email the Bureau of Property Management, who would then deactivate the card key badge. On the last day of employment, the employee's supervisor was to collect the card key badge and submit to HR. HR would then submit to the Bureau of Property Management for destruction.

Additionally, we reviewed 42 individuals with access to the CCF, noting six no longer required access. Upon notification, the Department removed the access rights for these six individuals. The card key system also had an absentee limit, whereby access rights were automatically revoked.

Individuals requesting a temporary badge were required to sign the Building Admittance Register prior to receiving the temporary badge from the security guard. We reviewed 83 individuals who had signed the Building Admittance Register for the CCF or the Communications Building and compared them to the access privileges defined in the card key system, noting no exceptions.

The Department had entered into a contract with a security firm to provide security guard services to select state facilities; including the CCF and Communications Building. The contract required at least one guard be on duty 24/7 at both locations and outlined their duties and responsibilities related to patrolling, and incident response/reporting.

In addition to the card keys, specific employees were also provided real property keys. The real property keys allowed access to specific doors within each facility. We reviewed the listing of real property keys for the CCF and Communications Building, noting:

- 63 of the 274 keys issued for the CCF could not be accounted for,
- 32 of the 207 keys issued for the Communications Building could not be accounted for,
- 13 of the 20 Grand Master keys for the CCF were indicated as lost or not found, and
- 3 of the 17 Grand Master keys for the Communications Building were indicated as lost or not found.

Additionally, video cameras were strategically placed throughout the interior and surrounding the exterior of the CCF and the Communications Building. Video feeds were monitored at the consoles located at the security guard desks. We viewed the digital video feeds, noting cameras were positioned to allow for clear unobstructed views and images were clear.

The guards at the CCF and the Communications Building maintained Site Specific Post Orders. The Orders provided general guidance and instructions related to the security guard's duties. In addition, the Orders provided guidance in responding to various types of "emergencies/threats."

Upon notification of an emergency/threat, the security guards were to contact the appropriate authorities and Department management. In addition, the security guards were to complete a Special Occurrence Report and submit it to the Facility Manager.

During the review period, there were three Special Occurrence Reports completed. The Reports indicated the security issues and the resolutions.

Offsite media was stored at a secure facility. Access to the facility was restricted to facility staff and authorized Department staff. We reviewed the listing of Department staff with access, noting no exceptions.

The Department did not ensure the ID Badge Request Form was properly completed and maintained. Additionally, the Department did not have adequate controls to ensure the timely deactivation of card key access rights or track and maintain real property keys.

Criteria: 3.7 - Procedures exist to protect against unauthorized access to system resources.

Department's Control: Access to system resources is restricted to authorized personnel through security software. Access to high-level access privileges is limited to security administration personnel. Firewalls and routers are used and configured to prevent unauthorized access.

Test Performed: Reviewed security defaults, security profiles, DS Monitor and CA-Examine reports, device configurations, hardware listing, vendor website, and interviewed staff.

Test Performed: Reviewed security defaults, security profiles, DS Monitor and CA-Examine reports, device configurations, hardware listing, vendor website, and interviewed staff.

Test Results: Access to system resources was restricted to authorized personnel. We reviewed the security default settings and confirmed access to system resources required an authenticated ID and password using complex password configuration requirements. We also reviewed the DS Monitor reports to review access rights to system-level libraries and high-level privileges. We noted two staff members with excessive access privileges.

The Department maintained the State of Illinois Statewide Network. Network Services (Network Operations and Enterprise Network Support) and LAN Services were tasked with maintaining the State's primary network consisting of firewalls, routers and switches.

We reviewed configurations, which contained software revision levels and fully documented high-level rule base descriptions, for a sample of devices (52 firewalls and 126 routers) maintained by Network Services and LAN Services, noting devices were configured to utilize authentication servers, logging servers and contained banners prohibiting unauthorized access and warning of prosecution. In addition, devices contained Access Control Lists (ACLs) to deny and permit specific types of network traffic.

Two staff members had excessive access privileges.

Criteria: 3.8 - Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.

Department's Control: The ability to install, modify, and replace operating systems is limited to authorized staff. Access to sensitive system functions is restricted to authorized staff. The Security and Compliance Solutions Team participates in user groups and subscribes to services related to computer viruses.

Test Performed: Reviewed access to system libraries and resources, security profiles, DS Monitor and CA-Examine Reports, emails, and interviewed staff.

Test Results: Users must have a valid RACF ID and password before they would gain access to resources.

We reviewed a sample of access rights to system configurations, powerful system privileges, and powerful utilities, noting one ID had excessive powerful access privileges. Additionally, we reviewed system defaults, access to system libraries including authorized libraries, security over established consoles and system monitoring, noting no exceptions.

The Department was a member of the Multi-State Information Sharing and Analysis Center, which provided members notifications related to security issues. We reviewed the notifications, noting they were received on an as needed basis and were prioritized based on criticality.

One ID had excessive powerful access privileges.

Criteria: 3.9 - Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.

Department's Control: The Department utilizes encryption technologies and access gateways for the transmission of sensitive or confidential information.

Test Performed: Reviewed standards, web portal, and interviewed staff.

Test Results: Network Services maintained 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, managed and maintained by Network Services, was utilized by the VPN solution.

To assist in managing and maintaining the Enterprise VPN solution, Network Services had developed the following standards:

- CMS Enterprise Virtual Private Network (VPN) Standard, and
- Enterprise VPN – Individual Remote Access Using SSL.

The CMS Enterprise VPN Standard defined the two types of VPNs currently available (individual remote access and site-to-site), as well as the type of encryption supported for the VPNs.

The Individual Remote Access Standard defined 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 were current on security and antivirus patches.



Upon review of the web portal utilized to login to the Enterprise VPN, we noted the existence of the security banner outlined in the Individual Remote Access Standard. Additionally, upon review of the web portal, we noted the security of authentication and communications to and from the web portal were the same as defined within the Individual Remote Access Standard.

Additionally, LAN Services maintained additional VPN technologies for eight agencies; however, we noted the technologies were aging. LAN Services had a project underway to migrate these VPNs to the Enterprise VPN Solution managed and maintained by Network Services. Department management indicated they would like to have the project completed within the next 12 months.

The State of Illinois Digital Signature Project provided a comprehensive system for public-key encryption and digital signature services (public-key infrastructure (PKI)). Public-key technology provided stronger levels of identification, privacy (encryption), verification and security management capabilities.

No deviation noted.

### **Criteria related to execution and incident management used to achieve objectives**

Criteria: 3.10 - Procedures exist to identify, report, and act upon system availability issues and related security breaches and other incidents.

Department's Control: The Department has tools in place to identify, log, and report security breaches and other incidents. The Department's website provides users instructions for communicating security issues to the CMS Service Desk. The Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provided guidance to users for the reporting of lost or stolen assets. The common system user manuals provide instructions for users to contact the CMS Service Desk to report issues.

Test Performed: Reviewed spreadsheets, device configurations, SolarWinds, vendor website, authentication servers, Department's website, policies, procedures, user manuals, Critical Incident Response team (CIRT) Reports, Remedy tickets, and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated anyone suspecting a security breach, including lost or broken IT resource assets were to report the incident to their immediate supervisor. However, the Policy did not document the actions to be taken by the supervisor.

Additionally, the Department's website instructed users to contact the Customer Service Center (Help Desk) regarding "IT service issues, concerns, requests, as well as issues regarding cyber security." However, no policies or procedures had been developed to ensure Help Desk staff assigned suspected breaches or security incidents to appropriate managers.

According to the Critical Incident Response Procedures, if the Major Outage Response Team and/or the Department's Infrastructure Services Team determined an incident had occurred, they

were to determine the extent of the incident and if applicable, notify the Critical Incident Response Team. In the event it was determined the incident was considered minor, the Department's Help Desk was to be notified. However, our review of the Procedures indicated it did not document the process for identifying security breaches and other incidents, tracking or logging of the incident and the process which the Help Desk was to follow for minor incidents.

In addition, the Critical Incident Response Procedures stated for each event a CIRT Report was to be completed, which documented the specifics of the event, devices affected, and the resolution the Critical Incident Response Team took. We reviewed 18 CIRT Reports, noting no exceptions.

The Enterprise Desktop/Laptop Policy and Mobile Device Security Policy stated users were to inform the Department's Help Desk of all lost or stolen assets.

According to the Department, there were five laptops which were reported lost or stolen during the review period. Upon further review, we noted four of the laptops were not protected with encryption as required by the Laptop Data Encryption Policy.

In addition, we reviewed the CIRT Reports to determine if a Report had been completed for the lost/stolen laptops, noting they had not.

The common system user manuals instructed users to contact the CMS Service Desk (Help Desk) to report issues (i.e. system availability) regarding the common system (Accounting Information System, Central Inventory System, Central Payroll System, and Central Time and Attendance System).

The Department's Data Processing Guide provided detailed instructions to the Operations Center reporting and rectifying mainframe system availability issues. The DP Guide provided instructions for taking mainframe systems down, and back up, notification of applicable management and staff, and recording of issues within Remedy.

Network Services had configured three servers to function as the primary logging servers for the firewalls, routers, and switches it maintained. To confirm, during our review of the configuration files for selected devices (5 firewalls and 109 routers), we identified the IP addresses of the defined logging servers in the configuration files. We noted all devices reviewed, except one, utilized logging servers. However, we did note seven Network Operations devices which did not utilize all three logging servers. In addition, we noted devices were configured to utilize several additional logging server in addition to the three primary logging servers that were utilized.

According to Department staff, log files on the logging servers utilized by Network Services were not typically reviewed in a proactive manner for potential incidents. Typically, log files located on these servers were utilized for error identification and resolution purposes.

LAN Services had configured two servers to function as the primary logging servers for the firewalls, routers, and switches it maintained. To confirm, during our review of the

configuration files for selected devices (47 firewalls and 17 routers), we identified the IP addresses of the defined logging servers in the configuration files. We noted all devices reviewed utilized the two logging servers utilized by LAN Services. In addition, we noted two additional IP addresses which had been designated as logging servers. Upon follow-up with Department management, we noted the IPs were no longer active.

To monitor the log files for potential issues, LAN Services had assigned an individual the responsibility of proactively reviewing logs daily for select devices. These reviews, as well as any issues noted, were tracked in a spreadsheet. Any issues identified were referred to LAN Services Data Center team for further review.

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

According to Department staff, all Network Services devices were connected to NPM. For each of the Network Services devices (5 firewalls and 109 routers) we reviewed configurations for, we also reviewed NPM to ensure connectivity of each of the devices to SolarWinds; noting all devices, except one, were connected to NPM.

According to Department staff, all LAN Services devices were connected to NPM. For each of the LAN Services devices (47 firewalls and 17 routers) we reviewed configurations for, we also reviewed NPM to ensure connectivity of each of the devices to SolarWinds; noting all devices were connected to NPM.

In addition Network Services and LAN Services had implemented controls to allow them to monitor failed access attempts to networking devices.

According to Department management, in the event a breach was identified, Network Services and LAN Services would utilize the Data Breach Notification Policy and the Action Plan for Notification of a Security Breach posted on the Department's website. In addition, a Remedy ticket would be opened and if necessary the Technical Safeguards team would be alerted.

The procedures did not document a process for identifying incidents, or the complete process for reporting and acting upon security breaches, security incidents and system availability issues. In addition, discrepancies in the assignment of logging servers existed.

### **Criteria related to the system components used to achieve the objectives**

Criteria: 3.11 - Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.

Department's Control: 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 Business Reference Model is periodically updated by the applicable agency.

Test Performed: Reviewed Policy, Department's data classification, and interviewed staff.

Test Results: The Business Reference Model collected and stored information related to application and data processing services provided based on the Data Classification and Protection Policy. The Data Classification and Protection Policy was developed to inform "data owners and data users the data classification and protection schema used by CMS/BCCS for protecting data."

The Policy outlined three categories in which data was to be classified:

- Public,
- Official Use Only, and
- Confidential.

The Data Classification and Protection Policy stated it was the responsibility of the data owner to determine the appropriate classification over their data and to ensure the appropriate security and protection protocols were in place.

In March 2011, the Department undertook a project to begin classifying their data in accordance with the Data Classification and Protection Policy.

As of March 2012, the Department had determined they were the data owners for 176 applications. Our review indicated:

- 38 had been classified as confidential,
- 36 had been classified as Official Use Only,
- 11 had been classified as Public, and
- 91 had not been classified.

The Department had not completed the classification of its data.

Criteria: 3.12 - Procedures exist to provide that issues of noncompliance with system availability and related security policies are promptly addressed and that corrective measures are taken on a timely basis.

Department's Control: Department staff are assigned the responsibility for monitoring and ensuring compliance with security policies.

Test Performed: Reviewed policies and interviewed staff.

Test Results: According to the Department's security policies posted on their website, the Department and security personnel were responsible for the monitoring, auditing, tracking, and for the validation of compliance with the policies and procedures. Additionally, they were responsible for investigating violations of laws, policies, and procedures.

The policies did not define who the security personnel were and we were unable to determine who, within the Department was responsible. In addition, according to the Chief Information

Security Officer, the designated personnel referenced in the policies had not been defined or formally assigned.

The Department had not clearly defined and communicated security personnel assignments.

Criteria: 3.13 - Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system availability and related security policies.

Department's Control: The IT Governance Policy governs the acquisition of systems and technology. Additionally, as part of the Governance process, agencies are to classify the data and system in accordance with the Data Classification and Protection Policy. The Remedy Change Management Guide guides the development, implementation and maintenance of systems. Standards provide guidance on the configuration and deployment of network devices. Authentication servers are utilized to control access to networking devices. Network diagrams are maintained.

Test Performed: Reviewed IT Governance Policy, IT Governance Gates (templates), IT Guiding Principles, charters, Remedy Change Management Guide, standards, authentication servers, network diagrams, and interviewed staff.

Test Results: To help achieve the acquisition and management of systems and technology, the Department developed the IT Governance Policy, IT Guiding Principles, and the IT Governance Gates, which were published on the Department's website.

IT Governance Policy stated "ITG applies to business-sponsored IT projects that satisfy at least one of the following criteria:

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

The Project Charter, Business Requirements, and Technical Requirements Templates solicit information related to the design, acquisition, implementation, configuration, system availability/recovery requirements, and security requirements.

All projects were to follow the IT Governance process. Any exceptions required a waiver from the State's CIO. During the review period, there were no exceptions that required a waiver

As part of the IT Governance process, the agencies were required to assess availability, accessibility, and data classification requirements.

We reviewed 25 charters to determine if the charters contained the required documentation and were appropriately approved, noting no exceptions.

The Remedy Change Management Guide was developed to provide corresponding procedures to the Change Management Policy. The Guide provided guidance on documenting changes and entering/tracking changes in the Remedy Action Request System. Additionally, the Guide defined the authorization and approval processes, roles and responsibilities, emergency changes, and user involvement over changes.

All changes to the infrastructure were required to follow the Guide. Additionally, the Guide stated emergency changes were to be reviewed and documented.

To assist in the configuration and deployment of network infrastructure managed and maintained by Network Services and LAN Services, various standards and templates were maintained. However, we noted the standards and templates maintained by Network Services addressed routers at the core, distribution, and access levels and did not address the other routers and firewalls they maintained. Upon review, we noted baseline configurations outlined in the documents provided for authentication servers, logging servers, and banners prohibiting unauthorized access and warning of prosecution.

To provide authorized access to configurations deployed on devices throughout the network, authentication servers were utilized by Network Services and LAN Services.

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

No deviation noted.

Criteria: 3.14 - Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting availability and security have the qualifications and resources to fulfill their responsibilities.

Department's Control: The Department's position descriptions specify the position's qualifications and responsibilities. The State's hiring procedures are followed for the hiring of staff. New employees are required to have background checks. Annual performance evaluations are completed. Staff is provided training based on their position's requirements. The Department conducts cross training for key positions.

Test Performed: Reviewed position descriptions, hiring procedures, background checks, performance evaluations, training records, and interviewed staff.

Test Results: The Department had established position descriptions for their positions. The position description outlined the position's responsibilities and requirements. The Personnel Code (20 ILCS 415) and the State of Illinois Personnel Rules dictated the hiring process for the Department.

New employees were required to have a background check completed prior to start of employment. We confirmed the background checks for the ten employees hired during the review period had been performed, noting no exceptions.

Employees were to receive a performance evaluation on an annual basis to provide timely feedback of their job performance. We reviewed 388 employees to determine if their annual evaluation had been completed on a timely basis noting, 190 (49%) had not received an evaluation by the prescribed date.

Employees were to receive mandatory training upon hiring: ethics, Family Medical Leave Act (FMLA), Health Insurance Portability and Accountability Act (HIPAA), and sexual harassment. In addition, employees were to continue to receive job specific training.

During the review period, the Department hired ten new employees. We reviewed their training files, noting they had received the mandatory training upon employment. Additionally, we reviewed 92 employee training records, noting 25 employees had received additional training.

According to Department management, cross training would be completed as required for the specific job.

Performance evaluations were not always completed by the prescribed date.

### **Change management-related criteria applicable to the system's availability**

Criteria: 3.15 - Procedures exist to maintain system components, including configurations consistent with the defined system availability and related security policies.

Department's Control: The Remedy Change Management Guide provides guidance in maintaining system components, including system configurations. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Standards provide guidance on the configuration and deployment of network devices. Tools are in place to assist in the deployment of and reporting on configurations.

