STATE OF ILLINOIS
DEPARTMENT OF INNOVATION AND TECHNOLOGY

INFORMATION TECHNOLOGY SHARED SERVICES

REPORT ON THE DESCRIPTION OF SYSTEM, SUITABILITY OF DESIGN,
AND OPERATING EFFECTIVENESS OF CONTROLS
FOR THE PERIOD
JULY 1, 2019 THROUGH JUNE 30, 2020

STATE OF ILLINOIS

DEPARTMENT OF INNOVATION AND TECHNOLOGY

TABLE OF CONTENTS

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

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

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

OFFICE OF THE AUDITOR GENERAL
FRANK J. MAUTINO

INDEPENDENT SERVICE AUDITOR'S REPORT ON THE STATE OF ILLINOIS, DEPARTMENT OF INNOVATION AND TECHNOLOGY'S DESCRIPTION OF ITS INFORMATION TECHNOLOGY SHARED SERVICES SYSTEM AND SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

Honorable Frank J. Mautino
Auditor General, State of Illinois

Scope

We have examined the State of Illinois, Department of Innovation and Technology's description of its information technology general controls and application controls that support its Information Technology Shared Services system of which are included in the "Description of the Information Technology Shared Services for the Information Technology General Controls and Application Controls" for the user entities throughout the period from July 1, 2019 to June 30, 2020, (description) and the suitability of the design and operating effectiveness of the State of Illinois, Department of Innovation and Technology's controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in the State of Illinois, Department of Innovation and Technology's assertion. The controls and control objectives included in the description are those that management of the State of Illinois, Department of Innovation and Technology believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Information Technology Shared Services system that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the State of Illinois, Department of Innovation and Technology's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The State of Illinois, Department of Innovation and Technology uses the Department of Central Management Services, a subservice organization to provide building maintenance activities; Zayo Group, LLC, a subservice organization to provide an alternate data center for off-site storage and replication of the production environment; Microsoft, LLC, a subservice organization to provide cloud hosting services; BMC Software, Inc., a subservice organization to provide software as a service; NIC, Inc., a subservice organization to provide software as a service; Google Cloud, a subservice organization to provide a web-based solution; Micro Focus, a

subservice organization to provide project and portfolio management tools; and Salesforce, a subservice organization to provide hosting services and software as a service. The description includes only the control objectives and related controls of the State of Illinois, Department of Innovation and Technology and excludes the control objectives and related controls of the Department of Central Management Services, Zayo Group, LLC, Microsoft, LLC, BMC Software, Inc., NIC, Inc., Google Cloud, Micro Focus, and Salesforce. The description also indicates that certain control objectives specified by the State of Illinois, Department of Innovation and Technology can be achieved only if complementary subservice organization controls assumed in the design of the State of Illinois, Department of Innovation and Technology's controls are suitably designed and operating effectively, along with the related controls at the State of Illinois, Department of Innovation and Technology. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information about the corrective action plan, business continuity and disaster recovery, and user entity listings in Section V, "Other Information Provided by the State of Illinois, Department of Innovation and Technology," is presented by management of the State of Illinois, Department of Innovation and Technology to provide additional information and is not part of the State of Illinois, Department of Innovation and Technology description of the Information Technology Shared Services system made available to user entities during the period from July 1, 2019 to June 30, 2020. Information about the State of Illinois, Department of Innovation and Technology's corrective action plan, business continuity and disaster recovery, and user entity listings have not been subjected to procedures applied in the examination of the description of the Information Technology Shared Services system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Information Technology Shared Services system and, accordingly, we express no opinion on it.

Service Organization Responsibilities

In Section II, the State of Illinois, Department of Innovation and Technology has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The State of Illinois, Department of Innovation and Technology is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and the standards applicable to attestation engagements contained in *Government Auditing Standards,* issued by the Comptroller General of the United States and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on criteria in management's assertions, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period from July 1, 2019 to June 30, 2020. We believe the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our qualified opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of control involves:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertions;
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- evaluating the overall presentation of the description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service organization in its assertions.

Inherent Limitations

The description is prepared to meet the common needs of the user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each user entity may consider important in its own particular environment. Because of their nature, controls at a service organization or subservice organizations may not prevent, or detect and correct, all misstatements in its information technology general controls and application controls system. 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 achieve the related control objectives, is subject to the risk that controls at a service organization or a subservice organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV.

Basis for Opinion

Our examination disclosed:

1) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services system states on page 46 the State of Illinois, Department of Innovation and Technology did not have controls in place to review access to the Communication Building during the period of July 1, 2019 to December 31, 2019. As a result, we were unable to determine whether controls were suitably designed and operating effectively during the period of July 1, 2019 to December 31, 2019 to achieve the control objective, "Controls provide reasonable assurance that physical security to facilities and data centers is restricted to authorized personnel, that are relevant to user entities' internal control over financial reporting."

2) The accompanying description of the State of Illinois, Department of Innovation and Technology Information Technology Shared Services system states on page 46 the State of Illinois, Department of Innovation and Technology did not have controls in place to review access to the Department's Central Computing Facility (CCF) highly secured area during the period of July 1, 2019 through November 30, 2019. As a result, we were unable to determine whether controls were suitably designed and operating effectively during the period of July 1, 2019 through November 30, 2019 to achieve the control objective, "Controls provide reasonable assurance that physical security to facilities and data centers is restricted to authorized personnel that are relevant to user entities' internal control over financial reporting."

3) The State of Illinois, Department of Innovation and Technology states in its description that it has controls in place to require access modifications to the State of Illinois, Department of Innovation and Technology's resources begin with the submission of a Remedy service request from an authorized ATSR or Department IT Coordinator. However, as noted at page 64 of the description of tests of controls and results, a population of access modifications to the State of Illinois, Department of Innovation and Technology's resources could not be provided. As a result, controls were not operating effectively to achieve the control objective, "Controls provide reasonable assurance that logical access to applications, data, and the environment is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions that are relevant to user entities' internal control over financial reporting."

4) The State of Illinois, Department of Innovation and Technology states in its description that it has controls in place to require access revocation to the State of Illinois, Department of Innovation and Technology's resources be initiated upon receipt of a Remedy service request, or under special or emergency circumstances, by instruction of senior management. However, as noted at page 64 of the description of tests of controls and results, documentation of the timely termination of an individual's access to the State of Illinois, Department of Innovation and Technology's resources could not be provided. As a result, controls were not operating effectively to achieve the control objective, "Controls provide reasonable assurance that logical access to applications, data, and the environment is restricted to authorized and appropriate users and such users are restricted

to performing authorized and appropriate actions that are relevant to user entities' internal control over financial reporting."

5) The State of Illinois, Department of Innovation and Technology states in its description that it has controls in place to require an approved DoIT Badge Request form in order to obtain access to the Communication Building and the CCF. However, as noted at page 95 of the description of tests of controls and results, a listing of individuals authorized to approve the DoIT Badge Request form could not be provided. As a result, controls were not operating effectively to achieve the control objective, "Control provide reasonable assurance that physical access to facilities and data centers is restricted to authorized personnel, that are relevant to user entities' internal control over financial reporting."

6) The State of Illinois, Department of Innovation and Technology states in its description that physical access is deactivated after official notice of separation or termination. However, as noted at page 96 of the description of tests of controls and results, documentation demonstrating the terminated individual's access badge was deactivated could not be provided. As a result, controls were not operating effectively to achieve the control objective, "Control provide reasonable assurance that physical access to facilities and data centers is restricted to authorized personnel, that are relevant to user entities' internal control over financial reporting."

7) As indicated in the accompanying description of the State of Illinois, Department of Innovation and Technology, ethics training was not conducted during the examination period; therefore, we did not perform any test of design or operating effectiveness of controls related to the control objective, "Controls provide reasonable assurance that policies and procedures related to employee responsibilities and hiring have been established, new employees and contractors are screened and on-boarded, and a defined organizational structure exists, that are relevant to user entities' internal control over financial reporting."

8) As indicated in the accompanying description of the State of Illinois, Department of Innovation and Technology, the Department did not report stolen or missing laptops which were not encrypted during the examination period; therefore, we did not perform any test of design or operating effectiveness of controls related to the control objective, "Controls provide reasonable assurance the entities' calls that are relevant to user entities' internal control over financial reporting are responded to, tracked, and resolved in a timely manner."

9) As indicated in the accompanying description of the State of Illinois, Department of Innovation and Technology, the Department did not have a request for a new system administrator during the examination period; therefore, we did not perform any test of design or operating effectiveness of controls related to the control objective, "Controls provide reasonable assurance that logical access to applications, data, and the environment is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions that are relevant to user entities' internal control over financial reporting."

10) As indicated in the accompanying description of the State of Illinois, Department of Innovation and Technology, the Department did not encounter failed backups during the examination period; therefore, we did not perform any test of design or operating effectiveness of controls related to the control objective, "Controls provide reasonable assurance that applications, data, and the environment is backed up and stored offsite that are relevant to user entities' internal control over financial reporting."

In our opinion, except for the matters referred to in the preceding paragraphs, in all material respects, based on the criteria described in the State of Illinois, Department of Innovation and Technology's assertion:

a. the description fairly presents the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services system that was designed and implemented throughout the period from July 1, 2019 to June 30, 2020.

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period from July 1, 2019, to June 30, 2020; and subservice organizations and user entities applied complementary controls assumed in the design of the State of Illinois, Department of Innovation and Technology's control throughout the period July 1, 2019 to June 30, 2020.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period from July 1, 2019 to June 30, 2020 if complementary subservice organization and user entity controls assumed in the design of the State of Illinois, Department of Innovation and Technology's controls operated effectively throughout the period July 1, 2019 to June 30, 2020.

Emphasis of Matter

As noted in the Description of the Information Technology Shared Services for the Information Technology General Controls and Application Controls, effective March 21, 2020, the Governor of the State of Illinois signed Executive Order 2020-10 requiring all individuals currently living within the State of Illinois to stay at home or at their place of residence, as a result of the global pandemic related to the COVID-19 outbreak. The Description of the Information Technology Shared Services for the Information Technology General Controls and Application Controls documents the changes to the Department's internal controls due to the requirements of Executive Order 2020-10.

The opinion was not modified as a result of this matter.

Other Reporting Required by Government Auditing Standards

In accordance with *Government Auditing Standards*, we have also issued our report dated August 5, 2020, on our consideration of the State of Illinois, Department of Innovation and Technology's internal control over (1) fairly presenting the State of Illinois, Department of Innovation and Technology's description of its Information Technology Shared Services system throughout the

period July 1, 2019 to June 30, 2020, and (2) establishing and maintaining effective internal control over the suitable design and operating effectiveness of the controls related to the control objectives within the State of Illinois, Department of Innovation and Technology's description of its Information Technology Shared Services system throughout the period July 1, 2019 to June 30, 2020 (internal control over reporting), and on our tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, and other matters, limited to the scope of this report. The purpose of that report is solely to describe the scope of our testing of internal control over reporting and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the State of Illinois, Department of Innovation and Technology's internal control over reporting or on compliance. That report is an integral part of an examination performed in accordance with *Government Auditing Standards* in considering the State of Illinois, Department of Innovation and Technology's internal control over reporting and compliance.

Restricted Use

This report is intended solely for the information and use of the State of Illinois, Department of Innovation and Technology, user entities of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services system during some or all of the period from July 1, 2019 to June 30, 2020, and their auditors who audit and report on such user entities' financial statements or internal controls over financial reporting and have sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

SIGNED ORIGINAL ON FILE
Jane Clark, CPA
Director of Financial and Compliance Audits

SIGNED ORIGINAL ON FILE
Mary Kathryn Lovejoy, CPA, CISA
Principal of IS Audits

August 5, 2020
Springfield, Illinois

SECTION II

DEPARTMENT OF INNOVATION AND TECHNOLOGY'S ASSERTION REGARDING THE INFORMATION TECHNOLOGY SHARED SERVICES SYSTEM

Honorable Frank J. Mautino
Auditor General, State of Illinois

We have prepared the description of the "Information Technology Shared Services system for the Information Technology General Controls and Application Controls" for the information technology general controls and application controls throughout the period from July 1, 2019, to June 30, 2020, (description) for user entities of the system during some or all of the period from July 1, 2019, to June 30, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves when assessing the risks of material misstatements of user entities' financial statements.

The State of Illinois, Department of Innovation and Technology uses subservice organizations to provide building maintenance activities, an alternate data center for off-site storage and replication of the production environment, cloud hosting services, software as a service, and a web-based solution. The description includes only the control objectives and related controls of the State of Illinois, Department of Innovation and Technology and excludes the control objectives and related controls of the subservice organizations. The description also indicated that certain control objectives specified in the description can only be achieved if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the State of Illinois, Department of Innovation and Technology's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

1) The description fairly presents the Information Technology Shared Services system made available to user entities of the system during some or all of the period July 1, 2019, to June 30, 2020, for the information technology general controls and application controls as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

    a) Presents how the system made available to user entities of the system was designed and implemented to provide the information technology general controls and application controls, including, if applicable:

i) The types of services provided, including, as appropriate, the information technology general controls and application controls.
ii) How the system captures and addresses significant events and conditions.
iii) The services performed by the subservice organizations, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
iv) The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the controls.
v) Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

b) Includes relevant details of changes to the State of Illinois, Department of Innovation and Technology's system during the period covered by the description.

c) Does not omit or distort information relevant to the system, while acknowledging that the description is prepared to meet the common needs of the user entities of the system and their user auditors, and may not, therefore, include every aspect of the Information Technology Shared Services system that each individual user entity of the system and its auditor may consider important in its own particular environment.

2) Except for the matters described in paragraph 3, the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period from July 1, 2019 to June 30, 2020 to achieve those control objectives if user entities applied the complementary user entity controls assumed in the design of the State of Illinois, Department of Innovation and Technology's controls throughout the period from July 1, 2019 to June 30, 2020. The criteria we used in making this assertion were that:

a) The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the State of Illinois, Department of Innovation and Technology;

b) The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and,

c) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

3) Description of Deficiencies in Fair Presentation, Suitability of Design, or Operating Effectiveness.

1) We stated on page 46 of the description that controls were not in place to review access to the Communication Building during the period of July 1, 2019 to December 31, 2019. As a result, controls were not suitably designed and operating effectively during the period of July 1, 2019 to December 31, 2019 to achieve the control objective, "Controls provide reasonable assurance that physical security to facilities and data centers is

restricted to authorized personnel, that are relevant to user entities' internal control over financial reporting."