Test Performed: Reviewed Change Management Guide, Requests for Change (RFC), CAC meeting minutes, standards, templates, SolarWinds, vendor website, and interviewed staff.

Test Results: The Remedy Change Management Guide provided guidance for maintaining system components, including system configurations. The Guide provided direction for the categorization, prioritization, and emergency changes.

We reviewed 50 RFCs to ensure they had been classified and prioritized, noting no exceptions. In addition, we reviewed nine emergency RFCs, noting they had been documented and approved.

Requestors were kept informed of their requests through the Change Advisory Committee documentation and the CAC meeting minutes. We reviewed the reports and meeting minutes from the ECM SharePoint site for July 2011 – January 2012, noting information related to changes.

To assist in the configuration and deployment of network infrastructure managed and maintained by Network Services and LAN Services, various standards and templates were maintained. However, we noted the standards and templates maintained by Network Services addressed routers at the core, distribution, and access levels and did not address the other routers and firewalls they maintained. Upon review, we noted baseline configurations outlined in the documents provided for authentication servers, logging servers, and banners prohibiting unauthorized access and warning of prosecution.

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

According to Department staff, all Network Services devices were connected to NCM. For each of the Network Services devices (5 firewalls and 109 routers) we reviewed configurations for, we also reviewed NCM to ensure connectivity of each of the devices to SolarWinds; noting all devices, except one, were connected to NCM.

According to Department staff, all LAN Services devices were connected to NCM. For each of the LAN Services devices (47 firewalls and 17 routers) we reviewed configurations for, we also reviewed NCM to ensure connectivity of each of the devices to SolarWinds; noting all devices were connected to NCM.

No deviation noted.

Criteria: 3.16 - Procedures exist to provide that only authorized, tested, and documented changes are made to the system.

Department's Control: The Remedy Change Management Guide provides guidance for the authorization and documentation requirements for changes to systems. Changes are prioritized and categorized. Changes are communicated to users via the Change Advisory Committee meeting minutes and reports, which are located on the ECM SharePoint site. High impact changes require backout, test, and implementation plans to be attached to the RFC for the use in the event of a disruption.

Test Performed: Reviewed Remedy Change Management Guide, Requests for Change (RFC), CAC meeting minutes, EMC SharePoint site, and interviewed staff.

Test Results: The Remedy Change Management Guide provided guidance for the authorization, prioritization, categorization and documentation requirements. In addition, the Guide stated backout, testing and implementation plans were required to be attached to the RFC for high impact changes. However, the Guide did not document the requirements or required documentation of the various plans. The Guide stated testing was the responsibility of the Shared Services Team.

During our review, we inquired with the managers of the Shared Services Teams of their documentation related to testing of changes. The managers indicated testing was to be



conducted; however, documentation was lacking. Additionally, it was indicated procedures had not been developed to outline testing requirements or documentation requirements.

We reviewed 50 RFCs to ensure they had been properly authorized, prioritized and categorized, noting no exceptions. In addition, we reviewed 18 high impact RFCs, noting the backout, test, and implementation plans had been attached. However, we were unable to determine the adequacy of the documentation due to the lack of documented requirements in the Guide.

Changes were communicated to users through CAC meeting minutes and reports on the ECM SharePoint site. We reviewed the reports and meeting minutes from the ECM SharePoint site for July 2011 – January 2012, noting information related to changes.

The Department had not included requirements over the backout, testing, and implementation plans in the Guide.

Criteria: 3.17 - Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).

Department's Control: Emergency changes are required to complete the standard documentation outlined in the Change Management Policy and the Remedy Change Management Guide. Emergency changes are reviewed by the technical and business approver post implementation. Emergency changes are communicated to users post implementation via the CAC meeting.

Test Performed: Reviewed emergency Requests for Change (RFC) Policy, Guide, CAC meeting minutes and interviewed staff.

Test Results: According to the Change Management Policy, an emergency was defined as “a change that does not present notification to the formal process in advance of implementation. Emergency changes will only be acceptable in the event of a system failure or the discovery of security vulnerability.” The Policy also stated “all emergency changes will be reviewed and documented.”

The Change Management Guide defined emergency changes as unscheduled changes. Emergency changes were only acceptable in the event of a system failure or the discovery of security vulnerability. Emergency changes were to follow all change management processes except they may be implemented in advance of approval in order to correct the failure in a timely manner.

We reviewed nine emergency RFCs, noting the documentation and proper approvals were obtained. However, we did note the Policy and the Guide did not include the documentation requirements of the Post Implementation Review; therefore, we were unable to determine the adequacy of the documentation.

In addition, we reviewed the CAC meeting minutes to ensure the nine emergency RFCs had been included for discussion, noting no exceptions.

The Policy and the Guide did not document the requirements for Post Implementation Reviews.

**4.0 – Monitoring: The entity monitors the system and takes action to maintain compliance with its defined availability policies.**

Criteria: 4.1 - The entity's system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.

Department's Control: The Department utilizes various tools to review and assess the infrastructure and vulnerabilities.

Test Performed: Reviewed Mainframe Security Procedures, violation reports, monitoring reports, standards, templates, device configurations, network diagrams, reports, authentication servers, spreadsheets, vulnerability assessments, SolarWinds, and interviewed staff.

Test Results: The Department utilized various tools to review and assess the infrastructure, system capacity and performance. The Department reviewed performance within their respective functional areas utilizing various tools.

The Department's System Software Support staff maintained a system configuration for the four mainframe computers and the alternate data center. The configuration identified the logical partitions, the location, mode, operating system and version, memory allocation, primary function, environment, and the primary user agencies assigned to each logical system. To assist the Department in assuring system availability and security performance, the Department's security administration staff maintained security software, security authorization lists, and periodically reviewed security violation reports.

To assist with assuring system capacity and availability of system resources were reasonable, the Department's System Software Support staff monitored system capacity and system downtime using available software tools including Resource Measurement Facility (RMF) for monitoring system capacity and Tivoli Directory Server (TDS) for monitoring system availability. An excel spreadsheet containing the history of system capacity measures for each logical system within each computer was maintained. With regards to system availability, TDS reports were maintained and emailed to System Support staff and Department management each Monday indicating the availability of each system. A summary of downtime by system was also maintained and forwarded to management for review.

To assist in the configuration and deployment of network infrastructure managed and maintained by Network Services and LAN Services, various standards and templates were maintained. However, we noted the standards and templates maintained by Network Services addressed routers at the core, distribution, and access levels and did not address the other routers and firewalls they maintained. Upon review, we noted baseline configurations outlined in the documents provided for authentication servers, logging servers, and banners prohibiting unauthorized access and warning of prosecution.

Department management indicated periodic reviews of configurations were performed; however, documentation of these reviews was not maintained. Upon review of the configurations for compliance with the standards and templates, we noted all devices reviewed, which the standards and templates applied to, utilized authentication servers, logging servers, and banners as outlined in documents.

Additionally, to keep the network aligned with Cisco's best practices and recommendations, Cisco periodically performed reviews and provided Network Services with a report. The last report, titled Best Practices Configuration Analysis Report, was prepared and provided to Network Services in December 2011.

Upon review of the Report and discussion with Department staff, the Report addressed only the segment of the network managed and maintained by Network Services Network Operations Team. The Report outlined two devices (of 150 reviewed) with High Risk Security exceptions. The Report also made recommendations regarding hardware and software upgrade needs; as well as, configuration enhancements to increase network security, efficiency, and redundancy.

According to Department management, due to other ongoing projects, resources have not been available to permit Network Services to review and take corrective actions; however, as resources permit the report would be reviewed and evaluated.

Authentication servers were utilized to provide authorized access to the firewalls, routers, and switches maintained by Network Services and LAN Services.

Department management indicated user access defined in the Network Services authentication servers was periodically reviewed; however, documentation of the reviews was not maintained.

The LAN Equipment Access Rights Standard indicated quarterly reviews of access rights were to be performed by LAN Services for networking devices they maintained. Department management indicated user access defined in the LAN Services authentication servers was periodically reviewed. Although documentation of the reviews was not maintained, if the review resulted in access rights which required modification/revocation, an Access Request Form was to be completed.

Network Services had configured three servers to function as the primary logging servers for the firewalls, routers, and switches it maintained. According to Department staff, we noted log files on the logging servers utilized by Network Services were not typically reviewed in a proactive manner for potential incidents. Typically, log files located on these servers were utilized for error identification and resolution purposes.

LAN Services had configured two servers to function as the primary logging servers for the firewalls, routers, and switches it maintained. To monitor the log files for potential issues, LAN Services had assigned an individual the responsibility of proactively reviewing logs daily for select devices. These reviews, as well as any issues noted, were tracked in a spreadsheet. Any issues identified were referred to LAN Services Data Center team for further review.

In addition Network Services and LAN Services had implemented controls to allow them to monitor failed access attempts to networking devices.

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

LAN Services also placed reliance on vulnerability assessment work performed by the Technical Safeguard team. As Technical Safeguards performed assessments for the various agencies supported by the Department, they would identify weaknesses such as open ports, open snmp strings, weak passwords, etc. Once notified by Technical Safeguards, LAN Services would take action as necessary.

Reports detailing the networks alignment with Cisco's best practices and recommendations were not reviewed to determine if corrective actions should be taken.

Criteria: 4.2 - There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system availability and related security policies.

Department's Control: Logs are analyzed either manually or by automated tools to identify trends that may have the potential to impact the Department's ability to achieve system security objectives. Security issues are addressed with management at various meetings.

Test Performed: Reviewed Mainframe Security Procedures, violation reports, monitoring reports, SolarWinds, Shift Reports, and interviewed staff.

Test Results: The Department utilized various tools to review and assess the infrastructure, system capacity and performance. The Department reviewed performance within their respective functional areas utilizing various tools. Although, the Department had established and maintained various reports for monitoring purposes, they did not formally document their reviews.

A technical staff member outlined methods used to identify security issues during interviews. However, the methods and outcomes were not documented.

In addition, security issues were to be addressed at the monthly management meetings. We reviewed the meeting agendas, noting security issues were discussed.

The Department utilized the Resource Measurement Facility software for monitoring the mainframe system capacity. Monitoring reports were reviewed for statistical performance and capacity statuses.

In addition, system capacity and availability were routinely reviewed by system software support staff. On March 19, 2012, system availability was 100% on all systems, and capacity was an average 76% on the four computers.

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

LAN Services also placed reliance on vulnerability assessment work performed by the Technical Safeguard Team. As Technical Safeguards performed assessments for the various agencies supported by the Department, they would identify weaknesses such as open ports, open snmp strings, weak passwords, etc. Once notified by Technical Safeguards, LAN Services would take action as necessary.

The Department utilized various tools to monitor the IT infrastructure and related events. These monitoring tools were visually monitored by the Operations Center Staff 24 hours a day, 7 days a week.

The Daily Shift Reports recorded activities which occurred on each shift.

We reviewed Daily Shift Reports for the weeks of October 24<sup>th</sup> 2011, December 12<sup>th</sup> 2011, January 16<sup>th</sup> 2012 and February 20<sup>th</sup> 2012, noting they appeared to be completed appropriately. Additionally, we reviewed 25 problems indicated in the Shift Reports, noting a corresponding Remedy Help Desk ticket.

Shift Change Checklists were utilized to aid in reviewing the status of the various operating systems and applications. The Shift Change Checklists were also utilized to determine if there were problems with systems or applications. We reviewed Shift Change Checklists during October, 2011, noting supervisory review and that they appeared to be appropriately completed.

The methods used to identify security issues and the outcomes of the reviews were not documented.

Criteria: 4.3 - Environmental, regulatory, and technological changes are monitored, and their effect on system availability and security is assessed on a timely basis; policies are updated for that assessment.

Department's Control: Department management considers technological developments, and laws and regulations during the planning process. Management conducts meetings with user agencies to determine their future needs.

Test Performed: Reviewed Strategic Priority Initiatives Summary, meeting agendas, and interviewed staff.

Test Results: The Strategic Priority Initiatives Summary documented projects which the Department had identified in order to allow them to stay current on technology changes, regulatory and environmental requirements. The Department had outlined 38 projects which were key to strategic objectives. Each project documented specifics, such as, business drivers (security, privacy), technology drivers (new hardware/software, DR/backup), the

ranking/prioritization, desired outcomes, metrics (reductions, system availability/uptime) and timeframe for completion.

The Summary was developed based on input from all levels of management within the Department.

The Department had conducted meeting with agencies to determine their future technological needs.

No deviation noted.

## **TRUST SERVICES - PROCESSING INTEGRITY PRINCIPLE, CRITERIA, RELATED CONTROLS AND TEST OF CONTROLS**

System processing is complete, accurate, timely, and authorized.

### **1.0 – Policies: The entity defines and documents its policies for the processing integrity of its system.**

Criteria: 1.1 - The entity's processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group.

Department's Control: The security policies addressing logical and physical security are reviewed and approved by the Department's Director, Deputy Director, Deputy General Counsel and the Chief Information Security Officer. The Department has implemented security policies, which are posted on the Department's website.

Test Performed: Reviewed policies, Department's website, position description, user manuals, and interviewed staff.

Test Results: According to the Chief Information Security Officer's position description, he was responsible for "policy development, planning, implementation and administration." Additionally, the Chief Information Security Officer was responsible for the development of "confidential comprehensive IT security plans and procedures."

The following policies, including but not limited to, were posted on the Department's website.

- Data Classification and Protection Policy, revised January 3, 2012
- General Security for Statewide IT Resources Policy, revised January 1, 2010
- General Security for Statewide Network Resources Policy, revised January 1, 2010
- IT Resource Access Policy, effective December 1, 2007
- Laptop Data Encryption Policy, revised January 1, 2010
- Statewide CMS/BCCS Facility Access Policy, revised January 1, 2010
- Change Management Policy, revised January 3, 2012
- Data Breach Notification Policy, revised January 1, 2010
- Action Plan for Notification of a Security Breach, effective August 31, 2007
- Electronically Stored Information Retention Policy, effective February 15, 2009
- IT Governance Policy, revised January 3, 2012
- Mobile Device Security Policy, effective October 1, 2009

The Department had implemented policies, which addressed logical and physical security. We reviewed the policies, noting they were reviewed and approved by the Department's Director, Deputy Director, Deputy General Counsel, and the Chief Information Security Officer.

During our review of the policies, we noted there was no formal policy requirement for periodic or routine reviews; however, four policies were updated during the review period.

The common system user manuals provided information on processing integrity and security. The applicable common systems' manager was responsible for updates to each of the user manuals and communicating the applicable changes to the users.

A formal requirement to ensure periodic reviews of policies did not exist.

Criteria: 1.2 - The entity's system processing integrity and related security policies include, but may not be limited to, the following matters:

Criteria: A - Identifying and documenting the system processing integrity and related security requirements of authorized users.

Department's Control: The security policies identify and document the general security requirements. The common system user manuals outline the processing integrity and security requirements of authorized system users.

Test Performed: Reviewed policies, user manuals, and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy defined the general security measures specific to the IT resources managed by the Department. The Policy outlined security measures related to validating a user's identity prior to use of resources, general controls over confidential and sensitive information, and security awareness training requirements. The Policy also stated in the event of any actual or suspected security breaches the individual was to report the issue to their immediate supervisor.

The General Security For Statewide Network Resources Policy defined the general security measures specific to the network environment managed by the Department. The Policy outlined the general standards for firewall/intrusion detection devices, wireless LANs, content filtering, vulnerability assessments, remote access, WAN, internet services, and off-net services.

The IT Resource Access Policy documented the general requirements in order to obtain physical and/or logical access to Department resources and facilities. In order to obtain access, an individual's identity was required to be validated, background check completed, and a business justification provided. Individuals requiring access to resources were to be provided a badge, digital certificate, and a user ID. Upon separation, access was to be revoked and all badges were to be returned to the Department.

The Statewide CMS/BCCS Facility Access Policy defined the requirements for the granting and revocation of an individual's physical access privileges to the Department's facilities. The Policy stated in order to obtain unescorted access to a Department facility, an individual was required to have a background check completed. In addition, an individual's identity was to be validated.

Additionally, the Statewide CMS/BCCS Facility Access Policy stated upon determination physical access was no longer required; the individual was required to return the access badge.



The Laptop Data Encryption Policy stated all newly issued and redeployed laptops were required to be equipped with full-disk encryption.

The Data Classification and Protection Policy stated data was to be classified into one of three categories; Public, Official Use Only, and Confidential. It was the responsibility of the data owner to determine the classification and to ensure appropriate security and protection protocols had been implemented.

The Mobile Device Security Policy defined the general security precautions; passwords, encryption, screen locking and timeout, to be taken with mobile devices. The Policy stated in the event a device was lost or stolen, the user was to report the incident to the Department's Help Desk.

The common system user manuals outlined the security requirements of authorized users. Access was controlled through Resource Access Control Facility (RACF) security software. Users were required to have a properly authorized security software user ID and password to gain access to the operating environment. Once access to the operating environment was obtained, users were required to use a separate application user ID and password to gain access.

According to the common systems user manuals, each user agency had a Security Administrator who was responsible for the maintenance of their user access to the common systems.

Additionally, the common system user manuals documented the system processing integrity requirements (errors/edits) of authorized users. It was the responsibility of the users to ensure the accuracy of the data entered.