2) We stated on page 46 that controls were not in place to review access to the Department's Central Computing Facility (CCF) highly secured area during the period of July 1, 2019 to November 30, 2019. As a result, controls were not suitably designed and operating effectively during the period of July 1, 2019 to November 30, 2019 to achieve the control objective, "Controls provide reasonable assurance that physical security to facilities and data centers is restricted to authorized personnel, that are relevant to user entities' internal control over financial reporting."

3) We stated on page 34 of the description that controls are in place to require access modifications to the State of Illinois, Department of Innovation and Technology's resources begin with the submission of a Remedy service request from an authorized Agency Technology Service Requester or Department IT Coordinator. However, we were unable to provide a population of access modifications to the State of Illinois, Department of Innovation and Technology's resources. As a result, controls were not operating effectively to achieve the control objective, "Controls provide reasonable assurance that logical access to applications, data, and the environment is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions that are relevant to user entities' internal control over financial reporting."

4) We stated on page 34 of the description that controls are in place to require access revocation to the State of Illinois, Department of Innovation and Technology's resources be initiated upon receipt of a Remedy service request, or under special or emergency circumstances, by instruction of senior management. However, we were unable to provide documentation of the timely termination of an individual's access to the State of Illinois, Department of Innovation and Technology's resources. As a result, controls were not operating effectively to achieve the control objective, "Controls provide reasonable assurance that logical access to applications, data, and the environment is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions that are relevant to user entities' internal control over financial reporting."

5) We stated on page 46 of the description that controls are in place to require an approved DoIT Badge Request form in order to obtain access to the Communication Building and the CCF. However, we were unable to provide a listing of individuals authorized to approve the DoIT Badge Request form. As a result, controls were not operating effectively to achieve the control objective, "Control provide reasonable assurance that physical access to facilities and data centers is restricted to authorized personnel, that are relevant to user entities' internal control over financial reporting."

6) We stated on page 47 of the description that controls are in place to deactivate physical access after official notice of separation or termination. However, we were unable to provide documentation demonstrating the terminated individual's access badge was deactivate. As a result, controls were not operating effectively to achieve the control objective, "Control provide reasonable assurance that physical access to facilities and data

centers is restricted to authorized personnel, that are relevant to user entities' internal control over financial reporting."

4) Description of Controls for Which There Is No Population to Test

During the period July 1, 2019 through June 30, 2020, the Department did not conduct ethics training, report stolen and missing laptops which were not encrypted, did not encounter failed backups, and did not have a request for new system administrator.

SIGNED ORIGINAL ON FILE

Ron Guerrier
Secretary
Department of Innovation and Technology
August 5, 2020

SECTION III

DESCRIPTION OF THE INFORMATION TECHNOLOGY SHARED SERVICES FOR THE INFORMATION TECHNOLOGY GENERAL CONTROLS AND APPLICATION CONTROLS

Description of the Information Technology Shared Services for the Information Technology General Controls and Application Controls

Overview of the Department of Innovation and Technology

The Department of Innovation and Technology (DoIT, the Department) was initially created under Executive Order 2016-01, and the Department of Innovation and Technology Act (Act) (20 ILCS 1370). As stated in Section 1-15 of the Act, the powers and duties of the Department are to "promote best-in-class innovation and technology to client agencies to foster collaboration among client agencies, empower client agencies to provide better service to residents of Illinois, and maximize the value of taxpayer resources."

Subservice Organizations

The Department utilizes the following subservice providers:

- The Department of Central Management Services (DCMS) provides building maintenance activities of Department occupied facilities;
- BMC Software, Inc. provides hosting services for the Department's service management tool, Remedy On Demand;
- Google Cloud provides a web-based solution (as of April 20, 2020);
- Microsoft LLC provides cloud hosting services;
- Micro Focus provides a project and portfolio management tool;
- NIC, Inc provides hosting services and a web-based Statewide Permits and Licensing Solution;
- Salesforce provides hosting services and a web-based solution (as of March 28, 2020); and
- Zayo Group LLC provides an alternate data center for off-site data storage and replication of the production environment.

Overview of Services Provided

As cited in the Act, the Department is responsible for "information technology functions on behalf of client agencies" with specific services related to:

- management of the procurement, retention, installation, maintenance, and operation of information technology (IT) used by client agencies;
- security protection, privacy of IT information as provided by law, and back-up facilities; and
- installation and operation of IT systems.

Scope of the Description

In accordance with the criteria in management's assertion, this Description includes a description of the Department's Information Technology (IT) General Controls and Application Controls provided to agencies. The Description excludes the control objectives and related controls of the Department of Central Management Services, BMC Software Inc., Google Cloud, Microsoft LLC, Micro Focus, NIC Inc, Salesforce, and Zayo Group LLC.

The Description is intended to provide information for the agencies and their independent auditors to understand the systems and controls in place for the Department's IT General Controls and Application Controls that are relevant to an agency's internal control over financial

reporting.

The Description covers information technology general controls and specific application controls related to:

- Accounting Information System (AIS);
- Central Inventory System (CIS);
- Central Payroll System (CPS);
- Central Time and Attendance System (CTAS); and
- eTime.

Internal Control Framework

This section provides information about the five interrelated components of internal control at the Department, including the Department's:

- Control environment;
- Risk Assessment;
- Information and Communication;
- Control Activities; and
- Monitoring.

Control Environment

Organizational Structure

The Department's organizational hierarchy supports internal control starting with the Department's Secretary. The Secretary is a member of the Governor's Cabinet and is the "Chief Information Officer for the State and the steward of State data with respect to those agencies under the jurisdiction of the Governor" per Section 1-30 of 20 ILCS 1370. During the examination period, one individual serves as Acting Secretary.

The Acting Assistant Secretary (vacant from July 1, 2019 to February 9, 2020) directly supervises the DoIT Group CIOs and applies primary focus on application development and technology delivery.

The Department's organizational hierarchy promotes separation of duties, monitoring of controls, and customer support through staff positions of: Affirmative Action/Equal Employment Opportunity Officer, Chief Administrative Officer, Chief Internal Auditor, Chief Information Security Officer, Chief Service Officer, Chief of Staff, Chief Enterprise Architect, Chief Technology Officer, Chief Data Officer, ERP Program Director, and seven Chief Information Officers (CIOs) grouped into service delivery taxonomies.

The Affirmative Action/Equal Employment Opportunity Officer serves as an advisor and consultant to the Department on issues, policies, guidelines, and standards related to affirmative action and equal employment opportunity activities. The position also participates in recruitment, investigates discrimination, and serves as the Department's coordinator for the Americans with Disabilities Act.

The Chief Administrative Officer (vacant from March 2, 2020 to present) consults with the Secretary and senior management to facilitate functional compatibility and alignment of Department objectives. Subordinate managers oversee the Department's Legal Services, Human

Resources, and Procurement. From July 1 to July 15, 2019, Property Control function and staff reported to the Chief Customer Officer. Effective July 16, 2019, and approved by CMS on October 1, 2019, Property Control function and staff were moved organizationally from the Chief Customer Officer to report to the Chief Administrative Officer.

The Chief Internal Auditor directs and manages the Department's internal audit program which validates compliance with the Fiscal Control and Internal Audit Act and verifies consistency with the Department's mission, program objectives, and regulatory statutes. In addition, internal audit operations identify and evaluate significant risk exposures and contribute to the improvement of the Department's overall control environment.

The Chief Information Security Officer (CISO) is responsible for strategies, policies, standards, processes, and assessments that promote protection over the Department's assets and reduce cyber risks. This includes development of a cybersecurity program that provides risk identification, mitigation, analysis, and resolution advice to the Department and to agencies. The CISO manages protective services of encryption, recovery, monitoring controls, incident detection, and response.

The Chief Service Officer (vacant from July 1, 2019 to present) plans, coordinates, reviews, and directs long and short-term strategic goals, policies, and procedures based on the Department's mission and initiatives with the ultimate goals of understanding, satisfying, and exceeding, if possible, customer expectations. This position is responsible for the delivery of customer-facing IT services, customer support, and change control.

The Chief of Staff advises the Secretary on the transformation status of legacy agency resources (personnel and equipment) to meet the requirements of the Act and provides the authority for transferring State resources into the Department. The Chief of Staff also supervises functional areas of the Department's fiscal officer, budget director, legislative liaison, and communications/public information manager.

The Chief Enterprise Architect develops and designs the enterprise architecture, sets priorities, and ensures that projects are aligned to the Department's mission, long-term strategic goals, and business objectives.

The Chief Technology Officer is responsible for building the Department's strategy for future technology innovations as well as for managing business functions covering infrastructure, applications, network, and software distribution. Each of these business functions have been assigned separate managers.

The Chief Data Officer (vacant from July 1, 2019 to November 17, 2019) reports to the Secretary and serves as a principal strategist and advisor. As a policy-making official, the Chief Data Officer sets and manages open government data effort including how the State of Illinois offers Application Program Interfaces (APIs) and creates public data products; implements big data strategy to create a statewide culture that is more data- and analytics-driven to better serves State of Illinois constituents; drives an evolving use of emerging technologies to support the best process for increased data availability.

The Enterprise Resource Planning (ERP) Program Director is responsible for directing, planning, developing, administrating, and implementing the Statewide ERP program. For participating agencies, the ERP provides consolidated management over financial services.

The seven Group CIOs promote quality of service and enhance the effectiveness of the Department's internal control environment through information exchange, general oversight of agency information processing, and strategic planning participation. The Group CIOs enhance agency awareness of Department policies, procedures, objectives, and new initiatives as well as providing a channel to communicate agency concerns and recommendations. These responsibilities have been categorized into seven (7) groups reflecting Statewide agency services. Categories are (1) family, children, elderly, and veterans; (2) government and public employees; (3) business and workforce; (4) natural and cultural resources; (5) public safety; (6) education; and (7) transportation. Vacancies within the Group CIOs include: Family, Children, Elderly, and Veterans vacant from July 1, 2019 to December 1, 2019; the education (formerly referred to as students until February 9, 2020) Group CIO vacant from September 16, 2019 to November 17, 2019; Transportation Group CIO has not yet been filled.

Human Resources

The Department's hiring practices adhere to legal requirements as published in the State Personnel Code, Personnel Rules, union contracts, *Rutan/Shakman* decisions, court orders, and applicable state/federal laws.

Workforce members are categorized into State employment workers (job protected or at will) and contractual workers (operating under a personal services contract). In addition, vendor contractors are hired based on contract requirements which follow Illinois procurement regulations and are outside of the Department's personnel hiring practices and statutorily mandated training obligations.

Each State employment position (job protected or at will) is identified on the organizational chart. Approved formal written job descriptions (CMS-104 forms) document the duties, responsibilities, qualifications, minimum acceptable competency education requirements, and experience levels for each position. Minimum acceptable competency education requirements and experience levels are identified in each job description to ensure a quality and qualified workforce. For positions subject to the Personnel Code, newly-developed and clarified job descriptions require final approval from the Department of Central Management Services' (DCMS) Division of Technical Services within the Bureau of Personnel. Job descriptions for positions not subject to the Personnel Code are approved by the Department's Secretary to ensure defined duties and required qualifications are clearly documented. For Personal Service Contractual employees (PSC), duties and responsibilities are defined initially in a PSC description of services to which the Secretary's signature is affixed and then included in the PSC contract drafted by Legal which is also signed by the PSC contractor and the Secretary.

Human Resources (HR) and the appropriate supervisor/manager verifies the accuracy of the job description or PSC description of services and identification of funding. The Department's HR prepares a Personnel Action Request (PAR) form used to initiate the posting of the employment opportunity. Prior to August 30, 2019, job postings advertised only the full salary range, as prescribed by the pay plan. As a result of Amendments to the Equal Pay Act and in accordance

with the August 29, 2019, "Follow-up to Yesterday's Equal Pay Act Amendments Training" memorandum from DCMS, beginning with positions posted August 30, 2019, job postings advertise the full salary range, as prescribed by the pay plan in addition to an anticipated starting salary determined by the hiring agency and the collective bargaining unit salary range for bargaining unit covered positions. The Secretary and the Department's Chief Fiscal Officer approve the PAR prior to HR's posting of the position.

Interview procedures, selection, and required forms vary depending on whether the position is covered by collective bargaining. For collective bargaining positions, HR compiles appropriate information as outlined in the position's collective bargaining agreement that dictates eligibility rights and forwards it to the interview panel who then conducts interviews based on *Rutan* guidelines as appropriate for the position.

For protected non-bargaining unit positions, HR identifies individuals who have submitted an employment application and have been deemed qualified and eligible through DCMS' examining process. HR forwards the information to the interview panel to commence the interview process.

For PSC positions, HR forwards candidate information to the hiring unit to schedule interviews. The most qualified candidate is selected, documented on a PSC Decision Form, and the hiring process continues concluding with a contract outlining the terms and conditions of the services to be provided.

"At will" positions require approval from the Office of the Governor in order to be filled. When filling "at will" positions, the HR Director is responsible for certifying the selected candidate meets minimum qualifications as stated in the job description. Prior to July 8, 2019, the completed certification form was provided to the Office of the Governor, the Office of the Executive Inspector General Hiring and Employment Monitor and the Special Master prior to the candidate's first working day. Per directive from the Office of the Governor, effective July 8, 2019, the completed certification form is provided only to the Office of the Governor prior to the candidate's first working day.

New employees and PSCs must pass a background check before being offered employment. The prospective candidate's demographic information is entered into the Illinois State Police's Criminal History Information Response Process (CHIRP) system. If/when the background check returns information that is acceptable to the Department, the hiring process continues with employment offered to the prospective candidate.

For State employees, performance evaluations are scheduled for probationary periods as well as annually. For employees serving a four-month probationary period, performance evaluations are completed two weeks prior to the end of the probationary period. For employees serving a six- month probationary period, performance evaluations are completed at the end of three months and again at two weeks prior to the end of the probationary period. For certified employees, performance evaluations are completed annually. Each month, HR distributes a list of due, past due evaluations and upcoming performance evaluations (due within in the next 60 days) to each respective supervisor. It is the supervisor's responsibility and obligation to complete the performance evaluation as required. Completed evaluations are returned to HR to

enter into the Human Resources Information System (HRIS) database for record tracking and keeping purpose, and completed evaluations bearing the Secretary's signature are provided to the employee and the supervisor as well as a being placed in the employee's personnel file.

For PSCs, the corresponding performance evaluation requirements vary dependent upon contract language. That is, a specific contract may mandate or simply recommend an evaluation be conducted. Contractual employment may be terminated without cause by either party which encourages satisfactory performance and quality work effort.