No deviation noted.

Criteria: B - Classifying data based on their criticality and sensitivity; that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements.

Department's Control: The Data Classification and Protection Policy documents the data classification schema used to value and classify information generated, accessed, transmitted or stored. The IT Resource Access Policy documents the requirements for obtaining access to resources. The Electronically Stored Information Retention Policy documents the retention requirements for electronic information. The General Security For Statewide IT Resource Policy documents the destruction requirements.

Test Performed: Reviewed policies and interviewed staff.

Test Results: The Data Classification and Protection Policy was developed to inform "data owners and data users of the data classification and protection schema used by CMS/BCCS for protecting data." The Policy stated it was "applicable to all structured and unstructured data generated, accessed, transmitted, or stored on systems and networks managed by CMS/BCCS."

The Policy stated data was to be classified into one of three categories:

- Public,
- Official Use Only, and
- Confidential.

The Policy stated it was the responsibility of the data owner to determine the appropriate classification over their data and to ensure the appropriate security and protection protocols were in place. Additionally, the data owner was responsible for ensuring the proper sharing of information based on its classification.

According to the IT Resource Access Policy in order to obtain access to resources, a user was required to have a background check completed, their identity validated, and a business justification for access.

The Electronically Stored Information Retention Policy stated agencies were required to maintain records for the minimum period of time as outlined in the State Records Act (5 ILCS 160). In addition, agencies were required to obtain approval from the State Records Commission prior to the destruction of records.

According to the General Security For Statewide IT Resource Policy disclosure of confidential or sensitive information was to be restricted to authorized individuals. Additionally, the destruction of confidential and sensitive information was to be conducted in accordance with agency specific procedures.

No deviation noted.

Criteria: C - Assessing risks on a periodic basis.

Department's Control: The IT Risk Assessment Policy documents the requirements for assessing risk.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: The IT Risk Assessment Policy stated the Department, along with the Business Owners, would conduct periodic risk assessments for "identifying threats and vulnerabilities and assessing the impact." Additionally, risk assessments could include new systems, major modifications, application servers, networks, and processes by which the systems were administered.

The Policy also stated the Department would establish risk assessment criteria and classifications. In addition, the Department would appropriately address and remediate the risk identified in risk assessments.

No deviation noted.

Criteria: D - Preventing unauthorized access.

Department's Control: The IT Resource Access Policy documents controls for preventing unauthorized access.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: According to the IT Resource Access Policy, in order to ensure access was controlled, individuals requiring access to protected IT resources were to be "issued physical badges, and/or digital certificate, and/or an user ID."

No deviation noted.

Criteria: E - Adding new users, modifying the access levels of existing users, and removing users who no longer need access.

Department's Control: The IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the Statewide CMS/BCCS Facility Access Policy documents the requirements for granting, assigning and revoking user access.

Test Performed: Reviewed policies and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated an individual's identity was to be validated prior to obtaining access to resources. Additionally, once it was determined an individual no longer required access, the individual was to return the IT resources and notify the appropriate parties.

In accordance with the IT Resource Access Policy, prior to obtaining access to Department resources, an individual was to have a completed background check and their identity verified. In addition, upon determination access was no longer required, the individual's rights were to be removed.

The IT Resource Access Policy stated prior to obtaining administrative access to Department resources; supervisory approval must be obtained.

However, the policies did not address the requirements for requesting and obtaining access; including but not limited to documentation, tracking, and approvals, periodic review of access rights and the process for revoking access.

The policies did not address the requirements for requesting, obtaining, modifying, removing, approving, or the periodic review of access rights.

Criteria: F - Assigning responsibility and accountability for system processing integrity and related security.

Department's Control: The IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the General Security For Statewide Network Resource Policy document the responsibilities and accountability of system security. The common system user manuals

outline the responsibility and accountability for the processing integrity and related security over the common systems.

Test Performed: Reviewed policies, user manuals and interviewed staff.

Test Results: Each of the policies, noted above, contained the following general statements regarding responsibilities:

- It was the responsibility of the users to understand the applicable policy and to follow the corresponding procedures.
- The Resource Custodians were responsible for understanding and adhering to the policies and for granting, reviewing, and removal of access to resources.
- The Department and security personnel were responsible for the monitoring, auditing, tracking, and for the validation of compliance with the policies and procedures. Additionally, they were responsible for investigating violations of laws, policies, and procedures.

The General Security For Statewide IT Resources Policy outlined general security measures over the usage of State resources in which users were responsible for; general provisions over resource use, credential rules, and inappropriate activities.

The General Security For Statewide Network Resources Policy stated it was a violation for users to circumvent the security measures put in place by the Department.

The common system user manuals outlined the user's responsibility and accountability over the processing integrity and security.

Data entered into the common systems was the responsibility of each user agency. Additionally, each user agencies Security Administrator was responsible for the security of their users.

No deviation noted.

Criteria: G - Assigning responsibility and accountability for system changes and maintenance.

Department's Control: The Change Management Policy documents the responsibility and accountability of Department staff for system changes and maintenance. The EAA Change Management Flowchart provides guidance to implement system changes related to the common systems. The Manager of the Enterprise Applications & Architecture Division is responsible and accountable for designing the control process for system changes and maintenance related to the common systems.

Test Performed: Reviewed Policy, position description and interviewed staff.

Test Results: The Change Management Policy stated it was the responsibility of the Department and supported agency staff to familiarize themselves with the policy and the corresponding change management process.

The Policy stated all changes to the production IT environment would be subject to the change management process. The requests for changes would be reviewed and would ensure the appropriate communication to users had occurred.

The Manager of the Enterprise Applications & Architecture Division had been assigned responsibility and accountability as a policy formulating administrator in planning, directing, implementing and administering the Enterprise Applications Division.

The Manager of the Enterprise Applications & Architecture Division decided to transition from the established change management process to a new process during the review period. The Manager was in the process of drafting policies and procedures related to the new process, responsibilities, and accountability.

The Department had not finalized policies outlining the responsibility and accountability for system changes related to the common systems.

Criteria: H - Testing, evaluating, and authorizing system components before implementation.

Department's Control: The Change Management Policy documents the process in which infrastructure changes are to follow. The EAA Change Management Flowchart provides guidance to implement system changes related to the common systems.

Test Performed: Reviewed Policy, Enterprise Applications and Architecture (EAA) Change Management Flowchart, and interviewed staff.

Test Results: The Change Management Policy stated all changes to the production IT infrastructure were to follow the change management process. All changes required a completed Request For Change and review by the Change Advisory Committee.

The Policy did not address the requirements over testing and authorization of system components prior to implementation.

The EAA Change Management Flowchart (Flowchart) was developed to provide guidance until the policies and procedures were finalized. The Flowchart indicated a request may originate via Remedy or the EPM. Once a manager determined the type of request, the request could follow the Remedy Help Desk path or the EPM change management path.

Our review of the Flowchart indicated:

- Management approvals were not required,
- Requests were not assigned a unique tracking number,
- Requests are not prioritized or categorized,
- Testing or documentation of testing requirements were not outlined, and
- Follow up after move to production was not required.

According to Department management, there were no major changes to the common systems during the review period.

Policies and procedures had not been implemented for testing, evaluating, and authorizing system components before implementation.

Criteria: I - Addressing how complaints and requests relating to system processing integrity and related security issues are resolved.

Department's Control: The General Security For Statewide IT Resources Policy states users are responsible for disclosing any actions or behaviors involving a State IT resource and report on actual or suspected breaches. The common system user manuals provide instructions for users to contact the CMS Service Desk to report issues.

Test Performed: Reviewed Policy, user manuals and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated all security issue complaints and requests were to be directed to the individual's immediate supervisor. However, we noted the Policy did not address the actions in which the supervisor was to take once a complaint or request was received.

The common system user manuals provided users instructions on contacting the CMS Service Desk (Help Desk) in the event processing integrity or security issues were identified. However, the Department had not developed policies for addressing the entire process of addressing issues.

The policies did not address the entire process for reporting and resolving security issues.

Criteria: J - Identifying and mitigating errors and omissions and other system processing integrity and related security breaches and other incidents.

Department's Control: The General Security For Statewide IT Resources Policy and the Action Plan For Notification of a Security Breach documents the identification and notification of security breaches and other incidents. The common system user manuals provide instructions for users to contact the CMS Service Desk to report issues.

Test Performed: Reviewed policies, user manuals and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated if an event of misuse, theft, or abuse of information was identified, the individual was to report the event to their supervisor. However, we noted the Policy did not address the actions the supervisor was to take once a complaint or request was received. In addition, the Policy did not address the process for the identification of breaches or other incidents.

However, in the event a breach of personal information was determined, the Action Plan For Notification of a Security Breach documented the required actions to be taken. Upon determination of such a breach, the individuals were to be notified in accordance with the Personal Information Protection Act (815 ILCS 530).

The common system user manuals provided users instructions on contacting the CMS Service Desk (Help Desk) to report any issues. However, the Department had not developed policies for addressing the entire process of addressing issues.

The policies did not address the entire process for reporting and resolving security issues.

Criteria: K - Providing for training and other resources to support its system processing integrity and related system security policies.

Department's Control: The General Security For Statewide IT Resources Policy documents the training requirements for Department staff.

Test Performed: Reviewed Policy and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated new employees were to certify their participation in new employee orientation which addressed security awareness. Additionally, current employees were to certify annually that they had completed the security awareness training.

No deviation noted.

Criteria: L - Providing for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies.

Department's Control: The General Security For Statewide IT Resources Policy and the General Security For Network Resources Policy indicates it is the responsibility of the users to inform the Department, in writing of any exceptions or special use requirements.

Test Performed: Reviewed policies and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy and the General Security For Network Resources Policy stated users were to inform the Department, in writing, of any exceptions to the Policies. Exceptions were granted upon approval of the Chief Information Security Officer.

No deviation noted.

Criteria: M - Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.

Department's Control: The IT Governance Policy documents the Department and the agencies responsibilities for identifying applicable laws, regulations, and other requirements as part of the new IT projects requirements.

Test Performed: Reviewed statute, Policy and interviewed staff.

Test Results: The Department carries out statutory responsibilities relating to data processing and telecommunication services (20 ILCS 405/405-10; 20 ILCS 405/405-20; 20 ILCS 405/405-250; 20 ILCS 405/405-255; 20 ILCS 405/405-260; 20 ILCS 405/405-270 and 20 ILCS 405/405-410). The Department was mandated to manage or delegate the management of the procurement, retention, installation, maintenance, and operation of all electronic data processing equipment used by State agencies to achieve maximum economy consistent with development of adequate and timely information in a form suitable for management analysis, in a manner that provides for adequate security protection and back-up facilities for that equipment.

According to the IT Governance Policy, the Department and agencies were responsible for identifying and ensuring compliance with applicable laws, regulations and applicable requirements as part of the IT Governance process.

The IT Governance Policy only addressed provisions of compliance with laws and regulations for new developments; it did not address provisions for existing systems. Additionally, the Policy did not document requirements for the identification of defined commitments, service-level agreements, and other contractual agreements.

Beyond statutory provisions, the Department did not have documented customer commitments or other agreements outlining requirements.

The Policy did not document the process for ensuring existing systems were in compliance with applicable laws and regulations. Additionally, the Policy did not document requirements for the identification of defined commitments, service-level agreements, and other contractual agreements.

Criteria: 1.3 - Responsibility and accountability for developing and maintaining entity's system processing integrity and related system security policies; changes, updates, and exceptions to those policies are assigned.

Department's Control: The Chief Information Security Officer has primary responsibility and accountability for the development and maintenance of the security policies.

Test Performed: Reviewed position description, user manuals, and interviewed staff.

Test Results: The Chief Information Security Officer was responsible for "policy development, planning, implementation and administration." Additionally, the Chief Information Security Officer was responsible for the development of "confidential comprehensive IT security plans and procedures."

The common system user manuals provided information on processing integrity and security. The applicable common systems' manager was responsible for updates to each of the user manuals and communicating the applicable changes to the users.

No deviation noted.



**2.0 – Communications: The entity communicates its documented system processing integrity policies to responsible parties and authorized users.**

Criteria: 2.1 - The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

Department's Control: The Department has published the Service Catalog on its website, which documents the services provided by the Department.

Test Performed: Reviewed Service Catalog and interviewed staff.

Test Results: The Department had published on its website a Service Catalog, which outlined the basic services to be provided to users. The Service Catalog outlined the following services:

- Application Services,
- Business Services,
- Computing Services,
- Network Services, and
- Telecommunication Services.

Each service outlined the standard service provided; however, the Catalog stated specific services may be provided upon request. Additionally, the Catalog documented the hours of availability for each service, help desk contact, and the availability of disaster recovery, security, and change management.

No deviation noted.

Criteria: 2.2 - The processing integrity and related security obligations of users and the entity's processing integrity and related security commitments to users are communicated to authorized users.

Department's Control: The Department's security commitments and obligations are outlined in the Service Catalog, which is posted on the Department's website. The security obligations of Department staff are communicated via the mandatory annual security awareness training, security policies, and periodic emails. New Department staff are required to sign a statement signifying that they have read, understand, and will comply with the security policies. Department staff reconfirm their compliance with the security policies through the annual security training. Contractors are required to take the annual security awareness training and certify they will comply with all security policies. The security obligations of users are communicated in several different fashions; policies published on the web, emails, and security notices on the website. The common system user manuals provide instructions for users to contact the CMS Service Desk to report processing and security issues.

Test Performed: Reviewed Service Catalog, communications to users and staff, security awareness training, security policies, user manuals, security policy acknowledgements, security training, Department website, and interviewed staff.

Test Results: The Department's Service Catalog, which was posted on their website, stated standard security measures would be provided with services. If the user agency required non-standard services, such a request could be made to the Department.

According to the General Security For Statewide IT Resources Policy, new Department "employees are required to participate in employee orientation which included certifying that they have completed any required security awareness training and agreed to comply with the General Security for Statewide IT Resources Policy."

During the review period, the Department had ten new employees. We requested and reviewed the policy acknowledgment forms for them, noting no exceptions.

Additionally, the General Security For Statewide IT Resources Policy stated "current employees shall, at each annual performance evaluation, certify that they have completed any required security awareness training and agree to comply with this General Security for Statewide IT Resources."

In February 2012, the Department conducted security awareness training for all Department staff and contractors. The security awareness training addressed various security topics. Additionally, at the conclusion of the training, the staff and contractors were required to certify they would comply "with all CMS Security Policies and failure to comply could result in discipline."

We requested and reviewed a listing of all Department staff and contractors to ensure each had completed the security awareness training, noting eight individuals had not.

During the review period the Department sent emails to Department staff and user agencies indicating security threats, security awareness, and the announcement of the new process for resetting of passwords. In addition, the Department had posted security policies and security bulletins on their website.

The common system user manuals provided users instructions on contacting the CMS Service Desk (Help Desk) in order to report processing and security issues.

Eight individuals had not completed security awareness training.

Criteria: 2.3 - Responsibility and accountability for the entity's system processing integrity and related security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.

Department's Control: The Chief Information Security Officer has primary responsibility and accountability for the development and maintenance of the security policies. Position descriptions have been defined and communicated to employees. The common system user manuals provide information on processing integrity and security. Common system managers are responsible for updates to the applicable user manuals

Test Performed: Reviewed position descriptions, user manuals, and interviewed staff.

Test Results: The Chief Information Security Officer was responsible for “policy development, planning, implementation and administration.” Additionally, the Chief Information Security Officer was responsible for the development of “confidential comprehensive IT security plans and procedures.”

Position descriptions, which define the requirements of the job were available upon request and were posted for open positions. Additionally, staff members were automatically notified when their position description was updated.

The common system user manuals provided information on processing integrity and security. The applicable common systems’ manager was responsible for updates to each of the user manuals and communicating the applicable changes to the users.

According to Department management there were no updates to the user manuals during the review period.

No deviation noted.

Criteria: 2.4 - The process for obtaining support and informing the entity about system processing integrity issues, errors and omissions, and breaches of systems security and for submitting complaints is communicated to authorized users.

Department’s Control: The process for users to inform the Department of possible security issues and other incidents is posted on the Department’s website. The General Security For IT Resources Access Policy documents the process for users to inform their supervisor of security incidents. The common system user manuals include information concerning processing integrity issues, and the process for informing the CMS Service Desk.

Test Performed: Reviewed Department’s website, policies, procedures, user manuals, and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated anyone suspecting a security breach, including lost or broken IT resource assets were to report the incident to their immediate supervisor.

In addition, the Department’s website instructed users to contact the Customer Service Center (Help Desk) regarding security issues. However, procedures had not been developed to ensure Help Desk staff assigned suspected breaches or security incidents to appropriate managers.

According to the Critical Incident Response Procedures, if the Major Outage Response Team and/or the Department’s Infrastructure Services Team had determined an incident had occurred, they were to determine the extent and if applicable, the Critical Incident Response Team was to be notified. In the event it was determined the incident was considered minor, the Department’s Help Desk was to handle.

The common system user manuals directed the users to contact the CMS Service Desk (Help Desk) in the event issues were encountered.

Procedures had not been developed to ensure suspected breaches, security incidents, or processing integrity issues were assigned to managers.

Criteria: 2.5 - Changes that may affect system processing integrity and system security are communicated to management and users who will be affected.