Newly-hired employees are provided the DCMS Policy Manual by HR during New Employee Orientation and are required to sign an acknowledgment form accepting responsibility to abide by the policies contained within the DCMS Policy Manual. Newly-hired PSCs are governed by the terms, conditions, and duties outlined in their legally-binding contract. PSCs acknowledge and accept compliance with Department policies and procedures, as each contract states that the "Contract Employee agrees to be bound by and comply with policies and procedures of the Agency." New Employee Orientation is being conducted virtually beginning April 1, 2020 due to COVID-19 remote work directives.

Employees and PSCs acknowledge awareness of responsibilities through affirming to follow policies as referenced above and through mandated annual calendar year training covering Security Awareness, Safeguard Disclosure, Ethics, and Sexual Harassment Prevention. The HR Training Coordinator provides assistance to other functional areas responsible for the monitoring, tracking, and reporting of these required compulsory trainings. Security Awareness and Safeguard Disclosure trainings are tracked by the Department's Security Program Manager via email, while the Department's General Counsel (Legal) office tracks and follows-up on Ethics and Sexual Harassment Prevention training via email.

Newly-hired employees and PSCs are directed to complete the following annual trainings via paper or through OneNet: Security Awareness Training, Safeguard Disclosure Training, Ethics Training and Sexual Harassment Prevention Training. Newly-hired employees and PSCs are required to take one-time Acceptable Use Policy training effective September of 2019, which is tracked by the Department Security Program Manager.

As directed by the Act (20 ILCS 1370), the Department transitioned existing, permanent State employees from other agencies into the Department in order to achieve consolidation of IT resources. Transition and consolidation of these workforce members fall outside the normal, personnel hiring regulations.

Over 220 Department badged employees from 11 agencies have been fully transformed to the Department's payroll and timekeeping systems as directed by the Act and designated by the Office of the Governor. This process involves:

- Receiving notification from the Governor's Office of Management and Budget (GOMB) that sufficient funds are available to proceed with the transition effort;
- Notifying the affected unions of the effective date of the transformation;
- Notifying the affected employees of the effective date of the transformation and if pay dates will change;
- Notifying the impacted agencies of the effective date of the transformation and

providing them with a transformation checklist to be completed and returned for each impacted employee;

- Providing a spreadsheet to DoIT Enterprise Applications Membership and Benefits Manager to have the impacted employees transferred systematically from their legacy agency to DoIT's "org proc" code in the benefits system;
- Conducting abbreviated New Employee Orientation for transforming employees;
- Providing/obtaining updated documents and fulfilling training requirements;
- Coordinating with and receiving applicable personnel, medical, benefit and payroll files from legacy agencies for each transferred employee;
- Identifying and processing appropriation code changes in the DCMS Personnel System for each impacted employee on the effective date;
- Printing and distributing CMS-2 turnaround documents for each transitioned employee to Payroll, Benefits, Timekeeping and HR;
- Distributing completed CMS-204 forms, as well as the transformation checklist forms, received from legacy agency to Payroll, Benefits, Timekeeping and HR;
- Entering affected employees into HRIS (if they aren't already in HRIS), HR, Central Payroll System, eTime and Central Time and Timekeeping Systems;
- Reconciling vacation base dates, updating and requesting any new schedule changes through DCMS' Compensation to maintain employee's current schedule;
- Verifying every payroll deduction listed on the transformation checklist and the CMS-204 form; confirming every payroll deduction has a corresponding supporting document;
- Updating organizational charts; and
- Assembling newly-transformed employees' personnel and payroll files including appropriation code change (CMS-2) and transformation checklists.

Voluntary separation procedures for an employee or a contractor result in HR generating an electronic Employee Exit Form (Exit Form) which is emailed to the supervisor. Once the Exit Form is completed by the supervisor, it is automatically forwarded to the Department IT Coordinator group via email which then prompts the Department IT Coordinator group to initiate the process of creating a Remedy service request to disable access and return equipment.

For an employee voluntarily separating from the Department (transferring, resigning, or retiring), once HR receives written confirmation from the employee, HR initiates a PAR, obtains appropriate Department authorizations from the Chief Fiscal Officer and the Secretary, and initiates the Exit Form. For an employee non-voluntarily being terminated from the Department, once HR receives either written or verbal direction from the Secretary or his designee, HR coordinates with the employee's manager to execute the separation process. For a PSC, the separation process begins upon expiration or termination of the contract at which time an electronic Exit Form is generated. Once the electronic Exit Form is completed by the supervisor, it is automatically forwarded to the Department IT Coordinator group which then initiates the process of creating a Remedy service request to disable access and return equipment.

Risk Assessment Process

The Department follows the IT Risk Assessment Policy published on the Department's website. The Risk Assessment Policy assigns responsibility for conducting risk assessments and vulnerability scanning to the Department with the scope spanning entities identified as client agencies under executive orders, compiled statutes, or inter-governmental agreements. The Risk Assessment Policy also requires the Department to share assessment results with client agency senior management and appropriate designees.

During the period of July 1, 2019, to September 8, 2019, the Department followed the Risk Management Program which describes the State of Illinois Risk Management process from data and system categorization to maturity level of existing security controls. Effective September 9, 2019, the Department reviewed and updated the Risk Management Program to reflect the current process.

The Risk Management Program describes the data and system categorization process of mission critical information systems. The results and conclusions of the risk assessment is used as leverage to justify expenditures, manpower, time, budgeting, technology purchases, and general procurements.

The Department conducts organizational risk assessments based on National Institute of Standards and Technology (NIST) security and privacy controls for agencies, boards, and commissions that report to the Governor. Based on the Department's Risk Management Program, a series of steps are followed to conduct a risk assessment. Each agency is provided an organization risk assessment survey and agency responses are given a qualitative maturity value for existing security controls. The results are calculated and help to identify and prioritize potential security weaknesses. The risk assessments are conducted based on the Department's workload and the client agency availability.

Agencies are responsible for providing mitigation plans corresponding to risk assessment results. Risks and mitigation plans are captured in a Risk Register by the Risk team for follow-up. The Risk team contacts agencies based on their risk mitigation anticipated completion date to confirm risk remediation implementation. Agency risk remediation efforts are documented and updated in the Risk Register, and artifacts are stored in their individual risk folders.

In addition, the Department receives threats, vulnerability, and incident intelligence from multiple sources, including the MS-ISAC and the Illinois Statewide Terrorism and Intelligence Center. Risks from potential and newly discovered vulnerabilities are assessed through interaction with Department's security employees and vendor subscription services. The Department also maintains contact with vendors to receive patch vulnerability information.

A vulnerability scanning process is employed to assess servers identified through server discovery scan for each agency. Vulnerability scans are scheduled weekly. The Department shares vulnerability scanning results with Group CIO's and agency CIO's via email weekly. The Department provides client agencies with the Agency Instructional Guide for Submitting Vulnerability and Remediation Tickets to mitigate identified server vulnerabilities. Unremediated vulnerabilities will continue be reported in the weekly scan reports. In the case where remediation efforts have failed or caused operational issues, corrective action plans are

developed by agency CIO. Agencies are responsible for providing corrective action plans to remediate identified server vulnerabilities.

Information and Communications

The Department's website delivers information to client agencies and to Department staff covering:

- Initiatives and accomplishments,
- Policies,
- Service Catalog (which describes services available to user agencies)
- Instructions on how to order services and products as well as how to report operational problems.

The policies located on the Department's website include:

Acceptable Use Policy
Access Control Policy
Accountability, Audit, and Risk Management
Privacy Policy
Audit and Accountability Policy
Awareness and Training Policy
CJIS Security Supplemental Policy
Configuration Management Policy
Contingency Planning Policy
Data Minimization and Retention Privacy Policy
Data Quality and Integrity Privacy Policy
FTI Supplemental Policy
Identification and Authentication Policy
Individual Participation and Redress Privacy Policy
Information Security Incident Management Policy
Media Protection Policy
Overarching Enterprise Information Security Policy
PCI Data Security Policy
Personnel Security Policy
PHI Supplemental
Physical and Environmental Protection Policy
Privacy Security Policy
Program Management Policy
Risk Assessment Policy
Security Assessment and Authorization Policy
Security Planning Policy
System and Communication Protection Policy
System and Information Integrity Policy
System and Services Acquisition Policy
System Maintenance Policy
Transparency, Authority, and Purpose Privacy Policy
Use Limitation Privacy Policy
Identity Protection Policy

Mobile Device Security Policy
Wireless Communication Device Policy

The website also provides links to the DoIT Digest content, which informs the reader of new initiatives, business applications, ongoing projects, administrative information, and Departmental news. The DoIT Digest publication is scheduled every two weeks. Due to COVID-19, beginning April 3, 2020, the DoIT Digest has been published weekly to include topics related to COVID-19 and the work from home effort.

In addition to the Department's website, client agencies are kept informed through direct correspondence and face-to-face meetings. The Department's Communication Office sends email correspondence to appropriate agency groups (directors, CIOs, Telecom Coordinators, Agency Technology Service Requestor (ATSR) known as Department IT Coordinators through November 2019 transition period) as appropriate to the message being conveyed. Group CIOs provide an exchange of information between the Department and agencies and keep both the Department and agencies informed regarding significant events, service issues, improvements, processes, and strategic goals. Group CIOs meet with agency CIOs when business need requires or when instructed by Department management to update and gather information from agencies. Group CIO communication occurs at an individual agency level. State-wide level agency communication is accomplished through CIO Council meetings which are held at the Secretary's request to update and inform agency CIOs of news and information.

Agency CIOs, along with Department leadership, are invited to attend "DoIT Daily" meetings (Mondays through Thursdays). DoIT Daily is a forum to share high-level and high-risk operational issues with a team equipped to discuss steps for resolution. Due to COVID-19, the DoIT Daily meetings have changed to Mondays through Fridays effective March 20, 2020 while working remotely.

Department internal staff are kept informed through multiple sources such as the Department's website, the Employee Portal (intranet), Town Hall meetings, and emails. The Employee Portal provides information covering topics such as pensions and retirement, insurance, training opportunities, payroll information, and workplace safety. Town Hall meetings keep Department workforce members informed on topics such as Department strategic priorities and new Department and/or Statewide initiatives. Direct email communications alert workforce members to technical, security, or emergency issues and concerns such as outages, phishing attempts, and scheduled upgrades.

SoundBytes is an employee blog located on the employee portal which provides a communication channel where Department employees can exchange information and updates. The blog is intended to serve as a platform for Department employees to communicate and connect virtually. The posting categories include:

- Celebrating Employees
- Comings & Goings
- Health & Fitness
- News & Updates
- Outside of Work
- Secretary G's Corner

SoundBytes allows all employees to create posts, which are then moved to a pending status. Members of the communication team are notified when there is a new post and they can either approve or reject the post.

Due to COVID-19 and State employees working remotely, beginning March 26, 2020, Remote Work – Reminder of the Day has been published daily to share information to facilitate work from home. A Remote Work webpage was published on the Department's website March 16, 2020 to provide guidelines and additional resources to support employees working remotely. Beginning June 8, 2020, Remote Work – Reminder of the Day is published as needed when there is remote work news or information to share.

Monitoring

Monitoring of Department Services and Performance

Effective July 15, 2019, the Audit Committee was formed to assist the Secretary in fulfilling his responsibilities for effectively and efficiently managing and maintaining an effective system of internal control. The Audit Committee consists of Chief of Staff, Chief Administrative Officer, and General Counsel. Effective February 10, 2020, the Audit Committee consists of Acting Assistant Secretary, Chief of Staff, Chief Administrative Officer, and General Counsel. The Audit Committee's responsibilities include monitoring of: internal controls, internal audits, external audits, and reporting responsibilities. The Committee is to meet four times per year, with the authority to convene more frequently if requested.

Customer Support Division staff conducts monthly meetings inviting representatives from appropriate Department teams to discuss performance metrics for team awareness. Critical and high level Remedy tickets that did not meet the performance metrics are discussed for potential service improvement going forward. Effective January 2020, the Customer Support Division staff changed the meeting frequency to quarterly, with the authority to convene more frequently if requested. In addition to storing data on a SharePoint site, service level metrics showing the Department customer service performance are posted on the Department's website.

Monitoring of Subservice Providers

The Department's Governance, Risk and Compliance unit collects and reviews subservice providers' System and Organization Controls (SOC) reports from BMC, Microsoft, Micro Focus, NIC, Google Cloud, Salesforce, and Zayo for alignment with State of Illinois enterprise information system security policies. Written review of subservice organization controls and exceptions noted in the SOC reports are presented to the business owner for their review. Business owner reviews and approves via signature on the workbook. Complementary User Entity Controls are also documented and provided to the business owner for them to provide attestation of compliance. The Compliance team collects business owner's confirmation of compliance, however, artifact to support the business owner's affirmation is not always collected. Quarterly follow-up with business owners is conducted, only if weaknesses are identified, to confirm identified weaknesses in attestation form are addressed.

The Department's baseline controls are utilized to evaluate subservice organizations' SOC reports to ensure compliance with the State of Illinois enterprise information system security policies. The Department's baseline controls include the following: access control, awareness

and training, system and information integrity, malicious code protection, contingency planning, configuration management, risk assessment, incident response, security assessment and authorization.

In addition, Department project management team conducts weekly meetings with BMC (meeting frequency has changed to bi-weekly since January 2020), NIC, Google (starting from May 7, 2020), Micro Focus, and Salesforce (starting from April 24, 2020) to ensure compliance with contractual requirements. A monthly meeting is held between the Department and Microsoft. The Department communicates with Zayo management face to face or via available communication media (email, phone, or other) regarding existing services as stated in the contracts.

The Department annually monitors the DCMS managed the Central Computing Facility (CCF) to ensure appropriate physical and environmental controls are in place. The Department reviews the CCF building related contracts and validates deliverables with a checklist and walkthrough to ensure contractual compliance. Identified weaknesses and recommendations are provided to the Department's Chief of Enterprise Infrastructure and DCMS facility manager for corrective action responses. Corrective action items are followed up with the business owners via meetings and emails.

The Department is in process of developing annual monitoring controls for the DCMS managed Communication Center to ensure appropriate physical and environmental controls are in place. Due to the COVID-19 crisis, the Communication Center physical environment walkthrough was delayed.

Environment

Midrange

The Department's midrange configuration consists of physical and virtual devices. These midrange devices host the various services the Department offers. The midrange primary operating systems software includes:

- Microsoft Windows Servers operating system is a series of enterprise-class servers operating systems designed to share services with multiple users and provide extensive administrative control of data storage, applications and corporate networks.
- VMWare Elastic Sky X Integrated (ESXi) is an enterprise class type-1 bare-metal Hypervisor that installs onto a physical server with direct access to and control of underlying resources and can effectively partition hardware to increase virtual servers' ratios.
- Advanced Interactive eXecutive (AIX) is an enterprise-class UNIX operating system for the POWER processor architecture found in the IBM Power Systems.
- LINUX is a family of free and open-source software operating systems built around the Linux kernel, typically packaged in a form known as a Linux distribution for both desktop and server use.