Department's Control: Infrastructure changes are communicated to users and management via the CAC meetings; in which the meeting minutes are posted on the ECM SharePoint site. Agencies have access to the ECM SharePoint site. Changes to the common systems are communicated to users via email or phone. Planned changes to the common systems are conducted during the scheduled maintenance window.

Test Performed: Reviewed ECM SharePoint site, CAC meeting minutes, and interviewed staff.

Test Results: Infrastructure changes were communicated to users through CAC meetings and reports on the ECM SharePoint site.

The ECM SharePoint site maintained various reports to inform the users:

- Change Advisory Committee Meeting Minutes,
- 30 Day Outage Report by Agency,
- Change Detail Report (Next 14 Days),
- Enterprise Change Schedule (Next 90 Days), and
- Overdue Change Report.

We reviewed the reports and meeting minutes from the ECM SharePoint site for July 2011 – January 2012, noting information related to changes.

Emails were sent to all agencies identifying the changes to be discussed at the upcoming CAC meeting and the email included a link to the SharePoint site.

System managers were to communicate common system changes to the users via email or phone; however, they were not required to maintain documentation of the communications. Additionally, planned changes were scheduled to be completed during the scheduled maintenance window.

According to Department management, there were no major changes to common systems during the review period.

No deviation noted.

**3.0 – Procedures: The entity placed in operation procedures to achieve its documented system processing integrity objectives in accordance with defined policies.**

Criteria: 3.1 - Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair processing integrity commitments and (2) assess the risks associated with the identified threats.

Department's Control: A risk assessment is performed periodically. As security threats are identified, they are assessed.

Test Performed: Reviewed Framework, risk assessments, and interviewed staff.

Test Results: The Department had developed the IDCMS/BCCS Security and Compliance Solutions IT Risk Management Framework (Framework), dated December 15, 2009, to assist in conducting risk assessments.

The Framework stated the risk management strategy the Department had undertaken was based on the model of continuous identification, assessment, treatment, and monitoring. Each 'phase' of the model outlined the tasks to be completed and the outcome/deliverable to be obtained.

Although the IT Risk Management Framework had been in place since December 2009, the Department had only recently embarked on a project of mapping the Department's IT controls to the principles/controls documented in the National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA). The Department was in the process of identifying the various controls, risks, business owners, artifacts and if applicable, the compensating controls.

During the review period, the Department had not conducted any other risk assessments.

The Department had recently started conducting risk assessments over the IT environment.

Criteria: 3.2 - The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integrity policies.

Department's Control: The common system user manuals provide procedures related to the completeness and accuracy of transactions, which are to be followed by users. Data entry screens contain field edits and range checks. Error handling procedures are followed during data origination to ensure that errors and irregularities are detected, reported, and corrected. Logical access controls restrict data entry capabilities to authorized personnel.

Test Performed: Reviewed user manuals, edits, errors, and interviewed staff.

Test Results: The CPS User Manual provided users with guidance on the entry of data, edits, and errors. CPS contained online edit checks to ensure transactions entered were valid. If an error occurred during data entry, users were not allowed to continue until the error had been corrected.

The online data entry function had error codes and corresponding messages, which were displayed online when an error occurred, and the field which contained the error was highlighted. Although the error messages were not discussed directly in the CPS Manual, the messages were understandable, and the CPS Manual would identify acceptable values for the field. In the event, the user encountered issues they could not resolve; the CPS User Manual instructed them to contact the CMS Service Desk.

We reviewed 20 CPS edits and errors, noting no exceptions.

The CTAS User Manual provided users with guidance on the entry of data, edits, and errors. CTAS contained online edit checks to ensure transactions entered were valid. If an error occurred during data entry, users were not allowed to continue until the error had been corrected.

We reviewed 20 CTAS edits and errors, noting no exceptions.

The AIS User Manual provided users with guidance on the entry of data, edits, and errors. AIS contained online edit checks to ensure transactions entered were valid. If an error occurred during data entry, users were not allowed to continue until the error had been corrected.

We reviewed 50 AIS edits and errors, noting no exceptions.

The CIS User Manual provided users with guidance on the entry of data, edits, and errors. CIS contained online edit checks to ensure transactions entered were valid. If an error occurred during data entry, users were not allowed to continue until the error had been corrected.

We reviewed 38 CIS edits and errors, noting no exceptions.

Input, accuracy, and authorization of data was the responsibility of the user agencies. Additionally, the establishment of logical access controls which restricted data entry capabilities was the responsibility of user agencies.

No deviation noted.

Criteria: 3.3 - The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies.

Department's Control: The common system user manuals provide procedures related to the completeness and accuracy of transactions, which are to be followed by users. Data entry screens contain field edits and range checks. Error handling procedures are followed during data origination to ensure that errors and irregularities are detected, reported, and corrected. The common systems provide various balancing reports to ensure accuracy of information.

Test Performed: Reviewed user manuals, agency data, and interviewed staff.

Test Results: The CPS User Manual provided users with guidance on the entry of data, edits, and errors. CPS contained online edit checks to ensure transactions entered were valid. If an error occurred during data entry, users were not allowed to continue until the error had been corrected.

Once CPS data was entered successfully, the Department staff executed a Gross-to-Net program, which processed the batch transactions for any errors and generated a Tentative Vouchers Report. If no errors occurred, a copy of the Tentative Vouchers Report was forwarded to the agencies for approval prior to being submitted to the Comptroller's Office for warrant generation. If an error occurred, it would be identified on the report, which also contained payroll totals and statistics. The totals and statistics were used by Department staff to ensure all payrolls had been processed. If an error occurred and could be fixed, the Department staff would fix the error, reschedule another voucher and complete a Payroll Adjustment form. The Payroll Adjustment forms were used to notify the agency of the error/correction. Each pay period standard payroll reports were provided to agencies.

We reviewed two agencies' CPS data and tested employee identification numbers, voucher numbers, warrant amounts, retirement tier, and date fields for proper input, edits, and compliance with date standards. We determined the 43,106 data records tested were entered properly and complied with date composition standards. During our testing of CPS data, we noted no exceptions.

The CTAS User Manual provided users with guidance on the entry of data, edits, and errors. CTAS contained online edit checks to ensure transactions entered were valid. If an error occurred during data entry, users were not allowed to continue until the error had been corrected.

During the "close" process, CTAS generated an error report, a reconciliation report, and a file maintenance activity report. All noted errors were to be reconciled before the "close" would be finalized.

We reviewed two agencies' CTAS data and tested date fields, vacation balances, and employee identification numbers for proper input, edits, and compliance with date standards. We determined the 10,404 data records tested were entered properly and complied with date composition standards. During our testing of CTAS data, we noted no exceptions.

The AIS User Manual provided users with guidance on the entry of data, edits, and errors. AIS contained online edit checks to ensure transactions entered were valid. If an error occurred during data entry, users were not allowed to continue until the error had been corrected.

AIS provided users with several different reports; balancing reports, vendor reports, appropriation reports, etc. Additionally, users were able to request specific reports. The AIS User Manual provided a listing of the various reports available to the users.

We reviewed two agencies' AIS data and tested the accounting records for proper input, edits, and compliance with data standards. We determined the 84,322 data records tested were

properly entered within the established parameters and compiled with the data composition standards. During our testing of AIS data, we noted no exceptions.

The CIS User Manual provided users with guidance on the entry of data, edits, and errors. CIS contained online edit checks to ensure transactions entered were valid. If an error occurred during data entry, users were not allowed to continue until the error had been corrected. Data entered into CIS was the responsibility of the user agency.

CIS provided users with inventory, transaction, and depreciation reports. Additionally, users were able to request special reports.

We reviewed two agencies' CIS data and tested the inventory records for proper input, edits, and compliance with date standards. We determined the 27,715 records tested were entered properly and compiled with date composition standards. During our testing of CIS data, we noted no exceptions.

Input, accuracy, and authorization of data was the responsibility of the user agencies.

No deviation noted.

Criteria: 3.4 - The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing integrity policies.

Department's Control: The common system user manuals outline various reports which may be produced for the user agency.

Test Performed: Reviewed user manuals and interviewed staff.

Test Results: Each pay period, the following standard CPS reports were provided to agencies:

- Personal Services Expenditure,
- Personal Services Expenditure/With Insurance,
- Employer Retirement Pick-Up,
- University Retirement Report,
- Group Insurance Salary Refund Report,
- Payroll/Group Insurance Discrepancy Report, and
- Position Occupied Report.

The reports were produced and retained by the Department until the user agency retrieved them.

CTAS provided user agencies two types of reports; Close Reports and Supplemental Reports. Each type of report had various reports, providing specific information. The CTAS User Manual outlined the various reports available to user agencies.

AIS provided users with several different reports; balancing reports, vendor reports, appropriation reports, etc. Additionally, users were able to request specific reports. The AIS User Manual provided a listing of the various reports available to the users.



The CTAS and AIS reports were able to be produced at the user agency or available on line, via Mobius. Additionally, the users had the capability for reports to be produced at the Department's print shop.

CIS provided users with inventory, transaction, and depreciation reports. Additionally, users were able to request special reports. The reports were produced at the user agencies.

Input, accuracy, and authorization of data was the responsibility of the user agencies.

No deviation noted.

Criteria: 3.5 - There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.

Department's Control: Each transaction is assigned an identifying number. The Department maintains transaction history for a defined period of time.

Test Performed: Reviewed user manuals, agency data and interviewed staff.

Test Results: As each transaction was entered into the common systems an identifying number (voucher number, control number, tag number) was assigned. During our review of the agencies common system data, we noted identifying numbers had been assigned to each transaction.

The Department maintained transaction history of:

- 12 years for CPS,
- 8 years for CTAS,
- 2 years for AIS, and
- 8 years for CIS.

The original source documentation was the responsibility of the user agency.

No deviation noted.

### **Security-related criteria relevant to the system's processing integrity**

Criteria: 3.6 - Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:

Criteria: A - Logical access security measures to access information not deemed to be public.

Department's Control: Logical access to information is protected through system security software and application security. Access to resources is granted to authenticated users based on the user's identity. System options have been configured to protect system resources.

Test Performed: Reviewed security default settings, security profiles, operating system defaults and parameters, access to specific system libraries, programs and data, authentication servers, vendor website, and interviewed staff.

Test Performed: Reviewed security default settings, security profiles, operating system defaults and parameters, access to specific system libraries, programs and data, authentication servers, vendor website, and interviewed staff.

Test Results: System software integrated with Resource Access Control Facility (RACF) security software controlled logical access. Users must have a valid RACF ID and password before they could gain access to resources. Access rights were user specific and based on those rights, users were permitted or denied access to resources.

We reviewed a sample of access rights, noting access to system level data was restricted.

Additionally, we reviewed established security default settings, noting users were required to have an authenticated ID and password to access system resources. We also reviewed system options to ensure access to system libraries, programs and data were adequately secured, noting one ID had excessive powerful access privileges.

Authentication servers were utilized to provide authorized access to the firewalls, routers, and switches.

One ID had excessive powerful access privileges.

Criteria: B - Identification and authentication of authorized users.

Department's Control: Users establish their identity and authentication to systems and applications through the use of user IDs and passwords. Unique user IDs are assigned to individual users. The sharing of individual IDs is prohibited. Password configurations have been established.

Test Performed: Reviewed security reports, security profiles, access to specific special purpose IDs, authentication servers, RACF, account parameters, and interviewed staff.

Test Results: Users were required to have a valid RACF ID and password before gaining access to mainframe resources.

We reviewed 107 users, noting eight active special purpose IDs (i.e. functional area – Command Center Consoles) were not uniquely assigned, and two IDs assigned to a retired staff member were still active.

In addition, we reviewed RACF reports and screens, noting users were identified and authenticated.

Passwords were complex and required specific syntax. Security configuration parameters forced passwords to be changed in defined intervals. Access was automatically revoked after a period of inactivity. Additionally, security configuration parameters forced IDs to be disabled after a defined number of unsuccessful login attempts.

The Network Services and LAN Services authentication servers utilized an administrative architecture in which groups were established with specific levels of administrative privileges for the individual's needs.

Upon review of the established parameters, we noted parameters had been established which required passwords to utilize specific syntax, forced passwords to be changed in defined intervals, maintained a history of previous passwords utilized, and disabled accounts after a defined number of unsuccessful login attempts.

The common system user manuals outlined the security requirements of authorized users. Access was controlled through RACF. Users must have a properly authorized security software user ID and password to gain access to the operating environment. Once access to the operating environment was obtained, users were required to use a separate application user ID and password to gain access.

The establishment of user access at the user agencies was the responsibility of each agencies Security Administrator.

Special purpose IDs were not always specifically assigned and IDs assigned to a retired staff member were still active.

Criteria: C - Registration and authorization of new users.

Department's Control: Network Services required manager review and approval of new access rights. LAN Services utilized the LAN Services Access Authorization in order for staff to obtain access rights. Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form and submit via a Remedy Enterprise Service Request. The Mainframe Application Access Request Form indicates the access required and proper approval. The ability to create and modify user access rights is limited to authorized staff.

Test Performed: Reviewed standards, authorization request forms, personnel listings, Mainframe Security Procedures, Mainframe Application Access Form, new hire listing, and interviewed staff.

Test Results: The Department had not developed procedures related to the registration and authorization of users; however, divisions within the Department had developed specific procedures.

Network Services was notified by Personnel when a new individual began employment. Once notified, the Network Services Management would decide the appropriate access privileges to be granted to the individual. Documentation of the request and approvals was not required to be maintained.

To ensure proper access was assigned to the LAN Services technicians, LAN Services had developed and implemented the LAN Equipment Access Rights Standard (dated November 23, 2010).

The Standard required supervisors to complete the LAN Services Access Rights Authorization (Form) for new individuals to obtain access.

Upon review of personnel listings, detailing new hires and transfers, we noted no individuals had been hired or transferred into the Network Services or LAN Services Teams.

The Mainframe Security Procedures stated in order to obtain a RACF ID, the Department or proxy agency user was required to complete the Mainframe Application Access Request Form. However, the Procedures had not been updated to reflect the process of submitting the Form via a Remedy Enterprise Service Request to the Help Desk.

The Mainframe Application Access Form indicated the required access and was to be approved by the user's supervisor.

During the review period, the Department had two new hires which required the completion of the Mainframe Application Access Request Form. Our review of the Forms indicated no exceptions.

Procedures related to the registration and authorization of users had not been developed. In addition, documentation of access requests for Network Services was not maintained.

Criteria: D - The process to make changes and updates to user profiles.

Department's Control: Network Services is notified by Personnel of changes in an individual's employment status and makes changes to user's access rights accordingly. Changes to LAN Services staff access rights are made based on the approved LAN Services Access Rights Authorization. Changes, updates, and password resets to Department and proxy agency user profiles are completed by the Department's RACF Coordinator and/or the RACF Security Administrator. Changes are made based on the approved Mainframe Application Access Request Form submitted via a Remedy Enterprise Service Request. Bi-monthly the Department's RACF Coordinator receives a separation report documenting separations from all agencies. The Department's RACF Coordinator will review and revoke the user's ID. Bi-annually, the Department's RACF Coordinator will send all agencies a listing of their users, requesting the agency to review for accuracy, note any modifications, and return to the Department.

Test Performed: Reviewed standards, authorization request forms, personnel listings, Mainframe Security Procedures, Mainframe Access Request Forms, separation listing, violation reports, emails, DS Monitor Report, access associated with high-level access privileges, and interviewed staff.

Test Results: The Department had not developed policies related to the changing and updating of user profiles; however, divisions within the Department had developed specific procedures. Additionally, policies or procedures requiring the periodic review of access rights did not exist.

Network Services was notified by Personnel of changes in an individual's employment. Once notified, Network Services would make necessary adjustments to the individual's access privileges. Documentation of the request and approvals was not required to be maintained.

To ensure proper access was assigned to the LAN Service technicians, LAN Services had developed and implemented the LAN Equipment Access Rights Standard (dated November 23, 2010).

The Standard required supervisors to complete the LAN Services Access Rights Authorization (Form) for existing individuals whose access rights needed to be removed.

Upon review of personnel listings, detailing individual separations and transfers, we noted no individuals had left the Network Services Team and two individuals had left the LAN Services Team. We reviewed the Forms for the two individuals, noting no exceptions.

In the event an individual's RACF access required modification, the Mainframe Access Request Form was to be completed and submitted to the Help Desk via a Remedy Enterprise Service Request (ESR). Once the Help Desk received the ESR, it was reviewed and a change ticket was created, along with the ESR and the Mainframe Access Request Form being attached. The Change Ticket was then assigned to the applicable Team for completion.

Upon receipt of the change ticket, the RACF Security Administrator or RACF Coordinator would make the appropriate updates, inform the individual or the individual's supervisor, if applicable and close the change ticket.

We noted ten individuals who had RACF IDs and had separated from the Department. We requested the Mainframe Access Request Form documenting the revocation of the IDs for the ten individuals; two Forms could not be located. Our review of the remaining eight Forms indicated no exceptions.

The Mainframe Security Procedures stated twice a month, the RACF Coordinator was to receive a separation report documenting separations from all agencies. The RACF Coordinator was to revoke the separated user's accounts. According to the RACF Coordinator, he received the separation reports and revoked the applicable accounts; however, documentation was not maintained.

On June 16, 2011 the Department's Deputy Director issued a memo to all State agencies implementing a new process for the resetting of RACF passwords. Effectively immediately, the user was to send an email to the Help Desk stating:

- Full Name,
- Agency,
- RACF ID, and
- Telephone number.

Upon receipt, the Help Desk would verify the information and phone the individual with a temporary password. The temporary password was not to be left on voice mail, provided to another individual or emailed.

During an interview with the Department's RACF Coordinator on March 14, 2012, it was stated he was not aware of the new process for resetting RACF and had not received the memo. The Department's RACF Coordinator indicated he received telephone calls and direct emails requesting RACF password resets.

In the event an individual would telephone the Department's RACF Coordinator, he would reset the password at that time. If the individual would send an email he would respond to the email with the temporary password.

Upon discussion with Department management, they notified the Department's RACF Coordinator on April 13, 2012 of the Department's process for resetting RACF passwords.

In order to ensure the Department's RACF Coordinator was complying with the new process, we reviewed the Violation Reports for the weeks of April 27 and May 4, 2012, noting the RACF password resets. During these two weeks, there were 19 resets which required an email from the user; our review indicated two resets did not have the corresponding email.

On a bi-annual basis the Department's RACF Coordinator was to send agencies a listing of their users for verification of appropriateness. The agencies were to review, note any modifications and return the listing to the Department's RACF Coordinator. On January 31, 2012, the Department's RACF Coordinator sent out the listings to the agencies requesting review.

The ability to change a user profile in RACF was limited to specific staff with special access rights. In addition, the capability to update user profiles (access rights to resources designated to a specific agency) was delegated to the RACF Coordinator and the RACF Security Administrator.

We reviewed the DS Monitor's Selected User Attribute Report noting access to high-level access privileges were restricted to security software administration staff. However, we noted one staff member with excessive high level access privileges. The RACF Security Administrator stated they performed updates to IDs for technical staff when requested.

We noted the RACF Coordinator performed updates to IDs for non-technical staff as well as specific (proxy) agencies. The RACF Security Administrator indicated the RACF Coordinator

had access to the proxy agencies default security group and special access permissions for making updates to proxy agencies user profiles. We reviewed the DS Monitor's Selected User Attribute Report and access to specific default user groups and confirmed the RACF Coordinator had access for making updates to proxy agencies user profiles.

Procedures related to the changing and updating of user profiles had not been developed. In addition, the Department did not follow the documented process for resetting RACF passwords and documentation of changes in access rights for Network Services was not maintained. Additionally, one staff member had excessive high level access privileges.

Criteria: E - Distribution of output restricted to authorized users.

Department's Control: The distribution of output is restricted to authorized users via logical and physical security barriers. Distribution of digital output is restricted to authorized users through the management of system software tools or the online viewing software. Distribution of hardcopy output is restricted through physical and manual controls. Hardcopy output is printed at a secure facility with security guards. Upon request for pick up, the individual must identify themselves and be on the authorization listing.

Test Performed: Reviewed Report Distribution Logs, observed pickup process, toured facility, and interviewed staff.

Test Results: The Department of Revenue maintained the print shop utilized by agencies. The print shop was secured by proximity card readers, which required unique access codes. In addition, security guards staffed the facility 24/7.

The Department of Central Management Services, Department of Healthcare and Family Services and the Department of Human Services print jobs were maintained in the secure print shops until they were picked up. The print jobs were picked up at the loading dock each morning by each agency's messenger. All other print jobs were taken to the Report Distribution Room. The individual picking up the reports must provide identification and sign the Report Distribution Log. Department of Revenue staff would then check the individual against an authorization listing before allowing them to take the reports.

On March 2, 2012, we observed the pickup process, noting no exceptions.

Additionally, we reviewed 25 individuals from the Report Distribution Logs for the weeks of October 24, 2011, November 14, 2011, December 12, 2011, and January 17, 2012 to determine if the individuals picked up reports were authorized, noting no exceptions.

In addition to obtaining hardcopy reports, agencies may view certain reports via an online reporting tool, Mobius. The reporting tool was secured via security software, which allowed only authorized individuals to view reports. It was the responsibility of each agency to establish appropriate access rights for their staff.

No deviation noted.

Criteria: F - Restriction of access to offline storage, backup data, systems, and media.

Department's Control: Access to offline storage, backup data, system and media is limited to authorized staff via physical and logical access controls.

Test Performed: Reviewed security profiles, access to DASD and system backup resources, and interviewed staff.

Test Results: The card key system was utilized to control and restrict access to the Central Computing Facility (CCF) and Communications Building. Proximity card readers were installed on the building's exterior doors and strategically throughout the interior of each building.

Resource Access Control Facility (RACF) security software restricted access to offline storage, backup data, systems, and media. To access systems and resources, users were required to have a valid RACF user ID and password.

In order to create, modify or delete a RACF ID, a Mainframe Application Access Request Form was to be completed and submitted via an Enterprise Service Request (ESR). The ESR was then assigned to the RACF Security Administrator or RACF coordinators for the granting of access.

During the review period, we noted one new employee had been hired to Enterprise Storage and Backup Team. We reviewed the Mainframe Access Request Form, noting no exceptions.

We reviewed a sample of access rights to these resources, noting no exceptions. Department management indicated periodic reviews of access rights were conducted; however, documentation was not maintained.

No deviation noted.

Criteria: G – Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).

Department's Control: Operating system configuration defaults are restricted to authorized personnel through logical access controls. Utility programs that can read, add, change or delete data or programs are restricted to authorized personnel. Master passwords are maintained in an encrypted database and also maintained in a secure safe. Authentication servers are utilized to control access, log access attempts, and alert management.

Test Performed: Reviewed system defaults, DS Monitor and CA-Examine reports, system consoles, supervisory calls, system exits, access over master passwords, access restrictions to powerful utilities, SMF recordings, access over SMF records, assessed access to APF-authorized libraries, authentication servers, access rights, device configurations, and interviewed staff.

Test Results: System software integrated with Resource Access Control Facility security software controls logical access. Users must have a valid RACF ID and password before they would gain access to resources.



We reviewed the DS Monitor's Selected User Attribute Report noting access to high-level access privileges were restricted to security software administration staff. The RACF Security Administrator stated they performed updates to IDs for technical staff when requested.

Based on our review of DS Monitor reports, we noted the Department encrypted the password database.

We confirmed a copy of the master password was maintained in a secured safe.

Authentication servers were utilized to provide authorized access to the firewalls, routers, and switches maintained by Network Services and LAN Services. We reviewed firewall and router configurations for the IP addresses of defined authentication servers and compared those IP addresses to those of the authentication servers in production.

Upon review of the firewall and router configuration files for Network Services, we noted all devices, except one, reviewed (5 firewalls and 109 routers) used all three of the Network Services authentication servers.

Additionally, we reviewed the users which had access to all firewalls, routers, and switches controlled by the three Network Services authentication servers, noting accounts with powerful access rights appeared to be appropriately assigned and controlled.

Upon review of the firewall and router configuration files for LAN Services, we noted all devices reviewed (47 firewalls and 17 routers) used both of the LAN Services authentication servers.

Additionally, we reviewed the user which had access to all firewalls, routers, and switches controlled by the two LAN Services authentication servers, noting accounts with powerful access rights appeared to be appropriately assigned and controlled, with two exceptions. We identified two accounts assigned to individuals no longer requiring access. Upon notification, management removed the two accounts noted.

Two accounts assigned to staff that no longer needed powerful access were identified.

Criteria: 3.7 – Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, offline storage media, backup media and systems, and other system components such as firewalls, routers, and servers.

Department's Control: Physical access controls restrict access to authorized individuals via card key systems. Card keys are utilized to restrict access to the CCF and Communications Building. In order to obtain a card key, an ID Badge Request Form is to be completed, approval must be obtained from an authorized manager, and presentation of a valid ID. Visitors are required to sign in and out, in addition to being escorted. The CCF and the Communications Building are guarded by security guards. Video surveillance is utilized to monitor the CCF and the Communications Building. Procedures exist for the identification and escalation of physical

security breaches. Physical access controls are in place to restrict access to the offsite storage location. Access to the offsite media is limited to authorized Department personnel.

Test Performed: Toured facilities, reviewed ID Badge Request Forms, Building Admittance Registers, card key system, access rights, key inventories, Site Specific Post Orders, Special Occurrence Reports, and interviewed staff.

Test Results: The card key system was utilized to control and restrict access to the CCF and Communications Building. Proximity card readers were installed on the building's exterior doors and strategically throughout the interior of each building.

In addition to other sensitive areas at the CCF, the card key system controlled and restricted access to the data center hosting the tape library, tape cleaning room, Operations Center, Public Key Infrastructure room, and telecommunications room.

In addition to other sensitive areas at the Communications Building, the card key system controlled and restricted access to the ICN network room, server and telecommunications rooms, Network Control Center (NCC), and Technical Safeguards lab.

In order to obtain a card key, an ID Badge Request Form was to be completed. The ID Badge Request Form was to be approved by an authorized manager and the employee was to present a valid ID.

During the review period, the Department had nine new employees, which requested a card key. We requested the completed ID Badge Request Form for the nine new employees, noting one Form could not be located and two Forms were not properly completed.

Upon leaving employment, Human Resources (HR) would email the Bureau of Property Management, who would then deactivate the card key badge. On the last day of employment, the employee's supervisor was to collect the card key badge and submit to HR. HR would then submit to the Bureau of Property Management for destruction.

Additionally, we reviewed 42 individuals with access to the CCF, noting six no longer required access. Upon notification, the Department removed the access rights for these six individuals. The card key system also had an absentee limit, whereby access rights were automatically revoked.

Individuals requesting a temporary badge were required to sign the Building Admittance Register prior to receiving the temporary badge from the security guard. We reviewed 83 individuals who had signed the Building Admittance Register for the CCF or the Communications Building and compared them to the access privileges defined in the card key system, noting no exceptions.

The Department had entered into a contract with a security firm to provide security guard services to select state facilities; including the CCF and Communications Building. The contract

required at least one guard be on duty 24/7 at both locations and outlined their duties and responsibilities related to patrolling, and incident response/reporting.

In addition to the card keys, specific employees were also provided real property keys. The real property keys allowed access to specific doors within each facility. We reviewed the listing of real property keys for the CCF and Communications Building, noting:

- 63 of the 274 keys issued for the CCF could not be accounted for,
- 32 of the 207 keys issued for the Communications Building could not be accounted for,
- 13 of the 20 Grand Master keys for the CCF were indicated as lost or not found, and
- 3 of the 17 Grand Master keys for the Communications Building were indicated as lost or not found.

Additionally, video cameras were strategically placed throughout the interior and surrounding the exterior of the CCF and the Communications Building. Video feeds were monitored at the consoles located at the security guard desks. We viewed the digital video feeds, noting cameras were positioned to allow for clear unobstructed views and images were clear.

The guards at the CCF and the Communications Building maintained Site Specific Post Orders. The Orders provided general guidance and instructions related to the security guard's duties. In addition, the Orders provided guidance in responding to various types of "emergencies/threats."

Upon notification of an emergency/threat, the security guards were to contact the appropriate authorities and Department management. In addition, the security guards were to complete a Special Occurrence Report and submit it to the Facility Manager.

During the review period, there were three Special Occurrence Reports completed. The Reports indicated the security issues and the resolutions.

Offsite media was stored at a secure facility. Access to the facility was restricted to facility staff and authorized Department staff. We reviewed the listing of Department staff with access, noting no exceptions.

The Department did not ensure the ID Badge Request Form was properly completed and maintained. Additionally, the Department did not have adequate controls to ensure the timely deactivation of card key access rights or track and maintain real property keys.

Criteria: 3.8 – Procedures exist to protect against unauthorized access to system resources.

Department's Control: Access to system resources is restricted to authorized personnel through security software. Access to high-level access privileges is limited to security administration personnel. Firewalls and routers are used and configured to prevent unauthorized access.

Test Performed: Reviewed security defaults, security profiles, DS Monitor and CA-Examine reports, device configurations, hardware listing, vendor website, and interviewed staff.

Test Results: Access to system resources was restricted to authorized personnel. We reviewed the security default settings and confirmed access to system resources required an authenticated ID and password using complex password configuration requirements. We also reviewed the DS Monitor reports to review access rights to system-level libraries and high-level privileges. We noted two staff members with excessive access privileges.

The Department maintained the State of Illinois Statewide Network. Network Services (Network Operations and Enterprise Network Support) and LAN Services were tasked with maintaining the State's primary network consisting of firewalls, routers and switches.

We reviewed configurations, which contained software revision levels and fully documented high-level rule base descriptions, for a sample of devices (52 firewalls and 126 routers) maintained by Network Services and LAN Services, noting devices were configured to utilize authentication servers, logging servers and contained banners prohibiting unauthorized access and warning of prosecution. In addition, devices contained Access Control Lists (ACLs) to deny and permit specific types of network traffic.

Two staff members had excessive access privileges.

Criteria: 3.9 – Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.

Department's Control: The ability to install, modify, and replace operating systems is limited to authorized staff. Access to sensitive system functions is restricted to authorized staff. The Security and Compliance Solutions Team participates in user groups and subscribes to services related to computer viruses.

Test Performed: Reviewed access to system libraries and resources, security profiles, DS Monitor and CA-Examine Reports, emails, and interviewed staff.

Test Results: Users must have a valid RACF ID and password before they would gain access to resources.

We reviewed a sample of access rights to system configurations, powerful system privileges, and powerful utilities, noting one ID had excessive powerful access privileges. Additionally, we reviewed system defaults, access to system libraries including authorized libraries, security over established consoles and system monitoring, noting no exceptions.

The Department was a member of the Multi-State Information Sharing and Analysis Center, which provided members notifications related to security issues. We reviewed the notifications, noting they were received on an as needed basis and were prioritized based on criticality.

One ID had excessive powerful access privileges.

Criteria: 3.10 – Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.

Department's Control: The Department utilizes encryption technologies and access gateways for the transmission of sensitive or confidential information.

Test Performed: Reviewed standards, web portal, Department website, and interviewed staff.

Test Results: Network Services maintained 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, managed and maintained by Network Services, was utilized by the VPN solution.

To assist in managing and maintaining the Enterprise VPN solution, Network Services had developed the following standards:

- CMS Enterprise Virtual Private Network (VPN) Standard, and
- Enterprise VPN – Individual Remote Access Using SSL.

The CMS Enterprise VPN Standard defined the two types of VPNs currently available (individual remote access and site-to-site), as well as the type of encryption supported for the VPNs.

The Individual Remote Access Standard defined 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 were current on security and antivirus patches.

Upon review of the web portal utilized to login to the Enterprise VPN, we noted the existence of the security banner outlined in the Individual Remote Access Standard. Additionally, upon review of the web portal, we noted the security of authentication and communications to and from the web portal were the same as defined within the Individual Remote Access Standard.

Additionally, LAN Services maintained additional VPN technologies for eight agencies; however, we noted the technologies were aging. LAN Services had a project underway to migrate these VPNs to the Enterprise VPN Solution managed and maintained by Network Services. Department management indicated they would like to have the project completed within the next 12 months.

The State of Illinois Digital Signature Project provided a comprehensive system for public-key encryption and digital signature services (public-key infrastructure (PKI)). Public-key technology provided stronger levels of identification, privacy (encryption), verification and security management capabilities.

No deviation noted.

### **Criteria related to execution and incident management used to achieve objectives**

Criteria: 3.11 – Procedures exist to identify, report, and act upon system processing integrity issues and related security breaches and other incidents.

Department's Control: The Department has tools in place to identify, log, and report security breaches and other incidents. The Department's website provides users instructions for communicating security issues to the CMS Service Desk. The Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provided guidance to users for the reporting of lost or stolen assets.

Test Performed: Reviewed spreadsheets, device configurations, SolarWinds, vendor website, authentication servers, Department's website, policies, procedures, CIRT Reports, Remedy tickets, and interviewed staff.

Test Results: The General Security For Statewide IT Resources Policy stated anyone suspecting a security breach, including lost or broken IT resource assets were to report the incident to their immediate supervisor. However, the Policy did not document the actions to be taken by the supervisor.

Additionally, the Department's website instructed users to contact the Customer Service Center (Help Desk) regarding security issues. However, no policies or procedures had been developed to ensure Help Desk staff assigned suspected breaches or security incidents to appropriate managers.

According to the Critical Incident Response Procedures, if the Major Outage Response Team and/or the Department's Infrastructure Services Team had determined an incident had occurred, they were to determine the extent of the incident and if applicable, notify the Critical Incident Response Team. In the event it was determined the incident was considered minor, the Department's Help Desk was to be notified. However, our review of the Procedures indicated it did not document the process for identifying security breaches and other incidents, tracking or logging of the incident and the process which the Help Desk was to follow for minor incidents.

In addition, the Critical Incident Response Procedures stated for each event a CIRT Report was to be completed, which documented the specifics of the event, devices affected, and the resolution the Critical Incident Response Team took. We reviewed 18 CIRT Reports, noting no exceptions.

The Enterprise Desktop/Laptop Policy and Mobile Device Security Policy stated users were to inform the Department's Help Desk of all lost or stolen assets.

According the Department, there were five laptops which were reported lost or stolen during the review period. Upon further review, we noted four of the laptops were not protected with encryption as required by the Laptop Data Encryption Policy.