Mainframe

The Department's mainframe configuration consists of multiple CMOS processors (Complementary Metal Oxide Semiconductor processors) segregated into logical 'production'

and 'test' partitions. Partitions are configured in a Sysplex platform, IBM's systems complex coupling environment.

The primary operating system software includes:

- IBM z/OS: a complex operating system (OS) that functions as the system software which controls the initiation and processing of work within the mainframe.
- z/Virtual Machine (z/VM): a time-sharing, interactive, multi-programming operating system.
-

Primary z/OS subsystems include:

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

The primary z/VM subsystem is NOMAD which is a database software system.

Information Systems Overview-Applications

The Department's Enterprise Business Applications group (also referred to as Enterprise Application & Architecture - EAA) offer several applications to agencies including:

- Accounting Information System (AIS) hosted on the Department's mainframe;
- Central Inventory System (CIS) hosted on the Department's mainframe;
- Central Payroll System (CPS) hosted on the Department's mainframe;
- Central Time and Attendance (CTAS) hosted on the Department's mainframe; and
- eTime hosted on the Department's midrange, server environment.

Agencies are responsible for the complete and accurate entry and maintenance of data into the applications. The Department is responsible for application updating and maintenance. Separate, stand-alone user manuals and guides are available for the AIS, CIS, CPS, and CTAS applications. User instructions and guides are imbedded into the application itself for eTime. Applications have edit features designed to reject erroneous or invalid data. When erroneous or invalid data is entered, an error message is displayed on the screen indicating the problem. Various reports are generated, based on the application, to assist with data integrity and reconciliation.

<u>Accounting Information System</u>

AIS functions include accounts payable, appropriation management, fund transfer and adjustment, vendor management, contract and contract amendment. AIS also tracks expenditures from the initial receipt of the invoice, throughout the production of vouchers, and updates the records with payment information once processed by the Office of the Comptroller.

AIS also provides both project and cost center accounting.

Transaction records allocate financial information into sub accounts according to the Office of the Comptroller's Statewide Accounting Management System (SAMS) procedures which allows agencies to track cost centers.

AIS supports segregation of responsibilities and functions by limiting the ability of data manipulation to bureau and accounting administration. The bureau level allows for the initial entry and maintenance functions, where the accounting level is the audit function and final approval process.

Upon passage of a State budget, agencies enter their applicable appropriations. After entry of the appropriations, agencies are required to enter their obligation data (contracts) against the applicable expenditure account. A contract must be entered before the corresponding obligation is recognized.

Upon receipt of a vendor's invoice, the agencies enter invoice information to assure sufficient funds are available in the appropriation. The agencies must indicate the fund, account, and line item in which the invoice is being charged to in order to ensure sufficient appropriations are available. Upon proper approval within AIS, the voucher is printed for agencies' head approval and submission to the Office of the Comptroller. In addition, the agencies can print the AIS13 for review.

AIS allows agencies to issue refunds/credits and make adjustments to invoices. The type is dependent on the circumstance. The refund/credit allows funds to be added back to the voucher and the appropriation/obligation line.

When erroneous or invalid data is entered, an error message will appear at the top of the screen and the field that is in error will be highlighted. AIS will not accept the entry until the error has been corrected or deleted. In addition, AIS will not allow a transaction to be processed without sufficient funds.

AIS interacts with the following applications and systems:

- ALS - Auto Liability System;
- ARPS - Accounts Receivable Posting System;
- CPS - Central Payroll System;
- CRIS - Comprehensive Rate Information System;
- ERP – Enterprise Resource Planning; and
- Office of the Comptroller systems.

Central Inventory System

CIS is an enterprise online and batch application that provides each user agency a platform to manage their inventory/real assets. The system provides the users the ability to create, update, track, transfer, and remove their property records for equipment, furniture, real property, and vehicles. Upon receipt of an asset, the agency user enters the asset's tag, location, voucher information, and description into CIS. In the event information regarding the asset needs to be revised, such as location change, the agency user enters the update. In the event an asset requires

deleting, the agency contacts DCMS' Property Control Division to obtain approval prior to deletion. Provided as an option, CIS also performs straight-line depreciation for agencies who request it. Depreciation is applied monthly to each agency's specifically flagged asset record and a series of reports are generated that list each asset's activity and the agency's overall asset counts and values.

CIS user online entry screens are equipped with data edit checks and range checks which provide the user with immediate notification of entered or missing data that do not pass the online edits. All data entry must pass the online edits before any information is stored. Since an asset tag number is the primary identifier of an asset, CIS does not allow reuse or duplicate tag number records; this includes the reuse of inactive tag numbers since CIS retains these as archive.

Reports are available and can be requested online by the agency user. Also, reconciliation reports may be requested to assist agencies in maintaining an on-going accuracy of their assets/inventory.

Central Payroll System

CPS enables agencies to process and manage payroll information for their employees. CPS generates payrolls for agencies providing for appropriation coding, base pay and overtime computation, updating of relevant tax tables, processing of supplemental and anticipated payrolls, net pay determination, and direct deposit. CPS also provides for warrant reversals to correct warrants issued in error.

Agencies are responsible for reviewing the payroll voucher to ensure the accurate calculation of deductions.

CPS has a ten-day working pay schedule, which allows agencies to enter their payroll ensuring that vouchers are processed timely. Every pay period is assigned a close date, which is the date that payroll data entry must be completed. On the night of the close, CPS freezes the data for that pay period and runs the Gross-to-Net process. The Gross-to-Net processes uses the data for the pay period, along with tax tables and withholding information to calculate and generate vouchers for employees that are to be paid. Error reports are generated if the Gross-to-Net process fails or problems are identified.

As part of the Gross-to-Net process, payroll vouchers are produced as a series of reports for each agency. Each agency prints the payroll voucher, approves, and submits to the Office of the Comptroller for warrant generation. In addition, CPS sends an electronic file of the vouchers to the Office of the Comptroller.

In the event the payroll is rejected by the Office of the Comptroller or the Gross-to-Net process, or if the agency identifies problems when they review the voucher reports, the data must be corrected and re-generated. This is accomplished by the agency submitting a Remedy ticket requesting a change and assigning to the CPS Support unit. Remedy procedures route the request to appropriate Department staff who then run special ad-hoc programs to correct the specific problem and then re-run the Gross-to-Net process.

The Office of the Comptroller verbally and/or through email informs the Department of any

federal tax rate change. The Department's CPS staff modifies federal tax tables accordingly.

When calculating State withholding, CPS recognizes a limited set of State identifiers which are listed in the Central Payroll User Manual. When a record is entered for which there is no recognized State identifier, CPS generates an error message on the screen. Appropriate action is taken to either correct an error by the Department or agency payroll administrator by entering the correct value or to request the addition of a State identifier by the Department or agency payroll administrator working with Office of Comptroller. After the Office of Comptroller confirms the addition, the technical Payroll manager follows the Department change management process to have a change made in the application.

On an annual basis, CPS staff research tax rates for CPS-recognized states and update state tax tables accordingly. In addition, the CPS manager receives email notifications from a procured service that identifies state tax rate changes. Upon notification, the CPS manager creates a Remedy work order that instructs CPS support team staff to update the state tax rate for states identified within CPS where the rate has changed.

When erroneous or invalid data is entered, an error message will appear at the top of the screen and the field that is in error will be highlighted. CPS will not accept the entry until the error has been corrected or deleted.

Reports are available to assist agencies in processing payroll.

CPS interacts with the following applications and systems:

- AIS;
- ERP; and
- Office of the Comptroller systems.

Central Time and Attendance

CTAS provides a system for recording and managing employee time. CTAS calculates and reports overtime, compensatory time, accumulated leave and benefits based on continuous service dates, accumulated leave and compensatory time, and monitors maximum vacation carryover. CTAS records attendance information using either the positive or exception method. The positive method requires the timekeeper enter or confirm an employee's general attendance information. The exception method assumes that an employee's scheduled work time is the correct attendance unless the timekeeper enters something different. CTAS also maintains historical records of employee time data and can generate audit trails pertaining to adjustments when requested.

Each agency's timekeeper is responsible for entry and maintenance of an employee's time and attendance; vacation, sick, personal, etc. For agencies using only CTAS, timekeepers have the responsibility for entry and maintenance of an employee's time and attendance.

To reconcile the time entered for a payroll period, CTAS performs a "close" process which checks for consistency and completeness and performs necessary calculations for overtime and compensatory time. The process utilizes the work schedule to create the attendance entries for "exception-entry" employees who did not have their attendance entered for a particular day.

Agencies complete a "pre-close" process and review information to ensure its accuracy.

Once the "close" process has been run, CTAS generates an error report, a reconciliation report, and a file maintenance activity report. Discrepancies need to be reconciled before a "close" can be finalized.

When erroneous or invalid data is entered, an error message will appear at the top of the screen and the field that is in error will be highlighted. CTAS will not allow transactions to be processed until errors are rectified.

In addition, CTAS produces other reports that assist in data integrity and processing including lists of pending pre-close transactions (which identifies potential warnings and errors that may occur during the close process), supplemental requests (lists information other than found in the close process report), and listing of employee historical information. Per an agency request, ad hoc, non- standard reports may be generated based on extracts from the CTAS database.

CTAS interacts with e-Time; sharing a back-end database where e-Time is the front- end GUI interface.

eTime

eTime allows agencies the ability to manage work time and attendance. eTime provides for the ability for employees to electronically report hours worked and to submit leave, overtime pre-approvals, time reports and overtime requests. For agencies using eTime, timekeepers have the responsibility for adjustments of an employee's time and attendance.

Specific eTime roles and access privileges are defined in the application access provisioning section.

Agencies may opt to use eTime as a mechanism for capturing, collecting, and reporting contractual worker (operating under a personal services contract) hours. Actual hours worked are entered by the contractor. Once their time report is submitted, eTime routes hours entered to the appropriate supervisor/delegate for approval. For a given pay period, the timekeeper searches eTime to retrieve approved contractual hour amounts and then manually posts them into CTAS.

Error messages are displayed on the screen as inconsistencies are encountered. Sample message topics include exceeding comp time; duplicate record or request, no preapproval, overtime exceeds pre-approved hours, and others. Supervisor/delegate roles are prohibited from correcting errors or changing employee entered information. Quick reference guides and context sensitive error messages are available to assist users when using the application.

Information Technology General Controls

Change Control

Remedy On Demand (referred to as Remedy or ROD) is the Department's control mechanism over changes to Department resources including infrastructure and applications (AIS, CIS, CPS,

CTAS, and eTime).

Remedy components include service requests, work orders, tasks, and change requests which can originate either externally from a customer request or internally from support staff.

Remedy accepts service requests from agency authorized ATSR or Department IT Coordinator. Service requests may generate work orders, tasks, or change requests. Internally, Remedy work orders, tasks, and change requests may also be created by authorized Department managers or support staff.

Work orders, tasks, and change requests are assigned to Department technicians, support staff, and subject matter experts through group (team) profiles and individual assignments as directed by the IT Service Processing or by a designated Department support staff. Remedy uses status indicators to manage work flow. Status indicator of complete, automatically generates an email notification to the requestor. The requestor may contest or challenge the completed status within 5 days from the email notification.

Agencies are responsible for submission of a Remedy ticket documenting issues and needs of the environment and applications.

Change Control – Other than Applications
Control over changes to the network, mainframe, mainframe patching, and midrange infrastructures as well as to data storage devices are documented in the Change Management Process Guide, ROD Change Management Guide, and the Change Management User Guide which provides a quick reference of the Department's change processes.

The Change Advisory Committee (CAC) supports the authorization of changes and assists Department managers and technicians in assessing and prioritizing changes and makes recommendations regarding significant impacts. The CAC consists of individuals from the Department as well as from multiple agencies and is chaired by the Enterprise Change Manager. Minutes, along with reports, are posted to the Change Management SharePoint site, accessible by authorized agency personnel.

Change requests are classified into class and impact categories with approval levels of Support Group Manager, Enterprise Change Manager, and the Change Advisory Committee. A matrix in the Change Management User Guide, published on the CAC SharePoint site (User Guide Quick Reference), identifies the level of approval based on combinations of class and impact categories.

In the event of an emergency, only verbal approval by the Support Group Manager is required to begin remediation. Remedy documentation is finalized once the emergency has subsided.

Significant or extensive impact changes require test, implementation, and back out information be provided within the change request. Emergency changes require a Post Implementation Review be provided within the change request.

Change Control - Applications (AIS, CIS, CTAS, CPS, and eTime)
For application changes, processing steps are documented in Application Lifecycle Management Manual, EAA Mainframe Change Management Procedures and the EAA Distributed Change Management Procedures. Effective November 1st, 2019, EAA Web Service Change Management Procedures was renamed as EAA Distributed Change Management Procedures.

An application change is initiated with the submission from an authorized ATSR, or Department IT Coordinator, or internal support staff of a Remedy request which then follows enterprise change management procedures and processes described within. A single request may be a body of work containing multiple tasks, some of which necessitate a change to application code, application database, or generating new reports.

For mainframe application changes, a revision control and code management system permit a developer to 'checkout' program code while prohibiting modified code from being placed back into the production area without proper authorization. Developers attach the Move Sheet to the corresponding change request record within Remedy. Remedy's built-in workflow approval process requires supervisory approval before Remedy releases the activity to the Library Services group that performs the move into production. Moves to the mainframe production environment are completed by Library Services based on the instructions within the Move Sheet. Developers are limited to read only access to the Production Libraries.

For distributed systems, Remedy's built-in workflow approval process requires supervisory approval prior to deployment into the production environment. Designated release staff, who did not code the change, can move the change into the production environment manually, and developers who coded the changes verify the changes to ensure accuracy, or via an automated release management module if configured, with supervisor approval.

The Remedy request is considered resolved after all tasks have been designated as completed. A Remedy status value of 'completed' automatically generates an email notification to the requestor who then may contest or challenge the result within 5 days from the notification.

Change Control Over Network
Network infrastructure modifications are performed in accordance with the Department's Change Management Process.

For common infrastructure devices, the Department maintains detailed technical specifications identifying mandatory configuration parameters. New Wide Area Network (WAN) backbone equipment is energized, configured, and operated in a lab environment to help ensure faultless operation in production.