In addition, we reviewed the CIRT Reports to determine if a Report had been completed for the lost/stolen laptops, noting they had not.

Network Services had configured three servers to function as the primary logging servers for the firewalls, routers, and switches it maintained. To confirm, during our review of the configuration files for selected devices (5 firewalls and 109 routers), we identified the IP addresses of the defined logging servers in the configuration files. We noted all devices reviewed, except one, utilized logging servers. However, we did note seven Network Operations devices which did not utilize all three logging servers. In addition, we noted devices were configured to utilize several additional logging server in addition to the three primary logging servers that were utilized.

According to Department staff, log files on the logging servers utilized by Network Services were not typically reviewed in a proactive manner for potential incidents. Typically, log files located on these servers were utilized for error identification and resolution purposes.

LAN Services had configured two servers to function as the primary logging servers for the firewalls, routers, and switches it maintained. To confirm, during our review of the configuration files for selected devices (47 firewalls and 17 routers), we identified the IP addresses of the defined logging servers in the configuration files. We noted all devices reviewed utilized the two logging servers utilized by LAN Services. In addition, we noted two additional IP addresses which had been designated as logging servers. Upon follow-up with Department management, we noted the IPs were no longer active.

To monitor the log files for potential issues, LAN Services had assigned an individual the responsibility of proactively reviewing logs daily for select devices. These reviews, as well as any issues noted, were tracked in a spreadsheet. Any issues identified were referred to the LAN Services Data Center Team for further review.

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

According to Department staff, all Network Services devices were connected to NPM. For each of the Network Services devices (5 firewalls and 109 routers) we reviewed configurations for, we also reviewed NPM to ensure connectivity of each of the devices to SolarWinds; noting all devices, except one, were connected to NPM.

According to Department staff, all LAN Services devices were connected to NPM. For each of the LAN Services devices (47 firewalls and 17 routers) we reviewed configurations for, we also reviewed NPM to ensure connectivity of each of the devices to SolarWinds; noting all devices were connected to NPM.

In addition Network Services and LAN Services had implemented controls to allow them to monitor failed access attempts to networking devices.

According to Department management, in the event a breach was identified, Network Services and LAN Services would utilize the Data Breach Notification Policy and the Action Plan for Notification of a Security Breach posted on the Department's website. In addition, a Remedy ticket would be opened and if necessary the Technical Safeguards Team would be alerted.

The procedures did not document a process for identifying incidents, or the complete process for reporting and acting upon security breaches or incidents. In addition, discrepancies in the assignment of logging servers existed.

### **Criteria related to the system components used to achieve the objectives**

Criteria: 3.12 – Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.

Department's Control: 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 Business Reference Model is periodically updated by the applicable agency.

Test Performed: Reviewed Policy, Department's data classification, and interviewed staff.

Test Results: The Business Reference Model collected and stored information related to application and data processing services provided based on the Data Classification and Protection Policy. The Data Classification and Protection Policy was developed to inform "data owners and data users the data classification and protection schema used by CMS/BCCS for protecting data."

The Policy outlined three categories in which data was to be classified:

- Public,
- Official Use Only, and
- Confidential.

The Data Classification and Protection Policy stated it was the responsibility of the data owner to determine the appropriate classification over their data and to ensure the appropriate security and protection protocols were in place.

In March 2011, the Department undertook a project to begin classifying their data in accordance with the Data Classification and Protection Policy.

As of March 2012, the Department had determined they were the data owners for 176 applications. Our review indicated:

- 38 had been classified as confidential,
- 36 had been classified as Official Use Only,
- 11 had been classified as Public, and
- 91 had not been classified.



The Department had not completed the classification of its data.

Criteria: 3.13 – Procedures exist to provide that issues of noncompliance with system processing integrity and related security policies are promptly addressed and that corrective measures are taken on a timely basis.

Department's Control: Department staff are assigned the responsibility for monitoring and ensuring compliance with security policies.

Test Performed: Reviewed policies and interviewed staff.

Test Results: According to the Department's security policies posted on their website, the Department and security personnel were responsible for the monitoring, auditing, tracking, and for the validation of compliance with the policies and procedures. Additionally, they were responsible for investigating violations of laws, policies, and procedures.

The policies did not define who the security personnel were and we were unable to determine who, within the Department was responsible. In addition, according to the Chief Information Security Officer; the designated personnel referenced in the policies had not been defined or formally assigned.

The Department had not clearly defined and communicated security personnel assignments.

Criteria: 3.14 – Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.

Department's Control: The IT Governance Policy governs the acquisition of systems and technology. Additionally, as part of the Governance process, agencies are to classify the data and system in accordance with the Data Classification and Protection Policy. The Remedy Change Management Guide guides the development, implementation and maintenance of systems. Standards provide guidance on the configuration and deployment of network devices. Authentication servers are utilized to control access to networking devices. Network diagrams are maintained. The Enterprise Application and Architecture Flowchart documents the change process; from initiation to production.

Test Performed: Reviewed IT Governance Policy, IT Governance Gates (templates), IT Guiding Principles, charters, Remedy Change Management Guide, standards, authentication servers, network diagrams, EAA Change Management Flowchart, and interviewed staff.

Test Results: To help achieve the acquisition and management of systems and technology, the Department developed the IT Governance Policy, IT Guiding Principles, and the IT Governance Gates, which were published on the Department's website.

IT Governance Policy stated “ITG applies to business-sponsored IT projects that satisfy at least one of the following criteria:

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

The Project Charter, Business Requirements, and Technical Requirements Templates solicit information related to the design, acquisition, implementation, configuration, system availability/recovery requirements, and security requirements.

All projects were to follow the IT Governance process. Any exceptions required a waiver from the State’s CIO. During the review period, there were no exceptions that required a waiver

As part of the IT Governance process, the agencies were required to assess availability, accessibility, and data classification requirements.

We reviewed 25 charters to determine if the charters contained the required documentation and were appropriately approved, noting no exceptions.

The Remedy Change Management Guide was developed to provide corresponding procedures to the Change Management Policy. The Guide provided guidance on documenting changes and entering/tracking changes in the Remedy Action Request System. Additionally, the Guide defined the authorization and approval processes, roles and responsibilities, emergency changes, and user involvement over changes.

All changes to the infrastructure were required to follow the Guide. Additionally, the Guide stated emergency changes were to be reviewed and documented.

To assist in the configuration and deployment of network infrastructure managed and maintained by Network Services and LAN Services, various standards and templates were maintained. However, we noted the standards and templates maintained by Network Services addressed routers at the core, distribution, and access levels and did not address the other routers and firewalls they maintained. Upon review, we noted baseline configurations outlined in the documents provided for authentication servers, logging servers, and banners prohibiting unauthorized access and warning of prosecution.

To provide authorized access to configurations deployed on devices throughout the network, authentication servers were utilized by Network Services and LAN Services.

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

The Manager of the Enterprise Applications & Architecture (EAA) Division decided to transition from the established change management process to a new process during the audit period. The Manager was in the process of drafting policies and procedures related to the new process.

The EAA Change Management Flowchart (Flowchart) was developed to provide guidance for the common systems until the policies and procedures were finalized. The Flowchart indicated a request may originate via Remedy or the EPM. Once a manager determined the type of request, the request could follow the Remedy Help Desk path or the EPM change management path.

Our review of the Flowchart indicated:

- Management approvals were not required,
- Requests were not assigned a unique tracking number,
- Requests are not prioritized or categorized,
- Testing or documentation of testing requirements were not outlined, and
- Follow up after move to production was not required.

According to Department management, there were no major changes to the common systems during the review period.

Policies and procedures had not been implemented for testing, evaluating, and authorizing system components before implementation.

Criteria: 3.15 – Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting processing integrity and security have qualifications and resources to fulfill their responsibilities.

Department's Control: The Department's position descriptions specify the position's qualifications and responsibilities. The State's hiring procedures are followed for the hiring of staff. New employees are required to have background checks. Annual performance evaluations are completed. Staff is provided training based on their position's requirements. The Department conducts cross training for key positions.

Test Performed: Reviewed position descriptions, hiring procedures, background checks, performance evaluations, training records, and interviewed staff.

Test Results: The Department had established position descriptions for their positions. The position description outlined the position's responsibilities and requirements. The Personnel Code (20 ILCS 415) and the State of Illinois Personnel Rules dictated the hiring process for the Department.

New employees were required to have a background check completed prior to start of employment. We confirmed the background checks for the ten employees hired during the review period had been performed, noting no exceptions.

Employees were to receive a performance evaluation on an annual basis to provide timely feedback of their job performance. We reviewed 388 employees to determine if their annual

evaluation had been completed on a timely basis noting, 190 (49%) had not received an evaluation by the prescribed date.

Employees were to receive mandatory training upon hiring; ethics, Family Medical Leave Act (FMLA), Health Insurance Portability and Accountability Act (HIPAA), and sexual harassment. In addition, employees were to continue to receive job specific training.

During the review period, the Department hired ten new employees. We reviewed their training files, noting they had received the mandatory training upon employment. Additionally, we reviewed 92 employee training records, noting 25 employees had received additional training.

According to Department management, cross training would be completed as required for the specific job.

Performance evaluations were not always completed by the prescribed date.

### **Change management-related criteria applicable to the system's processing integrity**

Criteria: 3.16 – Procedures exist to maintain system components, including configurations consistent with the defined system processing integrity and related security policies.

Department's Control: The Remedy Change Management Guide provides guidance in maintaining system components, including system configurations. Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Standards provide guidance on the configuration and deployment of network devices. Tools are in place to assist in the deployment of and reporting on configurations. The Enterprise Application and Architecture change management process provides guidance on changes to the common systems. Users of the common systems are kept informed of via phone and email.

Test Performed: Reviewed Change Management Guide, Requests for Change (RFC), CAC meeting minutes, standards, templates, SolarWinds, vendor website, EAA Change Management Flowchart, and interviewed staff.

Test Results: The Remedy Change Management Guide provided guidance for maintaining system components, including system configurations. The Guide provided direction for the categorization, prioritization, and emergency changes.

We reviewed 50 RFCs to ensure they had been classified and prioritized, noting no exceptions. In addition, we reviewed nine emergency RFCs, noting they had been documented and approved.

Requestors were kept informed of their requests through the Change Advisory Committee documentation and the CAC meeting minutes. We reviewed the reports and meeting minutes from the ECM SharePoint site for July 2011 – January 2012, noting information related to changes.

To assist in the configuration and deployment of network infrastructure managed and maintained by Network Services and LAN Services, various standards and templates were maintained. However, we noted the standards and templates maintained by Network Services addressed routers at the core, distribution, and access levels and did not address the other routers and firewalls they maintained. Upon review, we noted baseline configurations outlined in the documents provided for authentication servers, logging servers, and banners prohibiting unauthorized access and warning of prosecution.

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

According to Department staff, all Network Services devices were connected to NCM. For each of the Network Services devices (5 firewalls and 109 routers) we reviewed configurations for, we also reviewed NCM to ensure connectivity of each of the devices to SolarWinds; noting all devices, except one, were connected to NCM.

According to Department staff, all LAN Services devices were connected to NCM. For each of the LAN Services devices (47 firewalls and 17 routers) we reviewed configurations for, we also reviewed NCM to ensure connectivity of each of the devices to SolarWinds; noting all devices were connected to NCM.

The EAA Change Management Flowchart (Flowchart) was developed to provide guidance for the common systems until the policies and procedures were finalized. The Flowchart indicated a request may originate via Remedy or the EPM. Once a manager determined the type of request, the request could follow the Remedy Help Desk path or the EPM change management path.

Department staff informed common system users of changes via email and phone.

According to Department management, there were no major changes to the common systems during the review period.

No deviation noted.

Criteria: 3.17 – Procedures exist to provide that only authorized, tested, and documented changes are made to the system.

Department's Control: The Remedy Change Management Guide provides guidance for the authorization and documentation requirements for changes to systems. Changes are prioritized and categorized. Changes are communicated to users via the Change Advisory Committee meeting minutes and reports, which are located on the ECM SharePoint site. High impact changes require backout, test, and implementation plans to be attached to the RFC for the use in the event of a disruption. The Enterprise Application and Architecture Flowchart provide guidance related to the common systems.

Test Performed: Reviewed Remedy Change Management Guide, Requests for Change (RFC), CAC meeting minutes, EMC SharePoint site, Change Management Flowchart, EPM listing, move sheets, email approvals, and interviewed staff.

Test Results: The Remedy Change Management Guide provided guidance for the authorization, prioritization, categorization and documentation requirements. In addition, the Guide stated backout, testing and implementation plans were required to be attached to the RFC for high impact changes. However, the Guide did not document the requirements or required documentation of the various plans. The Guide stated testing was the responsibility of the Shared Services Team.

During our review, we inquired with the managers of the Shared Services Teams of their documentation related to testing of changes. The managers indicated testing was to be conducted; however, documentation was lacking. Additionally, it was indicated procedures had not been developed to outlined testing requirements or documentation requirements.

We reviewed 50 RFCs to ensure they had been properly authorized, prioritized and categorized, noting no exceptions. In addition, we reviewed 18 high impact RFCs, noting the backout, test, and implementation plans had been attached. However, we were unable to determine the adequacy of the documentation due to the lack of documented requirements in the Guide.

Changes were communicated to users through CAC meeting minutes and reports on the ECM SharePoint site. We reviewed the reports and meeting minutes from the ECM SharePoint site for July 2011 – January 2012, noting information related to changes.

The EAA Change Management Flowchart, utilized by the common systems, indicated a request may originate via Remedy or the EPM. Once a manager determined the type of request, the request could follow the Remedy Help Desk path or the EPM change management path.

According to Department management, there were no major changes to the common systems during the review period.

We reviewed the EPM listing for each common system in order to select a sample of changes to ensure compliance with the Flowchart. During our review of the listings, we noted each change was entered into EPM as one project with several milestones. However, the milestones did not provide a unique tracking number. Additionally, we noted changes related to CIS were not tracked within EPM, nor tracked elsewhere.

Due to the weaknesses identified in our review of the Flowchart (noted above), we selected a sample of milestones for AIS (3 out of 13), CTAS (6 out of 6) and CPS (11 out of 26) and requested management provide the applicable checklists, user approval/testing approval, and move sheets. In addition, we reviewed the “approval mailbox” to ensure proper approval for the move to production. Our review indicated:

- Two AIS changes required testing; however, the documentation did not indicate user or management approval, and
- The AIS programmer was authorized to “approve” moves to the production environment.

Due to CIS changes not being tracked in EPM, we were unable to select a sample for testing.

The Department had not included requirements over the backout, testing, and implementation plans in the Guide. Changes to the common systems were not adequately controlled.

Criteria: 3.18 – Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).

Department's Control: Emergency changes are required to complete the standard documentation outlined in the Change Management Policy and the Remedy Change Management Guide. Emergency changes are reviewed by the technical and business approver post implementation. Emergency changes are communicated to users post implementation via the CAC meeting. Emergency changes to the common systems follow the Enterprise Application and Architecture Flowchart.

Test Performed: Reviewed emergency Requests for Change (RFC), CAC meeting minutes and interviewed staff.

Test Results: According to the Change Management Policy, an emergency was defined as “a change that does not present notification to the formal process in advance of implementation. Emergency changes will only be acceptable in the event of a system failure or the discovery of security vulnerability.” The Policy also stated “all emergency changes will be reviewed and documented.”

The Change Management Guide defined emergency changes as unscheduled changes. Emergency changes were only acceptable in the event of a system failure or the discovery of security vulnerability. Emergency changes were to follow all change management processes except they may be implemented in advance of approval in order to correct the failure in a timely manner.

We reviewed nine emergency RFCs, noting the documentation and proper approvals were obtained. However, we did note the Policy and the Guide did not include the documentation requirements of the Post Implementation Review; therefore, we were unable to determine the adequacy of the documentation.

In addition, we reviewed the CAC meeting minutes to ensure the nine emergency RFCs had been included for discussion, noting no exceptions.

Common system changes which were deemed emergency were to follow the EAA Change Management Flowchart.

According to management, there were no emergency changes related to the common systems during the audit period.

The Policy and the Guide did not document the requirements for Post Implementation Reviews.

## **Availability-related criteria applicable to the system's processing integrity**

Criteria: 3.19 – Procedures exist to protect the system against potential risks (for example, environmental risks, natural disasters, and routine operational errors and omissions) that might impair system processing integrity.

Department's Control: The CCF and Communications Building are protected against fire using both smoke detectors and a fire suppression system. Water detectors are installed within the raised floor of the CCF. The CCF and Communications Building are protected against a disruption of power via the installation of an uninterruptible power supply and emergency power supplies. Preventive maintenance agreements and scheduled maintenance procedures are in place for key system hardware components. The common system user manuals instruct users to contact the CMS Service Desk to report any issues. Logical access to information is protected through system security software and application security. Physical access controls restrict access to authorized individuals via card key systems.

Test Performed: Toured facilities, reviewed card key systems, contracts, inspection reports, security software, user manual, and interviewed staff.

Test Results: The card key system was utilized to control and restrict access to the CCF and Communications Building. Proximity card readers were installed on the building's exterior doors and strategically throughout the interior of each building.

In addition to other sensitive areas at the CCF, the card key system controlled and restricted access to the data center hosting the tape library, tape cleaning room, Operations Center, Public Key Infrastructure room, and telecommunications room.

In addition to other sensitive areas at the Communications Building, the card key system controlled and restricted access to the ICN network room, server and telecommunications rooms, Network Control Center (NCC), and Technical Safeguards lab.

The CCF and the Communications Building maintained measures to protect against environmental factors.

The CCF third floor computer room contained fire suppression and detection systems that were Underwriter Laboratory approved and utilized an environmental friendly agency; FM-200. Upon review, we noted the system was last inspected in February 2012.

The Communications Building contained a fire detection and suppression system throughout the entire facility. Upon review, we noted the system was last inspected May 2005.

In addition to the fire suppression and detection system, the Department maintained fire extinguishers throughout the CCF and the Communications Building. During our review, we noted the fire extinguishers were inspected in January and March 2012, respectively.



The Department had maintained a preventive maintenance contract for the fire extinguishers at the CCF and the Communications Building.

Water detectors were installed within the raised floor area of the CCF. In the event sensors become damp, an alarm would sound at the Command Center.

The CCF was equipped with a uninterruptible power supply (UPS) and in the event of a power failure, the UPS would engage immediately and draw power from the battery farm until the generators would engage. The Department maintained a preventive maintenance contract for routine inspection and maintenance of the CCF UPS. Upon review of the inspection reports, we noted the UPS was last tested in January 2012.

Additionally, the Department maintained a preventive maintenance contract for the CCF generators. We reviewed the maintenance reports, noting the generator was inspected in November 2011.

The Communications Building was equipped with a UPS and in the event of a power failure, the UPS would engage immediately and draw power from the battery farm until the generators would engage. The Department maintained a preventive maintenance contract for routine inspection and maintenance of the UPS. Upon review of the inspection reports, we noted the UPS was last tested in October 2011.

The Department maintained a preventive maintenance contract for the Communications Building generators. Upon review of the inspection reports, we noted the generators were last inspected in December 2011.

Resource Access Control Facility (RACF) security software was the primary logical security control to prevent unauthorized actions to mainframe resources.

The common systems user manuals instructed users to contact the CMS Service Desk in the event of processing integrity or security issues.

The fire detection and suppression system at the Communications Building was last tested in 2005.

Criteria: 3.20 – Procedures exist to provide for restoration and disaster recovery consistent with the entity's defined processing integrity policies.

Department's Control: The Department has implemented a comprehensive strategy for backup and restoration. Backup procedures for the Department are documented and include daily backups and a complete backup of the entire week's changes on a weekly basis. The Department is notified of successful or failed backups. Daily and weekly backups are stored offsite. The DCMS/BCCS Infrastructure Services Recovery Activation Plan is documented. The DCMS/BCCS Infrastructure Services Recovery Activation Plan documents the roles and responsibilities of personnel. The agencies document their application recovery classification in the Business Reference Module. Testing is conducted annually. Critical personnel hold current

versions of the various disaster recovery documents. Current versions of the various documents are stored offsite. The common system's disaster recovery procedures provide guidance for the restoration and recovery of the systems.

Test Performed: Reviewed backup schedules, procedures, backup logs, Shift Reports, Remedy tickets, DCMS/BCCS Infrastructure Services Recovery Activation Plan, application listing, contracts, exercise documentation, hotbox inventory, common system user manuals and plans, and interviewed staff.

Test Results: The Department utilized CA-Scheduler to control and schedule backups. All systems were scheduled within CA-Scheduler to be backed up on a routine daily and weekly basis. Once scheduled, the backups ran automatically utilizing a utility within CA-Scheduler to perform the backup dumps.

To document backup jobs scheduled in CA-Scheduler and assist with the verification that backups were successful, the Department maintained and reviewed the CA-Scheduler Verify Backups document. Based on our review, we noted Department staff monitored the completion of the backup process.

The Department did not periodically verify the reliability of backups generated; however, they believed the current process of monitoring backups, the proven capability to restore files when needed, and the successful use of backups to perform disaster recovery testing were sufficient.

We compared the daily and weekly backup schedules detailed in CA-Scheduler Verify Backups document to the daily and weekly schedules defined within CA-Scheduler, noting no exceptions.

In the event a backup did not run successfully, Automation would send a notification to the Command Center, who would in turn notify Enterprise Storage and Backup staff of such issues. The Department would research and rectify the problem, then manually run cleanup jobs until all issues were resolved. Additionally, Department staff notified the user agency, explained the problem, and requested the agency rectify the problem.

We reviewed a sample of daily and weekly backups to ensure they were successful, noting no exceptions. Additionally, we reviewed a sample of daily and weekly backup success/failure logs, noting the Department did not maintain documentation of the corrective action taken.

In addition, Enterprise Storage and Backup staff monitored CA-Scheduler daily for any issues related to the backups.

We reviewed three months of the Shift Reports, noting nine instances affecting backups. The Shift Report indicated the Remedy ticket associated with the issue. We then reviewed the Remedy ticket to ensure corrective action had taken place, noting no exceptions.

The daily backups were maintained onsite, and the weekly backups were rotated to the Regional Vault.

The Department developed the State of Illinois, CMS/BCCS, Recovery Activation Plan (Plan) to provide ‘instructions and actions required when recovering CMS/BCCS computing facilities and services.’ The Plan was limited to the “events affecting CMS/BCCS computing facilities and services” and had a “defined scope of mainframe category 1, stage 0 applications.”

The Plan outlined the task/responsibilities of the various recovery teams. The Plan provided guidance from assessing the damage to obtaining the recovery services provider services.

The Plan stated the first 72 hours of an outage would be limited to the restoration of Stage 0, Category One (Human Safety) applications; along with applications and services added at the time of disaster.

In order to determine the Stage 0, Category One applications which were to be recovered, user agencies were to classify their applicable applications within the Business Reference Model. We reviewed the critical applications in the Business Reference Model, noting four agencies had deemed 13 applications as Stage 0, Category One.

The Department had a contract with an out of state disaster recovery service provider to provide recovery services in the event of a major regional disaster with prolonged outages.

According to the contract, the vendor would be required to provide mainframe recovery services, resources, personnel, and other services in order to continue the required processing capabilities.

The contract was set expire on June 30, 2012; however, the Department had an option to renew if the alternate data center was not equipped and ready. According to Department staff, the Department will not be renewing the contract for recovery purposes at June 30, 2012. The Department will be conducting recovery operations at the alternate data center.

In September 2011, the Department conducted testing of its computing facility, mainframe services, and the disaster recovery plans at the disaster recovery service provider data processing facility.

Our review of exercise documentation indicated four agencies, including the Department, participated in the exercise and tested the recovery of thirteen Stage 0, Category One applications.

Our review of the testing documentation indicated the overall test “went off well”. The documentation indicated problems were encountered; however, problems were addressed as testing progressed. The documentation consisted of application and system requirements, recovery scripts, and post-exercise reviews. However, our review of the detailed documentation noted several of the documents were incomplete.

The Activation Plan states “All critical data backups, media, and recovery documentation must be stored at an official CMS vault location.” The Activation Plan contained a listing of documents (hardcopy and electronic) which are to be maintained offsite.

During our review, we reviewed the contents of the Department's "hotbox" maintained at the Regional Vault. The "hotbox" contained recovery documentation as outlined in Activation Plan. Additionally, per discussion with the Recovery Services Manager, a CD of the recovery documentation was provided to the Recovery Management Team Chair, Co-Chair, and the Recovery Services Manager. The individuals maintained the CD at their respective residents.

In the event of an emergency, Central Payroll would submit to the Comptroller the last correct version of the payroll file for payment. User agencies were responsible for supplying the last correct version of the hardcopy voucher to allow the Office of the Comptroller to produce a warrant for that agency. User agencies were responsible for retaining the hardcopy payroll voucher for the three most current pay periods.

The Business Continuity Plan for CTAS, dated December 31, 2011, provided recovery scripts for the restoration of CTAS.

The Financial Applications Disaster Recovery Plan provided for disaster recovery of financial systems (AIS) in accordance with the Department's overall recovery plan. The Financial Applications Disaster Recovery Plan was comprised of two parts: Financial Systems Disaster Testing and Financial Systems Disaster Plan.

The Financial Systems Disaster Testing plan was to be reviewed annually to verify backup and restore components were still current and functional. The Financial Systems Disaster plan defined the detailed course of action in testing for the disaster, identified team individuals and their responsibilities, identified software, hardware, storage and any other resources needed for the financial systems.

The Department conducted testing in September 2011, which was indicated as successful.

The CIS Disaster Recovery Plan directed actions, identified responsibilities, and provided a detailed approach to resume processing following a disaster. The Plan stated testing was to be conducted twice a year; however, testing had not been conducted during the review period.

Disaster recovery testing had not been conducted as outlined in the CIS Disaster Recovery Plan. Additionally, the Department did not maintain documentation of the corrective action taken on failed backups.

Criteria: 3.21 – Procedures exist to provide for the completeness, accuracy, and timeliness of backup data and systems.

Department's Control: Backups are performed in accordance with the Department's defined backup strategy. Backups of systems and data are stored offsite at the facilities of a third party service provider.

Test Performed: Reviewed backup logs, procedures, backup schedules, backups maintained at the CCF and at the off-site storage location, inventory reports, and interviewed staff.

Test Results: The Department utilized CA-Scheduler to control and schedule backups. All systems were scheduled within CA-Scheduler to be backed up on a routine daily and weekly basis. Once scheduled, the backups ran automatically utilizing a utility within CA-Scheduler to perform the backup dumps.

To document backup jobs scheduled in CA-Scheduler and assist with the verification that backups were successful, the Department maintained and reviewed the CA-Scheduler Verify Backups document. Based on our review, we noted Department staff monitored the completion of the backup process.

Automated software was utilized to control and track media. Reports were utilized to inventory media in order to maintain current inventories.

The Department did not periodically verify the reliability of backups generated; however, they believed the current process of monitoring backups, the proven capability to restore files when needed, and the successful use of backups to perform disaster recovery testing were sufficient.

The Department utilized various reports for inventorying tape media. The Department conducted inventories in June and November 2011 and May 2012 of tape media. According to the May 2012 inventory, there were 37 discrepancies noted. The Department has subsequently conducted additional investigation, resulting in one remaining discrepancy.

Backups of the common systems were maintained at the CCF or the offsite storage location. We reviewed 18 common systems tapes to ensure they were properly located at the CCF or the offsite storage location, noting no exceptions.

In addition, we reviewed 30 tapes, which were to be located at the CCF or the offsite storage facility, noting all tapes were located appropriately and had a unique tracking alpha numeric identification number.

One discrepancy was noted in the May 2012 inventory of tape media.

**4.0 – Monitoring: The entity monitors the system and takes action to maintain compliance with the defined system processing integrity policies.**

Criteria: 4.1 – System processing integrity and security performance are periodically reviewed and compared with the defined system processing integrity and related security policies.

Department's Control: The Department utilizes various tools to review and assess the infrastructure and vulnerabilities. The Department reviews the violations and takes necessary action.

Test Performed: Reviewed the DP Guide, Daily Shift Reports, Shift Change Checklists, Remedy Tickets, standards, templates, device configurations, network diagrams, reports, authentication servers, spreadsheets, SolarWinds, observed monitoring tools, and interviewed staff.

Test Results: The Department utilized various tools to review and assess the infrastructure, system capacity and performance. The Department reviewed performance within their respective functional areas utilizing various tools.

The Department's System Software Support staff maintained a system configuration for the four mainframe computers and the alternate data center. The configuration identified the logical partitions, the location, mode, operating system and version, memory allocation, primary function, environment, and the primary user agencies assigned to each logical system. To assist the Department in assuring system availability and security performance, the Department's security administration staff maintained security software, security authorization lists, and periodically reviewed security violation reports.

To assist with assuring system capacity and availability of system resources were reasonable, the Department's System Software Support staff monitored system capacity and system downtime using available software tools including Resource Measurement Facility (RMF) for monitoring system capacity and Tivoli Directory Server (TDS) for monitoring system availability. An excel spreadsheet containing the history of system capacity measures for each logical system within each computer was maintained. With regards to system availability, TDS reports are maintained and emailed to System Support staff and Department management each Monday indicating the availability of each system. A summary of downtime by system is also maintained and forwarded to management for review.

To assist in the configuration and deployment of network infrastructure managed and maintained by Network Services and LAN Services, various standards and templates were maintained. However, we noted the standards and templates maintained by Network Services addressed routers at the core, distribution, and access levels and did not address the other routers and firewalls they maintained. Upon review, we noted baseline configurations outlined in the documents provided for authentication servers, logging servers, and banners prohibiting unauthorized access and warning of prosecution.

Department management indicated periodic reviews of configurations were performed; however, documentation of these reviews was not maintained. Upon review of the configurations for compliance with the standards and templates, we noted all devices reviewed, which the standards and templates applied to, utilized authentication servers, logging servers, and banners as outlined in documents.

Additionally, to keep the network aligned with Cisco's best practices and recommendations, Cisco periodically performed reviews and provided Network Services with a report. The last report, titled Best Practices Configuration Analysis Report, was prepared and provided to Network Services in December 2011.

Upon review of the Report and discussion with Department staff, the Report addressed only the segment of the network managed and maintained by Network Services Network Operations team. The Report outlined two devices (of 150 reviewed) with High Risk Security exceptions. The Report also made recommendations regarding hardware and software upgrade needs; as well as, configuration enhancements to increase network security, efficiency, and redundancy.

According to Department management, due to other ongoing projects, resources have not been available to permit Network Services to review and take corrective actions; however, as resources permit the report would be reviewed and evaluated.

Authentication servers were utilized to provide authorized access to the firewalls, routers, and switches maintained by Network Services and LAN Services.

Department management indicated user access defined in the Network Services authentication servers was periodically reviewed; however, documentation of the reviews was not maintained.

The LAN Equipment Access Rights Standard indicated quarterly reviews of access rights were to be performed by LAN Services for networking devices they maintained. Department management indicated user access defined in the LAN Services authentication servers was periodically reviewed. Although documentation of the reviews was not maintained, if the review resulted in access rights which required modification/revocation, an Access Request Form was to be completed.

Network Services had configured three servers to function as the primary logging servers for the firewalls, routers, and switches it maintained. According to Department staff, we noted log files on the logging servers utilized by Network Services were not typically reviewed in a proactive manner for potential incidents. Typically, log files located on these servers were utilized for error identification and resolution purposes.

LAN Services had configured two servers to function as the primary logging servers for the firewalls, routers, and switches it maintained. To monitor the log files for potential issues, LAN Services had assigned an individual the responsibility of proactively reviewing logs daily for select devices. These reviews, as well as any issues noted, were tracked in a spreadsheet. Any issues identified were referred to LAN Services Data Center Team for further review.

In addition Network Services and LAN Services had implemented controls to allow them to monitor failed access attempts to networking devices.

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

LAN Services also placed reliance on vulnerability assessment work performed by the Technical Safeguard Team. As Technical Safeguards performed assessments for the various agencies supported by the Department, they would identify weaknesses such as open ports, open snmp strings, weak passwords, etc. Once notified by Technical Safeguards, LAN Services would take action as necessary.

The Department utilized various tools to monitor the IT infrastructure and related events. These monitoring tools were visually monitored by the Operations Center Staff 24 hours a day, 7 days a week.

The Daily Shift Reports recorded activities which occurred on each shift. We reviewed Daily Shift Reports for the weeks of October 24<sup>th</sup> 2011, December 12<sup>th</sup> 2011, January 16<sup>th</sup> 2012 and February 20<sup>th</sup> 2012, noting they appeared to be completed appropriately. Additionally, we reviewed 25 problems indicated in the Shift Reports, noting a corresponding Remedy Help Desk ticket.

Shift Change Checklists were utilized to aid in reviewing the status of the various operating systems and applications. The Shift Change Checklists were also utilized to determine if there were problems with systems or applications. We reviewed Shift Change Checklists during October, 2011, noting supervisory review and that they appeared to be appropriately completed.

Reports detailing the networks alignment with Cisco's best practices and recommendations were not reviewed to determine if corrective actions should be taken.

Criteria: 4.2 – There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system processing integrity and related security policies.

Department's Control: Logs are analyzed either manually or by automated tools to identify trends that may have the potential to impact the Department's ability to achieve system security objectives. Security issues are addressed with management at various meetings.

Test Performed: Reviewed Mainframe Security Procedures, violation reports, monitoring reports, SolarWinds, and interviewed staff.

Test Results: The Department utilized various tools to review and assess the infrastructure, system capacity and performance. The Department reviewed performance within their respective functional areas utilizing various tools. Although, the Department had established and maintained various reports for monitoring purposes, they did not formally document their reviews.

The Department utilized the Resource Measurement Facility software for monitoring system capacity. Monitoring reports were reviewed for statistical performance and capacity statuses.

In addition, system capacity and availability were routinely reviewed by system software support staff. On March 19, 2012, system availability was 100% on all systems, and capacity was an average 76% on the four computers.

A technical staff member outlined methods used to identify security issues during interviews. However, the methods and outcomes were not documented.

In addition, security issues were to be addressed at the monthly management meetings. We reviewed the meeting agendas, noting security issues were discussed.