New Local Area Network (LAN) devices that meet Department standard specifications are attached to the network when received within operational workload constraints. Devices for which the Department has no detailed technical specification defined or for which the Department has determined may cause a significant impact, undergo a two-step change management process. The first step is a Network Operations internal peer review which is where the network modification is reviewed by subject matter experts and approved by Department

network architects. The second step is to submit the network modification by the Department Network staff through the change management process for approval by the Change Advisory Committee. The Department change management procedures are then followed to implement the network modification.

Change Control Over Mainframe
For z/OS maintenance only, the test systems are updated monthly and the production systems are updated quarterly. All production changes follow the Department's Change Management Process.

When patches become available, all other mainframe software components (IMS, CICS, DB2, ISV, etc) follow the Department's Change Management Process.

Mainframe hardware configuration changes follow the Department's Change Management Process.

Change Control Over Midrange Infrastructure
Enterprise changes impacting the Midrange infrastructure follow the Department's Change Management Process.

Changes to Midrange infrastructure are requested via Remedy ticket. Midrange technical staff review the request to ensure validity and determine any impact to the enterprise environment and follow the Department's Change Management Process to implement.

IT Service Desk
The Department's IT Service Desk serves as a central point of contact for processing and managing password resets and incident management (reporting, assignment, and resolution). Incidents are reported to the IT Service Desk by Department staff and client agency staff via phone, email, or website submission.

Incident Management
The Incident Management Process Guide documents Department workflow and remediation processes for incident management.

An incident is defined as an unplanned interruption to an IT service, reduction in the quality of an IT service, or a failure of a configured item. Agencies are responsible for reporting incidents to the IT Service Desk.

Incidents are reported to the IT Service Desk by Department staff and client agency staff via phone, email, or website form submission. When the IT Service Desk receives a report of an incident, a Remedy ticket is opened, documenting the user's name, agency, and contact information along with a detailed description of the incident. Each incident is categorized based on the service, system, or application impacted by the incident. Tickets are also prioritized based on the impact (the number of affected users) and urgency (how quickly the resolution is needed) of the incident. The IT Service Desk then assigns the Remedy ticket to the applicable service group for remediation and closure of the ticket. Reported incidents are tracked via a Remedy ticket until appropriate remediation efforts are completed.

From July 1st to August 22, 2019, incidents which are assigned both widespread/extensive impact and critical urgency, or events affecting an entire agency that has an unknown or uncertain resolution, are tagged as a major outage. Under these conditions, IT Service Desk support staff modify the Remedy ticket assignment group to "Major Outage Response Team" and update the MORT field to "Yes". Designated support staff send out notification of the Major Outage via distribution lists through available communication media (email, phone or other) for information purposes only. In addition, if the cause of the outage is unknown, MORT team members (subject matter experts and decision makers appropriate for the event and its resolution) are contacted to join a phone bridge to discuss the outage. Status updates will be provided until resolution or a work-around has been achieved. This information is also conveyed to affected users via distribution lists.

On August 23, 2019, the Remedy MORT field was updated to reflect outage type with options of "Individual", "Localized", "Unplanned Outage" and "MORT".

Incidents with any impact or urgency that affects a limited group of client agency staff or a single location, where notification is deemed necessary, are categorized "Localized" incidents. Designated support staff send out notification of the localized outage via distribution lists through available communication media (email, phone, or other) for informational purposes only. Status updates will be provided until resolution or a work-around has been achieved.

Incidents which are assigned both widespread/extensive impact and critical urgency, events affecting an entire agency or any other outage requiring visibility that has a known cause and can be tied to a specific support team are tagged as an unplanned outage. Under these conditions, designated support staff modify the Remedy ticket and update the Outage Type field to "Unplanned Outage". Designated support staff send out notification of the Unplanned Outage via distribution lists through available communication media (email, phone, or other) for informational purposes only. Status updates will be provided until resolution or a work-around has been achieved. This information is also conveyed to affected users via distribution lists.

Incidents which are assigned both widespread/extensive impact and critical urgency, or events affecting an entire agency that have an unknown or uncertain resolution, are tagged as MORT. IT Service Desk support staff modify the Remedy ticket assignment group to "Major Outage Response Team" and update the Outage Type field to "MORT". Designated support staff send out notification of the Major Outage via distribution lists through available communication media (email, phone or other) for information purposes only. In addition, MORT team members (subject matter experts and decision makers appropriate for the event and its resolution) are contacted to join a phone bridge to discuss the outage. Status updates will be provided until resolution or a work-around has been achieved. This information is also conveyed to affected users via distribution lists.

All other incidents are classified with the type of "Individual" with no notification necessary.

Effective January 23, 2020 incidents which are assigned both widespread/extensive impact and critical urgency, events affecting an entire agency or any other outage requiring visibility that has a known cause and can be tied to a specific support team are tagged MORT (No Bridge). IT

Service Desk support staff modify the Remedy ticket assignment group to "Major Outage Response Team" and update the Outage Type field to "MORT". Designated support staff send out notification of the MORT via distribution lists through available communication media (email, phone, or other) for informational purposes only. Status updates will be provided until resolution or a work-around has been achieved. This information is also conveyed to affected users via distribution lists.

Incidents which are assigned both widespread/extensive impact and critical urgency, or events affecting an entire agency that have an unknown or uncertain resolution, are tagged as MORT. IT Service Desk support staff modify the Remedy ticket assignment group to "Major Outage Response Team" and update the Outage Type field to "MORT". Designated support staff send out notification of the Major Outage via distribution lists through available communication media (email, phone or other) for information purposes only. In addition, MORT team members (subject matter experts and decision makers appropriate for the event and its resolution) are contacted to join a phone bridge to discuss the outage. Status updates will be provided until resolution or a work-around has been achieved. This information is also conveyed to affected users via distribution lists.

Any impact or urgency with a known cause that can be tied to a specific team (that does not qualify as MORT), can be tagged as "Unplanned Outage" if notification is deemed to be warranted by the Department staff or the team initiating the incident ticket. Under these conditions, regular incident management process is followed.

Lost or Stolen Equipment

As published in the Acceptable Use Policy, agencies or users are responsible for reporting lost or stolen equipment by notifying their immediate supervisor, who is responsible to notify the Department's IT Service Desk, or notifying the Department's IT Service Desk directly.

The IT Service Desk initiates a Remedy ticket to track and document the event that captures the asset/property tag, the user reporting the loss, and any police reports if available. IT Service Desk management reports the loss via email to the EUC Manager, EUC Image Management and the Security Operations Center (SOC).

An encryption protection feature is installed as part of laptop imaging prior to deployment. EUC Image Management verifies encryption status and responds to initial email with results.

If the device was encrypted, the Remedy ticket is assigned to Property Control unit for disposition. Property Control manager then completes a Request for Deletion form and assigns a staff to create an inventory removal request with police report and Request for Deletion form attached in SAP ERP, the Department inventory management system. Once the Property Control manager and DCMS approve the SAP ERP request, the device is marked as "INACTIVE" in SAP ERP, and the associated Remedy ticket is closed by the Property Control unit.

If encryption is inactive or was not installed as part of the device imaging process prior to deployment, EUC Image Management will assign the Remedy ticket to the SOC who will enact a breach investigation that consists of steps outlined in their Security Incident Playbook. The

first step is to interview the user to determine if sensitive or confidential data was stored on the device. If no sensitive or confidential data resided on the device, the SOC will update the Remedy ticket and assign to Property Control unit for disposition. Property Control completes a request for deletion of the device from inventory as described above. Otherwise, the SOC assists with the investigation to mitigate the impact of the potentially compromised data and affected users. Documentation, correspondence, and resolution actions are recorded and captured in the SOC's incident reporting tool. If further investigation is required, the Property Control unit forwards a copy of the police report to the Illinois State Police.

Logical Security

Access Provisioning
The Department policies titled Identification and Authentication Policy, Personnel Security Policy, Access Control Policy and Configuration Management Policy address logical security and are published on the Department's website.

Access or modifications to Department resources (network, shared services, mainframe processing, and applications) begins with submission of a Remedy service request from an authorized ATSR or Department IT Coordinator. The IT Service Processing team assigns Remedy tasks to support groups to satisfy the request. Once all tasks are completed, the Remedy ticket status indicator is automatically updated to "Complete", and the system automatically generates an email notification to the requestor.

Access revocation to Department resources starts when the Department has been notified an individual is separating employment or the initial justification for access has changed. The revocation process is initiated upon receipt of Remedy service request by an authorized ATSR or Department IT Coordinator, IT Service Processing team assigns Remedy tasks to support groups to satisfy the request. Under special or emergency circumstances, network access is disabled at the instruction of the Department senior management.

Access Provisioning – Applications
Access to AIS, CIS, CPS, and CTAS is a three-layer approach requiring acquisition and activation of (1) network, (2) mainframe, and (3) application-specific accounts. Remedy processes as noted above are followed to grant access to network and mainframe resources.

Application specific account provisioning is managed by the Agency Application Administrators who are responsible for assignment of their agency's application specific accounts, associated rights and privileges, password management, and deactivation or reassignment. Agencies are responsible for ensuring proper segregation of duties in the assignment of application user access rights. Additionally, agencies are responsible for reviewing the user access rights to their data.

Agency Application Administrators are established through the ATSR submission of a Remedy service request. The IT Service Processing team assigns Remedy tasks to support groups to satisfy the request. Once all tasks are completed, the status indicator is automatically updated to "Complete", and the system automatically generates an email notification to the requestor. The Department may assist an agency when issues arise which are managed through the Remedy

process.

Access to eTime application is authenticated via Active Directory (AD). Functionality within the eTime application is based upon assigned roles.

eTime has defined functional roles of system administrator, administrator, timekeeper, supervisor/delegate, employee, auditor, and chief financial/fiscal officer. The system administrator role is used to make agency specific changes to settings and/or to setup new agencies. The administrator role assigns roles to individuals within the administrator's agency. Agency eTime administrators are established through submission of a Remedy service request by the agency's ATSR as approved by the agency's Human Resource Director or designee. The timekeeper role processes exceptions that may result from leave requests and/or overtime worked. The supervisor/delegate role approves employee time reports, overtime pre-approvals, overtime worked, and leave requests. The employee role permits direct entry of time worked and adjustments to the standard work schedule by the workforce member. The auditor role provides search capabilities in a view only mode. The chief financial/fiscal officer role provides limited search capabilities in view only mode.

After authentication is granted into the browser-accessible log-in screen, the user selects from multiple options based on the action to be taken and the user's functional role. For employees, the process begins with entering exceptions to standard, scheduled hours established in CTAS. This is accomplished by requesting overtime pre-approvals and leave requests, submitting overtime worked hours, or canceling or modifying previously entered information. Conditions requiring approvals are automatically routed to the appropriate supervisor/delegate. Supervisors/delegate enter approvals for overtime and leave requests which are processed nightly via the CTAS batch process.

Agencies are responsible for managing eTime and review the user access rights to their data.

Password Resets

Password Resets – Mainframe

In the event a user requires a reset of their mainframe password, they are required to either submit the request via email to the IT Service Desk or use the Department's self-service option: DoIT Identity Management tool. Email reset requests are to include the user's name, mainframe ID and a contact phone number. The IT Service Desk staff will create a Remedy ticket and contact the user at the number provided and reset the mainframe ID password. If the IT Service Desk staff are not able to reach the user,a message is left for the user that includes the Remedy ticket number and instructing them to contact the IT Service Desk, at which time the password will be reset.

When the individual returns the IT Service Desk call, the individual's ID is verified with the information within the Remedy ticket prior to resetting the password.

In the event the IT Service Desk does not have appropriate rights to reset a mainframe password, the user is instructed to contact their Agency System Software Coordinator. In the event the Department is the agency's proxy, a Remedy ticket is assigned to the Department's Security Software Coordinator or Security Software Administrator. Using information from the Remedy

ticket, the Security Software Coordinator or the Security Software Administrator contacts the user to reset the password. If unable to contact the user on the first attempt, a message is left asking the user to call back. No password is left in the message. Passwords used in the resetting process are temporary, one-time use only. The Remedy ticket remains open until the password has been successfully reset after which the Remedy ticket is closed.

Password Resets - Active Directory
Active Directory accounts are reset by users calling the IT Service Desk or by one of the Department's self-service options – Microsoft Identity Management (MIM) or the Department's Identity Management (DIM) tool. IT Service Desk encourages use of the self-service option.

When a call is received by the IT Service Desk for an Active Directory password reset, IT Service Desk staff will determine if the caller is eligible to use MIM/DIM and if they have previously registered. If registered, users will be directed to reset their password via this method. If they are unsuccessful, have not previously registered or are not eligible to use MIM/DIM, IT Service Desk staff will create a Remedy ticket and proceed with the reset after verification of two of the following three pieces of information; phone number, email address and physical address. Once a successful reset has taken place, users will be instructed to either register or re-register for MIM/DIM if eligible.

Password Resets – Novell
Self-service options are not available for Novell. IT Service Desk staff will create a Remedy ticket and perform a verification of two of the following three pieces of information; phone number, email address and physical address before resetting the password.

Agencies are responsible for contacting the IT Service Desk or the utilization of the self-service options, in order to reset the AD or Novell accounts.

<u>System Security</u>
System Security-Mainframe
The Department utilizes security software as a method of controlling and monitoring access to the mainframe resources. The security software requires an established ID and password to verify the identity of the individual. The primary means of defining an individual's access is the security software profile. The security software profile defines the level of access a user has.

For the creation of a security software account, agencies are responsible for the submission of an approved service request or Mainframe request form if Remedy service request is not available for the agency. Once the service request is created in Remedy, or Mainframe request form is submitted, then the agency Security Software coordinator designate or, in the case of a client agency not having a Security Software coordinator, the Department's Software Security coordinator will receive the Remedy ticket, and follow the security software ID creation procedures to create an account as specified.

Password security parameters have been established and configured to ensure access to mainframe resources is appropriate:

- Minimum password length;
- Password complexity;

- Password history;
- Minimum password age; and
- Number of invalid login attempts.

Additionally, the security software passwords are maintained as encrypted values within the system security database.

For agencies that do not have a Security Software coordinator, the Department conducts the Security Software coordinator activities on their behalf (proxy agencies). Agencies with a Security Software coordinator are responsible for monitoring/reviewing the security software accounts assigned to their agency.

On an annual basis, the Security Software coordinator sends proxy agencies and the Department a listing of security software IDs assigned to their agency and the Department for review. The agencies and the Department are to review the listing and provide a response back to the Security Software coordinator stating the IDs are appropriate or indication which IDs are to be revoked, re-assigned or deleted. Proxy agencies are responsible for reviewing the appropriateness of their agencies security software accounts and responding to the Security Software Coordinator or designee. Additionally, on a monthly basis, the Security Software coordinator or designee runs a report documenting the Department and the proxy agencies' security software IDs which have not been utilized in the past 90-days; upon review, the IDs are revoked.

The Security Software coordinator or designee runs a weekly violation report which is reviewed for invalid and unauthorized access attempts of the Department and proxy agency security software IDs. The Security Software coordinator follows up with the review results as stated in the Security Violation Report Procedure. The Security Software coordinator or designee contacts the individual or their supervisor to determine the reason for the violation.

Semi-monthly, the Security Software coordinator receives a separation report from the Security Software system. The Security Software coordinator or designee reviews the separation reports, noting separation of individuals from the Department and proxy agencies. If a separation is noted, the Security Software coordinator will revoke the individual's security software ID.

System Security-Midrange
The Department utilizes Active Directory as its method for controlling and monitoring access to the midrange resources.

In order to access the midrange environment, an ID and password are required. Password security parameters have been established and configured to ensure access to midrange resources is appropriate:

- Minimum password length;
- Password complexity;
- Password history;
- Minimum password age; and
- Number of invalid login attempts.

The Department performs a monthly review of Illinois.gov Active Directory accounts and

disables accounts which have been dormant for 60 days. Agencies are provided a listing of the disabled accounts instructing them to review and take appropriate actions to keep accounts active. In the event the agency determines the account is no longer needed, they are instructed to submit a Remedy service request for removal of the account. The stale account will remain disabled, and if the agency does not provide a response, the account will be automatically deleted after 90 days from the Department's disable notification. Deletion of accounts was temporarily suspended as of May 2020, due to COVID-19 crisis and State employees working remotely.

Agencies are responsible for reviewing AD accounts that have been dormant for 60 or more days and taking appropriate actions to keep accounts active.

Administrators

System Administrators-Mainframe

Access to the operating system configurations is limited to system support staff. Access with powerful privileges, high-level access and access to sensitive system functions is restricted to authorized personnel. To request access, the Department access provisioning process is to be followed.

System Administrators-Midrange

Access to administer the midrange environment is limited to authorized technical support personnel. To request access, the Department's access provisioning process is to be followed.

On an annual basis, the Department's Security Compliance team sends a list of the technical accounts to appropriate supervisors. The supervisor of the technical account owner is requested to review and update continued access. In the event the technical account is no longer required, a Remedy ticket is submitted by the immediate supervisor or their designee to deactivate the account. Unused accounts are deactivated after 60 days of inactivity. Review results from responsible supervisors are documented.

Application Administrators/Programmers

Access to application source code, Job Control Language (JCL) streams, data files and sensitive application functions are restricted to authorized personnel. To request access, the Department's access provisioning process is followed. Revoking access is initiated upon receipt of Remedy service request or, under special or emergency circumstances, by instruction of the Department senior management.

The Security Software Coordinator conducts annual reviews of the Department security software ID access.

Network Services

Network Services is comprised of three areas of responsibility;

- Local Area Network Services is responsible for managing firewalls, switches, servers, and software that are the components to the local area network.
- Agency Wide Area Network Services is responsible for managing firewalls, routers, switches, servers, and software that are the components to the wide area network and virtual private network infrastructures.

- Backbone Wide Area Network is responsible for managing wave equipment, firewalls, routers, switches, cabling, servers, and software that are the components to the backbone, wide area network as well as peering and Internet Access (Illinois Century Network).

Common Controls

- Mandatory backbone design and configuration standards and guides are defined and maintained.
- A security banner serves as a security awareness mechanism and is displayed at initial network connection warning of prosecution for unauthorized access.
- Modification to the network is restricted to Department authorized technicians and authorized vendors.
- Authorization and access rights to a network-attached device by either a Department technician or vendor specialist requires assignment of an Active Directory account, inclusion in a specific access-rights group, and use of a Department issued token before network access is granted. Access requests are made through Remedy on Demand, and follows the Department access provisioning process. Active Directory is used as the centralized user and password authenticator.
- Active Directory accounts are assigned and issued through the Department's access provisioning procedures. Department staff with a business need to access or modify network devices are added to a designated Active Directory access group and setup with a two-factor authentication token. A token is issued to only authorized staff which requires supervisor approval. Once the supervisor request for multifactor authentication is received by the two factor administrators via email, administrators and the supervisor will work together on assigning and configuring the two factor authentication. Two factor authentication activation and revocation is tracked by the individual supervisor. Tokens serve as a secondary confirmation and utilized once AD credentials are validated as the first step in authentication. If the AD account is disabled or deactivated the token is rendered ineffective and useless for authentication purposes. Token remains inactive until a challenge/response procedure is successfully completed. This procedure requires the Department's Two-Factor Authentication Administrator communicate certain information to the technician in real time to activate the token.
- Additional security measures are applied through use of Access Control Lists and Authentication Servers. Access Control Lists reside on the network device itself and restrict communication to only certain IP addresses or address ranges.
- Authentication Servers control access through assignment of access right privileges (read only or update) based on Department-defined group profiles.
- The Department applies self-monitoring hardware and software, redundant backbone construction, scheduled backups, and vendor-based services to maintain network availability.
- Self-monitoring network hardware devices record all events and forward to multiple logging servers. These servers use filters to automatically generate alerts when a Network Services' configured parameter or condition occurs.
- Network diagrams depict common connectivity configurations.

Local Area Network (LAN)

The Department has implemented redundancy in the Data Center LANs and at agency locations

where technically, fiscally, and operationally feasible. Infrastructure component equipment is physically located at either Department facilities or on agency premises.

Network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to LAN Services Support staff and a console display alert when a predefined event occurs, or a threshold is reached. LAN Services Support staff follow up on these alerts and engage operational teams for resolution as necessary. Alerts are tracked in the Network monitoring system.

Authentication Server records failed login attempts to the network equipment. Logs are imported into the Department's security information and event management tool for archival, historical, or investigative purposes upon request.

Data Center firewall and switch configurations have incremental backups performed twice a day that are stored for a minimum of 60 days at the Central Computing Facility (CCF) and Alternate Data Center (ADC). LAN access switch configurations are saved on a network management server, which verifies device configuration revisions daily, and new configurations are backed up when detected. Configurations saved on the network management server are backed up daily to the CCF and the ADC.

Agency Wide Area Network (WAN)
The Department has implemented last mile redundancy where technically, fiscally, and operationally feasible. Infrastructure component equipment is physically located at either Department facilities or on agency premises.

Network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to the 24x7x365 Network Operations Center and / or console display alert when a predefined event occurs, or a threshold is reached. The 24x7x365 Network Operations Center determines if further action is required and engages operational teams for resolution as necessary. 24x7x365 Network Operation Center staff reviews each occurrence and engage operation teams for resolution.

Authentication Server records failed login attempts to the network equipment. Failed attempts are stored and recorded within the authentication server. This server automatically generates an email notification which is forwarded to Network Design & Engineering staff to determine, on a case by case basis, if further action is required.
Virtual Private Networks (VPN) provide controlled and trusted connections between devices when required for data traversing public networks including the Internet. The Department's Enterprise VPN Standard provides guidance when establishing a VPN connection. When data travels across a public network, it is encrypted at the access router and while in transit across the public network until it reaches the distribution router and enters the private network.

Device configurations are saved on network management server, which verifies device configuration revisions daily, and new configurations are backed up when detected. Configurations saved on the network management server are backed up daily to the CCF and the ADC through the midrange backup system.

Backbone Wide Area Network (WAN)
Infrastructure component equipment is physically located either at Department facilities or on agency premises. The Department has implemented redundancy between Point of Presence sites where technically, fiscally, and operationally feasible and has also installed fiber optic wave transmission technologies to provide high speed backbone transport services.

Network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to the 24x7x365 Network Operations Center and / or console display alert when a predefined event occurs or a threshold is reached. The 24x7x365 Network Operations Center determines if further action is required and engages operational teams for resolution as necessary. Alerts are tracked in the Network monitoring system.

Authentication Servers record failed login attempts to the network equipment. Failed attempts are stored and recorded within the authentication server. This server automatically generate an email notification which is forwarded to Network Design & Engineering staff to determine, on a case by case basis, if further action is required.

Device configurations are saved on a network management server, which verifies device configuration revisions daily, and new configurations are backed up when detected. Configurations saved on the network management server are backed up daily to the CCF and the ADC through the midrange backup system.

Security Operations Center
The Security Operations Center continuously monitors the network for the detection and analysis of potential intrusions, cybersecurity threats, and incidents. Depending on the threat, the Security Operation Center has established Standard Operating Procedures to assist with the detection, analysis and resolution.

Upon notification of a threat, the Department follows the Cyber Security Incident Response Plan.

Additionally, weekly activity reports which document a summary of the incidents noted during the week, and their resolutions are available to management.

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

Linux patches every 90 days, while VMware and Unix (AIX) patches are scheduled as needed and provided by the vendor. All patches are reviewed and tested by technicians before pushing out. The Department's Change Management Process is followed to patch all the operating systems.

The End Point Protection Group is responsible for pushing definitions and other antivirus software updates out. A tool is applied to manage definitions and antivirus software updates. The

tool is used to automatically push virus definition files to all systems after receipt from antivirus vendors. The endpoint protection group has tools available to monitor the state of systems and detect systems which fail to load updates and are not running the latest supported version. The End Point Protection group follows the Department's Change Management Process to bring these systems up to date. Additionally, agencies are responsible for notifying the Department of actual or suspected information security breaches, compromised accounts, or unauthorized access.

Computer Operations

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

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

The Daily Shift Report documents the activity conducted on mainframe production systems and incident calls received at the Operations Center. The Report contains the date, time, system involved in the incident, along with a narrative providing any necessary information regarding the incident. The Report is forwarded to Enterprise Infrastructure management and supervisors for awareness and follow-up of outstanding issues.

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

The Operator Shift Change Checklist (an action list shared between shifts) is completed at the beginning of each shift to ensure the production systems are operating appropriately and any open items are passed on to the next shift and to identify any changes which need to be made. The Operator Shift Change Checklist are signed off by Operations Center supervisors.

Mainframe

The mainframe environment is monitored through the z/OS systems console for errors and issues. Operations Center continuously monitors the system console.

Mainframe system performance and capacity is monitored by System Software programming personnel, via Resource Measurement Facility reports which are run daily and monthly. Performance and capacity monitoring are documented via internal memorandum distributed via email to Enterprise Infrastructure management monthly.

The Department has implemented system options to protect resources and data. The System Management Facility records operating system activities. The System Coordinator runs a System Management Facility violation report weekly for review and signs off on the report after resolving any unusual violations. The System Coordinator and Mainframe manager review a high-level systems programmer user ID listing on an annual basis. It is signed off on by both

after the listing is deemed to be correct, or modifications have been made to the Mainframe System Security Software user IDs.

The Department has developed the operations manuals to provide staff with instruction related to their various tasks.

Midrange

Midrange availability is monitored by the Operations Command Center via the What's Up Gold system. Command Center technicians notify System and/or Storage technicians of What's Up Gold alerts.

Structured Query Language (SQL) database servers use the Idera tool set for additional monitoring. The Idera system alerts have been set up to generate emails to SQL support staff. The SQL support staff use the Idera tools to help trouble shoot SQL issues.

The Active Directory Domain Controllers use Microsoft System Center for additional monitoring. System Center alerts have been set up to email alerts to AD support staff. The AD staff uses Microsoft System Center to help trouble shoot AD issues.

Data Storage

Data Storage performance and capacity are monitored using EMC Toolsets. When there is an equipment outage or performance issues, Data Storage Technicians contact the equipment or software vendor. Automated alerts are sent via email to Data Storage Technicians and management when capacity is reached or exceeds 80%. Mid-Range System Data Backups are monitored by EMC tools and IBM Spectrum Protect.

The secure, encrypted transfer of mainframe data is achieved using the File Transfer Protocol Secure (FTPS). The software MOVEit is used to transmit midrange data between servers and applications. The MOVEit software sends email alerts for any failures to Department and agency support staff. The Department and / or Agency support staff review the email alerts and determine if further action is required. Formal review documentation is not maintained due to large amount of alerts received, and tasks can be initiated by multiple teams. Access to MOVEit systems are reviewed and followed up on an annual basis by the Department's Midrange Wintel Group.

Another option available to valid Illinois.gov users for the secure transmission of data is the file transfer utility 'FileT'. This utility uses random key generation to access files stored on a server. Only those with a valid key may download files from the server. Files are automatically purged from the server after 5 days. The sender must acknowledge a warning of unauthorized access message by clicking a box before transfer is allowed. The sender receives a confirmation message containing a link to the transfer status as well as a link to remove the file from the server if necessary. A valid Illinois.gov email address is required to use this utility for State resources; either as the recipient or the sender.

Backups

Mainframe
The Department is responsible for the scheduling and monitoring of the backup process except for the agency database data and applications. Agencies are responsible for scheduling the backups of their applications and database data. Agencies are responsible for informing the Department of their business needs. Data on mainframe systems are backed up daily and weekly utilizing Virtual Tape Technology (Disk Library Management (DLM)). The Department utilizes CA Scheduler to schedule and verify the completion of the backups.

The Department has implemented backup procedures to assist staff in the event of failures.

Daily, Storage staff review the output of the daily backup jobs for any failures. In the event of a mainframe daily backup job failure, the Operations Center staff records the incident in the Shift Report. The next working day, Storage staff review the Shift Report to identify the problem, correct and resubmit the failed portion of the backup job.

The Storage staff review the output of the weekly backup jobs for success or failure. The failure is researched and corrected, and then the failed portion of the backup job is resubmitted for completion.

Data replication is performed between the CCF and the ADC. Mainframe data replication occurs every 15 minutes between the CCF and the ADC DLM. The monitoring software sends the Enterprise Storage and Backup group an alert if the data is out of sync for more than 24 hours. If there is an issue, a Remedy ticket is submitted to track the Enterprise Storage and Backup group's progress on resolution of the issue.

The DLM Replicated Status log keeps a log of replication between the two DLMs and tracks library replication outcomes for DLM replication activity. These logs document the status of the replicated Data Domain pool and the time of the last sync and are maintained for seven days. The Storage staff reviews, and corrects any issues.