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

LAN Services also placed reliance on vulnerability assessment work performed by the Technical Safeguard Team. As Technical Safeguards performed assessments for the various agencies supported by the Department, they would identify weaknesses such as open ports, open snmp strings, weak passwords, etc. Once notified by Technical Safeguards, LAN Services would take action as necessary.

The methods used to identify security issues and the outcomes of the reviews were not documented.

Criteria: 4.3 – Environmental, regulatory, and technological changes are monitored, their impact on system processing integrity and security is assessed on a timely basis, and policies are updated for that assessment.

Department's Control: Department management considers technological developments, and laws and regulations during the planning process. Management conducts meetings with user agencies to determine their future needs.

Test Performed: Reviewed Strategic Priority Initiatives Summary, meeting agendas, and interviewed staff.

Test Results: The Strategic Priority Initiatives Summary documented projects which the Department had identified in order to allow them to stay current on technology changes, regulatory and environmental requirements. The Department had outlined 38 projects which were key to strategic objectives. Each project documented specifics, such as, business drivers (security, privacy), technology drivers (new hardware/software, DR/backup), the ranking/prioritization, desired outcomes, metrics (reductions, system availability/uptime) and timeframe for completion.

The Summary was developed based on input from all levels of management within the Department.

The Department had conducted meeting with agencies to determine their future technological needs.

No deviation noted.

This page intentionally left blank

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

## Department's Corrective Action Plan (Not Examined)

The deficiencies noted in the Auditor's report were considered significant by both the Auditors and Department Management. The Department is taking the following actions to address the noted deficiencies.

The Enterprise Applications and Architecture Division will finalize policies and procedures documenting the change control process over application changes related to common systems. The policy and procedures will document the requirements for a change and the documentation requirements. Additionally, we will ensure all changes are tracked from initiation to implementation.

The Department has informed the employees involved in non-compliance to immediately comply with the policy. There is an active project underway to centralize all password resets covered to the Department's Help Desk. This centralization will help us to ensure that policies and procedures related to these password resets are properly communicated and complied with and to help prevent future non-compliance issues.

The Department has initiated a project to ensure the monitoring and enforcement of compliance with the security policies. The project will begin with a comprehensive review of the policies. Additionally, procedures and guidelines will be developed which will define the roles and responsibilities. These documents will be distributed to the Bureau's division managers and training sessions will be conducted. For policy compliance outside the Bureau, the Department has begun a risk management project that includes Bureaus outside Communications and Computer Services. Policy compliance will be included in that project.

The following are the actions taken or to be taken by the Department to address the deficiencies noted in the examination report.

<b>Principle</b>	<b>Criteria</b>	<b>Corrective Action Plan</b>
Security	1.1	The Bureau will review policies at a monthly meeting on security issues, and update as appropriate.
	1.2 E	The Department will add the ESR process for requesting access rights to the policies and the details in the related procedures.
	1.2 H	The Change Policy will be updated to outline the requirements and procedures will be developed to meet the policy requirements.
	1.2 I	The Bureau has an active project underway to solidify the processes for the handling of security issues reported by users.
	1.2 J	The Bureau has an active project underway to solidify the processes for the handling of security issues reported by users.
	1.2 M	The Bureau has a project to establish terms of services agreements.
	2.2	All Bureau staff completed the training during the review period. We will work with Department management to emphasize the importance of other staff also completing the training.

	2.4	The Bureau has an active project underway to solidify the processes for the handling of security issues reported by users, including an appropriate escalation procedure for the handling of security breaches and incidents
	3.1	The Department is progressing on developing an Enterprise Risk Management Program that will include all bureaus in the Department and all systems for which the department is responsible.
	3.2 B	The active ID for a retired employee has now been deactivated.
	3.2 C	The Department will develop procedures for granting access to staff and will ensure documentation is maintained.
	3.2 D	The Department will add the submission through ESR to the procedures. Additionally, the Department will add the ESR process for requesting access rights to the policies and the details in the related procedures. The Bureau will review and remove powerful access ID's in a timelier basis.
	3.2 G	The Bureau will review and remove powerful access ID's in a timelier basis.
	3.3	The Bureau will work with its managers and the Bureau of Facilities Management to ensure the ID badge request process is properly followed. We are in the process of investigating the missing keys and will develop a process to manage key distribution and retrieval.
	3.4	The Bureau will review and remove powerful access ID's in a timelier basis.
	3.5	The Bureau will review and remove powerful access ID's in a timelier basis.
	3.7	The Bureau has an active project underway to solidify the processes for the handling of security issues reported by users, including an appropriate escalation procedure for the handling of security breaches and incidents. The Department will work to insure that all device configurations are updated as necessary to insure that they are utilizing the logging servers.
	3.8	The Department now has classified all of its data.
	3.9	The Department has initiated a project to ensure the monitoring and enforcement of compliance with the security policies. The project will begin with a comprehensive review of the policies. Additionally, procedures and guidelines will be developed which will define the roles and responsibilities. These documents will be distributed to the Bureau's division managers and training sessions will be conducted. For policy compliance outside the Bureau, the Department has begun a risk management project that includes Bureaus outside Communications and Computer Services. Policy compliance will be included in that project.
	3.11	The Department will continue to emphasize the importance of performing performance evaluations in a timely manner.

	3.13	The Change Guide will be updated to document when back out, testing, and implementation plans are required and documentation requirements for each.
	3.14	The Change Guide will be updated to document when implementation plans are required and the documentation requirements.
	4.1	As staffing resources allow, the Bureau will continue to attempt to align with the Cisco best practices report.
	4.2	LAN services will document remediation of issues found by the Technical Safeguards group during consolidated agency vulnerability assessments.
Availability	1.1	The Bureau will review policies at a monthly meeting on security issues, and update as appropriate.
	1.2 E	The Department will add the ESR process for requesting access rights to the policies and the details in the related procedures.
	1.2 H	The Change Policy will be updated to outline the requirements and procedures will be developed to meet the policy requirements.
	1.2 I	The Bureau has an active project underway to solidify the processes for the handling of availability and security issues reported by users.
	1.2 J	The Change Policy will be updated to outline the requirements and procedures will be developed to meet the policy requirements.
	1.2 M	The Bureau has a project to establish terms of services agreements.
	1.2 N	The Bureau has a project to establish terms of services agreements.
	1.2 O	The Bureau will continue to monitor system capacity and develop documentation to outline the policies and procedures.
	2.2	All Bureau staff completed the training during the review period. We will work with Department management to emphasize the importance of other staff also completing the training.
	2.4	The Bureau has an active project underway to solidify the processes for the handling of security issues reported by users, including an appropriate escalation procedure for the handling of security breaches and incidents
	3.1	The Department is progressing on developing an Enterprise Risk Management Program that will include all bureaus in the Department and all systems for which the department is responsible.
	3.2	The Department has determined the end-of-life equipment is not of a critical nature and spares have been procured for failures. This equipment will be replaced as funds and staff becomes available.
	3.3	The Bureau has plans to replace older equipment that is not currently backed up. Based on an analysis, we do not believe this equipment is critical.
	3.4	The Bureau will review its processes for the handling of tapes.
	3.5 A	The Bureau will review and remove powerful access ID's in a timelier basis.
	3.5 B	The active ID for a retired employee has now been deactivated.

	3.2 C	The Department will develop procedures for granting access to staff and will ensure documentation is maintained.
	3.5 D	The Department will add the submission through ESR to the procedures. Additionally, the Department will add the ESR process for requesting access rights to the policies and the details in the related procedures. The Bureau will review and remove powerful access ID's in a timelier basis.
	3.5 F	The Bureau will review and remove powerful access ID's in a timelier basis.
	3.6	The Bureau will work with its managers and the Bureau of Facilities Management to ensure the ID badge request process is properly followed. We are in the process of investigating the missing keys and will develop a process to manage key distribution and retrieval.
	3.7	The Bureau will review and remove powerful access ID's in a timelier basis.
	3.8	The Bureau will review and remove powerful access ID's in a timelier basis.
	3.10	The Bureau has an active project underway to solidify the processes for the handling of security issues reported by users, including an appropriate escalation procedure for the handling of security breaches and incidents
	3.11	The Department now has classified all of its data.
	3.12	The Department has initiated a project to ensure the monitoring and enforcement of compliance with the security policies. The project will begin with a comprehensive review of the policies. Additionally, procedures and guidelines will be developed which will define the roles and responsibilities. These documents will be distributed to the Bureau's division managers and training sessions will be conducted. For policy compliance outside the Bureau, the Department has begun a risk management project that includes Bureaus outside Communications and Computer Services. Policy compliance will be included in that project.
	3.14	The Department will continue to emphasize the importance of performing performance evaluations in a timely manner.
	3.16	The Change Guide will be updated to document when back out, testing, and implementation plans are required and documentation requirements for each.
	3.17	The Change Guide will be updated to document when implementation plans are required and the documentation requirements.
	4.1	As staffing resources allow, the Bureau will continue to attempt to align with the Cisco best practices report.
	4.2	LAN services will document remediation of issues found by the Technical Safeguards group during consolidated agency vulnerability assessments.

Processing Integrity	1.1	The Bureau will review policies at a monthly meeting on security issues, and update as appropriate.
	1.2 E	The Department will add the ESR process for requesting access rights to the policies and the details in the related procedures.
	1.2 G	The Enterprise Applications and Architecture Division will finalize policies and procedures documenting the change control process over application changes related to common systems. The policy and procedures will document the requirements for a change and the documentation requirements. Additionally, we will ensure all changes are tracked from initiation to implementation.
	1.2 H	The Enterprise Applications and Architecture Division will finalize policies and procedures documenting the change control process over application changes related to common systems. The policy and procedures will document the requirements for a change and the documentation requirements. Additionally, we will ensure all changes are tracked from initiation to implementation.
	1.2 I	The Bureau has an active project underway to solidify the processes for the handling of security issues reported by users.
	1.2 J	The Bureau has an active project underway to solidify the processes for the handling of processing and security issues reported by users.
	1.2 M	The Bureau has a project to establish terms of services agreements.
	2.2	All Bureau staff completed the training during the review period. We will work with Department management to emphasize the importance of other staff also completing the training.
	2.4	The Bureau has an active project underway to solidify the processes for the handling of security issues reported by users, including an appropriate escalation procedure for the handling of security breaches and incidents
	3.1	The Department is progressing on developing an Enterprise Risk Management Program that will include all bureaus in the Department and all systems for which the department is responsible.
	3.3	The Bureau has plans to replace older equipment that is not currently backed up. Based on an analysis, we do not believe this equipment is critical.
	3.6 A	The Bureau will review and remove powerful access ID's in a timelier basis.
	3.6 B	The active ID for a retired employee has now been deactivated.
	3.6 C	The Department will develop procedures for granting access to staff and will ensure documentation is maintained.
	3.6 D	The Department will add the submission through ESR to the procedures. Additionally, the Department will add the ESR process for requesting access rights to the policies and the details in the related procedures. The Bureau will review and remove powerful access ID's in a timelier basis.
	3.6 G	The Bureau will review and remove powerful access ID's in a timelier basis.



	3.7	The Bureau will work with its managers and the Bureau of Facilities Management to ensure the ID badge request process is properly followed. We are in the process of investigating the missing keys and will develop a process to manage key distribution and retrieval.
	3.8	The Bureau will review and remove powerful access ID's in a timelier basis.
	3.9	The Bureau will review and remove powerful access ID's in a timelier basis.
	3.11	The Bureau has an active project underway to solidify the processes for the handling of security issues reported by users, including an appropriate escalation procedure for the handling of security breaches and incidents
	3.12	The Department now has classified all of its data.
	3.13	The Department has initiated a project to ensure the monitoring and enforcement of compliance with the security policies. The project will begin with a comprehensive review of the policies. Additionally, procedures and guidelines will be developed which will define the roles and responsibilities. These documents will be distributed to the Bureau's division managers and training sessions will be conducted. For policy compliance outside the Bureau, the Department has begun a risk management project that includes Bureaus outside Communications and Computer Services. Policy compliance will be included in that project.
	3.14	The Change Guide will be updated to document when back out, testing, and implementation plans are required and documentation requirements for each.
	3.15	The Department will continue to emphasize the importance of performing performance evaluations in a timely manner.
	3.17	The Change Guide will be updated to document when back out, testing, and implementation plans are required and documentation requirements for each.
	3.18	The Change Guide will be updated to document when implementation plans are required and the documentation requirements.
	3.19	Based on our analysis, we do not believe the equipment at the facility is critical enough to warrant the expense of testing the fire suppression system.
	3.20	The Department will review and update the related policy and ensure future compliance.
	3.21	The Bureau will review its processes for the handling of tapes.
	4.1	As staffing resources allow, the Bureau will continue to attempt to align with the Cisco best practices report.
	4.2	LAN services will document remediation of issues found by the Technical Safeguards group during consolidated agency vulnerability assessments.

**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.

<b>Fiscal Year</b>	<b>Number of Separations</b>	<b>Number of Hires</b>	<b>Net Staff Loss</b>
2007	57	39	18
2008	49	12	37
2009	38	23	15
2010	47	9	38
2011	49	7	42
2012*	72	16	56
<b>TOTAL</b>	<b>312</b>	<b>106</b>	<b>206</b>

\*Through 5/31/2012

**Department's Information Related to the New Alternate Data Center  
(Not Examined)**

Beginning July 1, 2012, the Department contracted with an in-state vendor for a “high available alternate data center, failover services, and other services as needed.” The contract will provide floor space, electricity, security and telecommunication services.

**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 Employment Security
12. Department of Financial and Professional Regulation
13. Department of Healthcare and Family Services
14. Department of Human Rights
15. Department of Human Services
16. Department of Insurance
17. Department of Juvenile Justice
18. Department of Labor
19. Department of Lottery
20. Department of Military Affairs
21. Department of Natural Resources
22. Department of Public Health
23. Department of Revenue
24. Department of Transportation
25. Department of Veterans' Affairs
26. Department on Aging
27. East St. Louis Financial Advisory Authority
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 Historic Preservation Agency
49. Illinois Housing Development Authority
50. Illinois Labor Relations Board
51. Illinois Law Enforcement Training and Standards Board
52. Illinois Math and Science Academy

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

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

1. 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 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. Human Rights Commission
22. Illinois Arts Council
23. Illinois Civil Service Commission
24. Illinois Commerce Commission
25. Illinois Community College Board
26. Illinois Council on Developmental Disabilities
27. Illinois Criminal Justice Information Authority
28. Illinois Deaf and Hard of Hearing Commission
29. Illinois Educational Labor Relations Board
30. Illinois Emergency Management Agency
31. Illinois Gaming Board
32. Illinois Historic Preservation Agency
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 Power Agency
37. Illinois Prisoner Review Board
38. Illinois Procurement Policy Board
39. Illinois Racing Board
40. Illinois Student Assistance Commission
41. Illinois Violence Prevention Authority
42. Illinois Workers' Compensation Commission
43. Judges' Retirement System
44. Judicial Inquiry Board
45. Office of Management and Budget
46. Office of the Attorney General
47. Office of the Auditor General
48. Office of the Executive Inspector General
49. Office of the Governor
50. Office of the Lieutenant Governor
51. Office of the State Appellate Defender
52. Office of the State Fire Marshal
53. Property Tax Appeal Board
54. State Board of Elections
55. State Employees' Retirement System
56. State Police Merit Board
57. State Universities Civil Service System
58. Supreme Court of Illinois

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

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

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

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

\* Agency Payroll information entered into the system by  
CPS staff.

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

## ACRONYM GLOSSARY

ACL – Access Control List  
ADC – Alternate Data Center  
AIS – Accounting Information System  
BCCS – Bureau of Communication and Computer Services  
Bureau – Bureau of Communication and Computer Services  
CAC – Change Advisory Committee  
CCF – Central Computer Facility  
CICS – Customer Information Control System  
CIO – Chief Information Officer  
CIRT – Critical Incident Response Team  
CIS – Central Inventory System  
CISO – Chief Information Security Officer  
CMC – Customer Management Center  
CMS – Central Management Services  
CPS – Central Payroll System  
CPU – Central Processing Unit  
CRF – Communications Revolving Fund  
CSC – Communications Solutions Center  
CSC – Customer Service Center  
CSD – CICS System Definition File  
CTAS – Central Time and Attendance  
CTO – Chief Technology Officer  
DASD – Direct Access Storage Device  
DB2 – Database 2  
DCMS – Department of Central Management Services  
Department – Department of Central Management Services  
DNS – Domain Name Service  
DP – Data Processing  
DR – Disaster Recovery  
EAA – Enterprise Application & Architecture  
ECM – Enterprise Change Management  
EoL – End of Life  
EPMO – Enterprise Program Management Office  
ESR – Enterprise Service Request  
FISMA – Federal Information Security Management Act  
FMLA – Family Medical Leave Act  
FY – Fiscal Year  
GRF – General Revenue Fund  
HIPAA – Health Insurance Portability and Accountability Act  
HR – Human Resources  
ICN – Illinois Century Network  
ID – Identification  
ILCS – Illinois Compiled Statutes  
IMS – Information Management System

IT – Information Technology  
ITG – Information Technology Governance  
LAN – Local Area Network  
NCC – Network Control Center  
NCM – Network Configuration Manager  
NIST – National Institute of Standards and Technology  
NOMAD – Name of application utilized by z/VM  
NPM – Network Performance Module (alt. Manager)  
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  
SSRF – Statistical Services Revolving Fund  
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