Midrange
Spectrum Protect and Avamar are used to back up the midrange environment. Data Protection Advisor is used to monitor and report on midrange backups. Midrange server backups are performed daily or weekly and are either incremental or full. Spectrum Protect and Data Protection Advisor automatically generate daily reports indicating the backup status of scheduled jobs from the prior day. These daily reports are emailed to the Enterprise Storage and Backup group who then investigates the cause of failures and works to resolve the problem.

Backed up server data is written to a Data Domain storage system and then replicated to another Data Domain storage system at the ADC. The Data Domain storage systems generate a daily status report which is emailed to the Enterprise Storage and Backup group. The Data Domain storage systems also send email alerts to the Enterprise Storage and Backup group when issues arise that may need additional attention. Enterprise Storage and Backup group investigate the issue until a satisfactory conclusion is reached. The Data Domain systems automatically alert vendor support in the event of hardware or system failures.

The Data Domain storage systems are also a target for SQL, DB2, and Oracle backups. The database backups are written to the Data Domain storage systems via Common Internet File System or Network File System and then replicated to the ADC. It is the responsibility of the database administrators to perform and monitor the success of the database backups.

A PowerShell script goes through the production SQL servers and creates a report with the latest backup date and it is sent to the SQL team daily. The SQL team reviews it and follows up for any failures. The SQL team also gets alerts from the SQL servers when backup jobs fail. Additionally, the SQL team receives alerts from the Idera monitoring software if a database has missed a backup.

Any data, including, but not limited to SQL, Access, DB2 databases, user shared documents and user profiles are located on the Isilon storage device via the Network File System or the Service Message Block shares. The Enterprise Storage and Backup group has policies on the Isilon that take daily snapshots of all shares which are then retained up to 60 days. The Isilon also has daily synchronization with the ADC to another Isilon storage system. The Isilon generates a daily report showing successful and failed synchronization attempts with the ADC. Enterprise Storage and Backup group investigate failed synchronization attempts until a satisfactory conclusion is reached. The Isilon has a call home feature that notifies vendor support. For critical issues, the Isilon call home feature additionally notifies the Enterprise Storage and Backup group.

Physical Security

The Department's warehouse physical security is managed by cameras and badge proximity readers that are installed at the front and rear entrances and at the dock doors. Dock door badge readers operate from inside the building only. Authorized badged individuals may enter the Warehouse or End User Computing (EUC) areas through swiping of a Velocity badge. Visitors alert Warehouse or EUC staff who then unlock the door. A visitor's log captures who enters the building. Unescorted access is permitted when appropriate, as determined by Warehouse or EUC staff, and for maintenance personnel.

For the Department's Communication Center and CCF, security guards monitor 24x7x365, proximity badge readers located at various interior and exterior entry points, security alarms, and cameras. Individuals not registered in the Velocity system (no permanent badge issued) must present proof of identification and sign the visitor register log at the guard station to obtain a visitor badge. Visitors are required to be escorted while in either building. For individuals registered in the Velocity system but not having a permanent badge immediately available, guards issue a temporary badge upon proof of identification. Temporary badges are also issued to approved vendors once identification has been validated by the facility security guard. Temporary badges allow movement within the building without escort.

Additional physical restrictions and levels of access are applied at the CCF to the area housing computing processing and storage equipment. Access to this secured area is limited to a small group of individuals with specific business need and requires special badge permission to exit the elevator or enter through the stairway door. Surveillance is enhanced with additional cameras and door sensors.

Midrange Wintel Manager or designee conducts monthly review of individuals who were granted access or removed access from the previous month to the CCF highly secured area to ensure proper access is being granted. Review results are documented.

From July 2019 to November 2019, the Department Security team was developing a repeatable process utilizing Central Management Services Security Section Person Access by Door reports for reviewing physical door access to the Communication Center and CCF highly secured area. The Department's Security team conducts a physical access review each calendar quarter for Communication Center. The first review was conducted in February 2020. Starting in December 2019, Department's Security team conducts monthly CCF highly secured area physical access review. Effective January 1, 2020, Physical Access Door Group Review Procedure was created to reflect the current physical access review process. Security team documents the review results from responsible managers, and identified improper access is sent to HR for removal. HR sends a confirmation email to the Security team after access is removed, and the email is stored on the Department shared drive.

The Department uses the Hirsh/Velocity Access Control System (Velocity) to create and maintain badges that allow physical access to a Department building, floor, or room with the exception of the James R. Thompson Center (JRTC). For DoIT employees based at the JRTC, ISP Protective Services Unit is responsible for all badging tasks associated with JRTC access. Badges display the badge holder's photo, date of issuance, date of expiration and are color coded to show affiliation of employee (blue border) or contractor (yellow border). Velocity captures dates, times, and doors when a badge is swiped.

To obtain a badge, the DoIT Badging Process is to be followed. The Department's process requires HR to be in receipt of a DoIT Badge Request form. HR maintains a list of roles authorized to request badge action be taken. The form facilitates a request for several types of badging tasks, including creation of a new badge, a change in access needs, renewal of an expiring badge, replacement of a broken/lost badge, a name change or deactivation. The form requires entries regarding requestor, badge holder, reason for access, and access needs. Badge tasks may be requested for Department employees, non-Department employees and contractors. Access to the Department occupied facilities may be granted by the Department HR through badges issued by other state agencies.

Valid proof of identity and a photo are required for creation of a new badge. For non-state employees, documentation of a clear background check, performed in the past five years, must be provided prior to initial badge issuance.
Valid proof of identity and a photo supplied within the last 12 months are required for creation of a renewal or replacement badge.

Access requested for the CCF highly secured area requires approval from those designated as approvers for the secured area. HR maintains a list of roles authorized to provide approval.

Upon review of the DoIT Badge Request form, HR processes the badge task using the Velocity system.

Badge access is revoked by the Velocity system at badge expiration date. HR may manually deactivate badge access after official notice of separation/termination is provided. Effective January 2, 2020, a DoIT Badge Request form will then be supplied by an individual in the respective authorized role (list of authorized roles maintained by HR) to document the action taken.

Creation of badges was temporarily suspended as of March 17, 2020 due to the Governor's Executive Order 2020-10 requiring all individuals to stay at home due to the COVID-19 pandemic. Due to work being performed remotely in accordance with COVID-19, newly-hired permanent employees, 75-day employees, contractors and vendors who need access to the Department facilities will be assigned visitor badges requiring escort until such time as a badge can be created. Permanent employees, 75-day employees, contractors and vendors who need a replacement badge (due to either a broken or expired badge) will be assigned visitor badges requiring escort until such time as a replacement badge can be created.

Complementary Subservice Organization Controls

The Department's controls related to the Information Technology General Controls and Application Controls cover only a portion of the overall internal control for each user entity. It is not feasible for the control objectives related to the Information Technology General Controls and Application Controls to be achieved solely by the Department. Therefore, each user entities' internal control over financial reporting must be evaluated in conjunction with the Department's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization described below.

1) Controls are implemented to provide IT managed services which are performed in accordance with contracts.

2) Controls are implemented to provide assurance that access to networks and applications is approved, reviewed periodically, and access is terminated timely.

3) Controls are implemented to provide reasonable assurance that only authorized personnel are able to make changes to network and applications.

4) Controls are implemented to provide reasonable assurance that updates to networks and applications are documented, approved, and tested prior to implementation.

5) Control are implemented to provide adequate security around the network and application operations.

6) Controls are implemented to address incidents that are identified, tracked, resolved and closed in a timely manner.

Complementary User Agency Controls

The Department of Innovation and Technology's controls related to the Information Technology Shared Services system for the information technology general controls and application controls cover only a portion of the overall internal control structure for each user entity of the Department of Innovation and Technology. It is not feasible for the control objectives related to Information Technology Shared Services system for the information technology general controls and application controls to be achieved solely by the Department of Innovation and Technology. Therefore, each entity's internal control over financial reporting must be evaluated in conjunction with the Department of Innovation and Technology's controls and the related tests and results described in Section IV of this report, taking into account the related complementary user entity controls identified under each control objective, where applicable. In order for entities to rely on the control reported on herein, each user entity must evaluate its own internal control structure to determine if the identified complementary user entity controls are in place.

Control Objective	Complementary User Entity Controls
Risk Assessment	Agencies are responsible for providing mitigation plans corresponding to risk assessment results.
Vulnerability Scan	Agencies are responsible for providing corrective action plans to remediate identified server vulnerabilities.
#1	Agencies are responsible for the complete and accurate entry and maintenance of data into the applications.
#2	Agencies are responsible for reviewing the payroll voucher to ensure the accurate calculation of deductions.
#3	Agencies are responsible for submission of a Remedy ticket documenting issues and needs of the environment and applications.
#4	Agencies are responsible for reporting incidents to the IT Service Desk.
#4	Agencies are responsible for reporting lost or stolen equipment to the IT Service Desk.
#5	Agency ATSRs are responsible for the submission of an approved Remedy service request for the creation, modification, and termination of user access.
#5	For the creation of a security software account, agencies are responsible for the submission of an approved service request or Mainframe request form if Remedy service request is not available for the agency.
#5	Agencies are responsible for the submission of an approved Remedy service request for the establishment of the agency Application Administrator.
#5	Agencies are responsible for the submission of an approved Remedy service request for the establishment of an eTime Administrator.
#5	Agency Application Administrator is responsible for assignment of their agency's application specific accounts, associated rights and privileges, password management, and deactivation or reassignment.
#5	Agencies are responsible for ensuring proper segregation of duties in the assignment of application user access rights.
#5	Agencies are responsible for reviewing the user access rights to their data.
#5	Agencies are responsible for managing eTime and review the user access rights to their data.

Provided by the Department of Innovation and Technology

#5	Agency's timekeeper is responsible for entry and maintenance of an employee's time and attendance; vacation, sick, personal, etc.
#5	Agencies are responsible for contacting the IT Service Desk or the utilization of the self-service options, in order to reset the AD or Novell accounts.
#5	Proxy agencies are responsible for reviewing the appropriateness of their agencies security software accounts and responding to the Security Software Coordinator or designee.
#5	Agencies with a Security Software Coordinator are responsible for monitoring/reviewing the security software accounts assigned to their agency.
#5	Agencies are responsible for reviewing AD accounts that have been dormant for 60 or more days and taking appropriate actions to keep accounts active.
#5	Agencies are responsible for scheduling the backups of their applications and database data.
#5	Agencies are responsible for informing the Department of business needs.

Objectives and Related Controls

The Department of Innovation and Technology has specified the control objectives and identified the controls that are designed to achieve the related control objectives. The specified control objectives, related controls, and the complementary user agency controls are presented in section IV, "Description of the Department of Innovation and Technology's Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results", and are an integral component of the Department of Innovation and Technology's description of Information Technology Shared Services System for the information technology general controls and application controls.

SECTION IV

DESCRIPTION OF THE DEPARTMENT OF INNOVATION AND TECHNOLOGY'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND THE INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

Description of the Department of Innovation and Technology's Control Objectives and Related Controls, and the Independent Service Auditor's Description of Tests of Controls and Results

Information Provided by the Independent Service Auditor

This report, when combined with an understanding of the controls at the user agencies, is intended to assist auditors in planning the audit of user agencies' financial statements or user agencies' internal control over financial reporting and in assessing control risk for assertions in user agencies' financial statements that may be affected by controls at the Department of Innovation and Technology.

Our examination was limited to the control objectives and related controls specified by the Department of Innovation and Technology in Sections III and IV of the report, and did not extend to controls in effect at the user agencies.

It is the responsibility of each user agency and its independent auditor to evaluate this information in conjunction with the evaluation on internal control over financial reporting at the user agencies in order to assess total internal control. If internal control is not effective at the user agencies, the Department of Innovation and Technology's controls may not compensate for such weaknesses.

The Department of Innovation and Technology's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of controls specified by the Department of Innovation and Technology. In planning the nature, timing, and the extent of our testing of the controls to achieve the control objectives specified by the Department of Innovation and Technology, we considered aspects of the Department of Innovation and Technology's control environment, risk assessment process, monitoring activities, and information and communication.

The following table clarifies certain terms used in this section to describe the nature of tests performed:

Test	Description
Inquiry	Inquiry of personnel and management.
Observation	Observation, performance, or existence of the control.
Inspection/Reviewed	Inspection/review of documents and reports indicating performance of the control.

In addition, as required by paragraph .35 of AT-C Section 205, *Examination Engagements* (AICPA, *Professional Standards*), and paragraph .30 of AT-C Section 320, when using information produced or provided by the Department of Innovation and Technology, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Control Environment Objective 1: Controls provide reasonable assurance that policies and procedures related to employee responsibilities and hiring have been established, new employees and contractors are screened and on-boarded, and a defined organizational structure exists, that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
CE1.1	The organizational hierarchy promotes separation of duties, monitoring of controls and customer support.	Reviewed the organizational chart to determine if appropriate segregation of duties, monitoring and customer support are promoted.	No deviations noted.
CE1.2	The hiring practices adhere to legal requirements as published in the State Personnel Code, Personnel Rules, union contracts, *Rutan/Shakman* decisions, court orders and applicable state/federal laws.	Reviewed the hiring procedures, Personnel Code, union contract, *Rutan/Shakman* decisions, court orders, and applicable federal and State laws to determine hiring process.	No deviations noted.
CE1.3	Vendor contractors are hired based on contract requirements, which follow Illinois procurement regulations.	Reviewed contract requirements and Illinois procurement regulations.	No deviations noted.
CE1.4	Each employee position has an approved formal written job description which documents the duties, responsibilities, qualifications, minimum acceptable competency education requirements, and experience levels.	Selected a sample of employee positions to determine if a job description had been completed and approved.	No deviations noted.
		Selected a sample of job descriptions to determine if they outlined duties and qualifications.	No deviations noted.
CE1.5	New employee and personal service contractors must pass a background check prior to being offered employment.	Selected a sample of new employees and personal service contractors to determine if background checks were completed prior to being offered employment.	No deviations noted.
CE1.6	Performance evaluations for new employees serving a four month probationary period are completed two weeks prior to the end of their probationary period.	Selected a sample of employees serving a four month probationary period to determine if applicable probationary evaluations had been completed.	34 of 38 selected employees' probationary evaluations were completed between 14 to 262 days late.

CE1.7	Performance evaluations are completed at the end of the three months and six months for employees serving a six months probationary period.	Selected a sample of employees serving six month probationary periods to determine if the three and six months probationary evaluations had been completed.	19 of 22 selected employees' probationary evaluations were completed between 3 and 152 days late.
CE1.8	Certified employee performance evaluations are completed annually.	Selected a sample of employees to determine if an annual evaluation had been completed.	31 of 60 selected employees' annual evaluations were completed between 6 and 204 days late.
CE1.9	Newly-hired employees are provided the DCMS' Policy Manual and are required to sign an acknowledgment form acknowledging responsibility to abide by the policies contained within the DCMS Policy Manual.	Selected a sample of new employees to determine if the DCMS Policy Manual acknowledgement had been signed.	No deviations noted.
CE1.10	Personal service contractors acknowledge and accept compliance with Department policies and procedures, as each contract states that the "contract employee agrees to be bound by and comply with policies and procedures of the Agency."	Selected a sample of personal service contractors to determine if the contract contained the clause the "contract employee agrees to be bound by and comply with policies and procedures of the Agency."	No deviations noted.
CE1.11	Newly-hired employees and PSCs are directed to complete the Security Awareness Training, Safeguard Disclosure Training, Ethics Training, and Sexual Harassment Prevention Training for State Employees and Acceptable Use Policy effective September 2019. An acknowledgement is generated at the end of each training.	Selected a sample of employees and personal services contractors to determine if annual Security Awareness training, Safeguards Disclosure training, Ethic training, and Sexual Harassment Prevention training and Acceptable Use Policy acknowledgement had been completed.	No deviations noted.
CE1.12	Employees and PSCs acknowledge awareness of responsibilities through affirming to follow policies as referenced above and through mandated annual calendar year training covering Security Awareness, Safeguard Disclosure, Ethics, and Sexual Harassment Prevention.	Selected a sample of employees and contractors to determine if they had completed the annual Security Awareness training, Safeguard Disclosure training, and Ethics training and Sexual Harassment Prevention training.	Ethics training was not conducted during the examination period. Therefore, the Service Auditor was unable to test the operating effectiveness of the control. 6 of 1,505 required employees and contractors selected did not complete the Safeguard Disclosure training.

			3 of 1,429 required employees and contractors selected did not complete the Security Awareness training. No deviations noted with Sexual Harassment Prevention training.
CE1.13	An Employee Exit form and a Remedy Service Request are completed to ensure remove of access and retrieval of equipment for employees and contractors.	Selected a sample of terminated employees and contractors to determine if an Exit form and Remedy Service Request had been completed for employees and contractors.	2 of 31 terminated employees selected did not have a Remedy Service Request completed. There were no deviations noted in testing of the Exit form.

Control Objective 1: Controls provide reasonable assurance that invalid transactions and errors that are relevant to user entities' internal control over financial reporting are identified, rejected, and correctly reentered into the application in a timely manner.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C1.1	The applications have edit features designed to reject erroneous or invalid data. When erroneous or invalid data is entered, an error message will appear on the screen and the field will be highlighted.	Selected a sample of field edits to determine if they were functioning appropriately and error notifications appeared.	No deviations noted.
C1.2	Separate, stand-alone user manuals and guides are available for the AIS, CIS, CPS, and CTAS applications.	Reviewed user manuals to determine if they provided guidance to users.	No deviations noted.
C1.3	User instructions and guides are imbedded into the application itself for eTime.	Reviewed instructions and guides to determine if they provided guidance to users.	No deviations noted.

Control Objective 2: Controls provide reasonable assurance that appropriate federal and state specifications are used for tax calculations during processing, that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C2.1	The Department's CPS staff modifies federal tax tables accordingly.	Selected a sample of federal tax rates to determine if the rates had been updated within CPS.	No deviations noted.
	The CPS staff receives email notification from a procured service that identifies state tax rate changes.	Selected a sample of state tax rates to determine if the rates had been updated within CPS.	1 of 6 state tax rates were incorrect. The State of Illinois' tax rate was correct.

Control Objective 3: Controls provide reasonable assurance that application programs and environment changes are properly authorized, tested, approved and implemented to result in complete, accurate, and timely processing and reporting that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C3.1	Control over changes to the network, mainframe, mainframe patching and midrange infrastructures as well as to data storage devices are documented in the Change Management Process Guide, ROD Change Management Guide, and the Change Management User Guide.	Reviewed the Change Management Process Guide, ROD Change Management Guide, and the Change Management User Guide to determine if controls were documented.	The Change Management Process Guide did not contain information on the change freeze process.
C3.2	Significant or extensive impact changes require test, implementation, and backout information to be provided with the change request.	Selected a sample of significant or extensive impact changes to determine if test, implementation, and backout information was provided with the change request.	4 of 60 significant or extensive changes selected did not contain a test plan. 5 of 60 significant or extensive changes selected did not contain a backout plan. 5 of 60 significant or extensive changes selected did not contain a implementation plan.
C3.3	Emergency changes require a Post Implementation Review be provided within the change request.	Reviewed a sample of emergency changes to determine if a Post Implementation Review was provided within the change request.	2 of 19 emergency changes selected did not have a Post Implementation Review conducted.

			1 of 19 emergency changes selected was created and approved by the same individual.
C3.4	Change requests are classified into class and impact categories with approval levels of Support Group Manager, Enterprise Change Manager, and the Change Advisory Committee.	Reviewed a sample of changes to determine if the change was properly approved based on its class and impact categories.	1 of 61 changes selected had a class of "expedited" which was not addressed in the change management policies. 1 of 61 changes selected was improperly categorized as "no impact" instead of "significant."
C3.5	For application changes, processing steps are documented in the Application Lifecycle Management Manual, EAA Mainframe Change Management Procedures, and the EAA Distributed Change Management Procedures.	Reviewed the Application Lifecycle Management Manual, EAA Mainframe Change Management Procedures, and the EAA Distributed Change Management Procedures to determine if they documented the change management procedures.	No deviations noted.
C3.6	An application change is initiated with the submission from an authorized ATSR or Department IT Coordinator or internal support staff of a Remedy request which then follows enterprise change management procedures and processes described within.	Selected a sample of application changes to determine if a Remedy request had been submitted and if the change followed the enterprise change management procedures and processes.	No deviations noted.

C3.7	For mainframe application changes, a revision control and code management system permit a developer to "checkout" program code while prohibiting modified code from being placed back into the production area without proper authorization.	Selected a sample of mainframe changes to determine if proper authorization was obtained prior to placing in the code management system.	No deviations noted.
C3.8	Moves to the mainframe production environment are completed by Library Services, based on instruction within the approved move sheet.	Selected a sample of changes to determine if Library Services completed the moves to the mainframe production environment based on approved move sheets.	No deviations noted.
C3.9	Developers are limited to read only access to the Production Libraries.	Reviewed developers' access to determine if their access to the production libraries was read only.	No deviations noted.
C3.10	For distributed systems, Remedy’s built-in workflow approval process requires supervisory approval prior to deployment into the production environment.	Selected a sample of changes to determine if the supervisor approved the request for deployment into the production environment.	No deviations noted.
C3.11	Designated release staff, who did not code the change, can move the change into the production environment manually, and developers who coded the changes verify the changes to ensure accuracy, or via an automated release management module if configured, with supervisor approval.	Selected a sample of changes to determine if a developer who did not code the change completed the move to the production environment.	No deviations noted.

Control Objective 4: Controls provide reasonable assurance the entities' calls that are relevant to user entities' internal control over financial reporting are responded to, tracked, and resolved in a timely manner.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C4.1	The Incident Management Process Guide documents Department workflow and remediation processes for incident management.	Reviewed the Incident Management Response Process Guide to determine if it documented the workflow and remediation process of reported incidents.	No deviations noted.
C4.2	Reported incidents are tracked via a Remedy ticket until appropriate remediation efforts are completed.	Reviewed Remedy to determine if incidents were tracked until remediation efforts were completed.	No deviations noted.
C4.3	The IT Service Desk initiates a Remedy ticket to track and document the event that captures the asset property tag, the user reporting the loss, and any police reports if available.	Reviewed Remedy to determine if missing or stolen equipment was tracked.	No deviations noted.
C4.4	An encryption protection feature is installed as part of laptop imaging prior to deployment.	Selected a sample of stolen and missing laptops to determine if verification of the installation of encryption was completed.	2 of 6 stolen and missing laptops selected did not have verification that encryption was installed.

C4.5	If encryption is inactive or was not installed as part of the device imaging process prior to deployment, EUC Image Management will assign the ticket to the SOC who will enact a breach investigation that consists of steps outlined in their Security Incident Playbook.	Selected a sample of stolen and missing laptops which did not have encryption installed to determine if the Security Operations Center enacted a breach investigation.	The Department did not report any unencrypted laptops stolen or missing. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

Control Objective 5: Controls provide reasonable assurance that logical access to applications, data, and the environment is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
	Access Provisioning		
C5.1	The Department policies titled Identification and Authentication Policy, Personnel Security Policy, Access Control Policy and Configuration Management Policy address logical security and are published on the Department's website.	Reviewed the Identification and Authentication Policy, Personnel Security Policy, Access Control Policy, and Configuration Management Policy to determine if they documented logical security controls.	No deviations noted.
		Reviewed the Department's website to determine if the Identification and Authentication Policy, Personnel Security Policy, Access Control Policy, and Configuration Management Policy had been published.	No deviations noted.
C5.2	Access or modifications to Department resources (network, shared services, mainframe processing, and applications) begins with submission of a Remedy service request from an authorized ATSR or Department IT Coordinator.	Selected a sample of new employees and contractors to determine if a Remedy service request was submitted by an authorized ATSR or Department IT Coordinator.	3 of 25 selected new employees' and contractors' Remedy service requests were not submitted by an authorized ATSR or Department IT Coordinator.

			1 of 26 selected new employees and contractors did not have a Remedy service request submitted to obtain access to the Department's resources.
		Selected a sample of access modifications to determine if a service request was authorized by an ATSR or Department IT coordinator.	The Department did not provide a complete and accurate population of access modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.
C5.3	Revoking access is initiated upon receipt of Remedy service request or, under special or emergency circumstances, by instruction of the Department senior management.	Selected a sample of terminated employees and contractors to determine if access was timely terminated.	The Department was unable to provide documentation related to the timely termination of terminated employee and contractors access. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.
	Password Resets-Mainframe		
C5.4	In the event the user requires a reset of their mainframe password, they are required to either submit the request via email to the IT Service Desk or use the Department's self-service option: DoIT Identity Management Tool.	Reviewed the DoIT Identity Management Website to determine solution to reset passwords.	No deviations noted.

C5.5	The IT Service Desk is to verify the individual's ID with the information within the Remedy ticket prior to resetting the password.	Observed the IT Service Desk staff to determine if an individual's identity was verified prior to resetting the password.	No deviations noted.
C5.6	For proxy agencies, the Security Software Coordinator or Security Software Administrator will reset the mainframe password upon receipt of a Remedy request.	Observed the Security Software Coordinator or Security Software Administrator reset the mainframe password upon receipt of a Remedy request.	No deviations noted.
	Active Directory		
C5.7	Active Directory accounts are reset by users calling the IT Service Desk or by one of the Department's self-service options - Microsoft Identity Management (MIM) or the Department's Identity Management (DIM) tool.	Reviewed the DoIT Identity Management Website to determine solutions to reset passwords.	No deviations noted.
C5.8	The IT Service Desk staff will proceed with the reset after verification of two of three pieces of information.	Observed the IT Service Desk staff to determine if an individual's identity was verified.	No deviations noted.
	Novell		
C5.9	The IT Service Desk staff will proceed with the reset after verification of two of three pieces of information.	Observed the IT Service Desk staff to determine if an individual's identity was verified.	No deviations noted.

	Mainframe Security		
C5.10	The security software requires an established ID and password to verify the identity of the individual.	Observed a security software ID and password was required to access the mainframe environment.	No deviations noted.
C5.11	Security software profiles define the level of access a user has.	Observed a security software profile to determine if the profile defined the level of access.	No deviations noted.
C5.12	Password security parameters have been established and configured to ensure access to mainframe resources is appropriate: · Minimum password length; · Password complexity; · Password history; · Minimum password age; and, · Number of invalid login attempts.	Reviewed the system options to determine if password standards had been established.	No deviations noted.
C5.13	Security software passwords are maintained as encrypted values within the system security database.	Reviewed the system options to determine if security software passwords were maintained as encrypted values within the system security database.	No deviations noted.
C5.14	On an annual basis, the Security Software Coordinator sends proxy agencies and the Department a listing of security software IDs assigned to their agency and the Department for review.	Reviewed the annual review of security software IDs to determine if the review had been conducted.	No deviations noted.

C5.15	On a monthly basis, the Security Software Coordinator or designee runs a report documenting the Department and the proxy agencies' security software IDs which have not been utilized in the past 90-days; upon review, the IDs are revoked.	Selected a sample of monthly reports to determine if the IDs had been disabled.	No deviations noted.
C5.16	The Security Software coordinator or designee runs a weekly violation report which is reviewed for invalid and unauthorized access attempts of the Department and proxy agency security software IDs. The Security Software coordinator follows up with the review results as stated in the Security Violation Report Procedure. The Security Software coordinator or designee contacts the individual or their supervisor to determine the reason for the violation.	Selected a sample of weekly reports to determine if the Security Software Coordinator or designee had reviewed and followed up on invalid and unauthorized access attempts.	No deviations noted.
C5.17	Semi-monthly, the Security Software coordinator receives a separation report from the Security Software system. The Security Software coordinator or designee reviews the separation reports, noting separation of individuals from the Department and proxy agencies. If a separation is noted, the Security Software coordinator will revoke the individual's security software ID.	Selected a sample of semi-monthly reports to determine if the Security Software Coordinator had reviewed and revoked the security software IDs for individuals who had separated.	No deviations noted.

	System Administrators-Mainframe		
C5.18	Access to the operating system configurations is limited to system support staff.	Reviewed access rights to the mainframe operating system configurations to determine if access was limited to support staff.	No deviations noted.
C5.19	Access with powerful privileges, high-level access and access to sensitive system functions is restricted to authorized personnel.	Reviewed access rights to powerful privileges, high-level access, and access to sensitive system function to determine if access was limited to authorized personnel.	No deviations noted.
C5.20	To request access as a system administrator, the Department's Remedy access provisioning process is to be followed.	Selected a sample of new system administrators to determine if the Remedy access provisioning process was followed.	The Department did not have a request for a new system administrator. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.
	Midrange Security		
C5.21	In order to access the midrange environment, an ID and password are required.	Observed an ID and password were required to gain access to the environment.	No deviations noted.
C5.22	Password security parameters have been established and configured to ensure access to midrange resources is appropriate: · Minimum password length; · Password complexity;	Reviewed the password parameters to determine whether parameters had been established.	No deviations noted.

	· Password history; · Minimum password age; and, · Number of invalid login attempts.		
C5.23	The Department performs a monthly review of Illinois.gov Active Directory accounts and disables accounts which have been dormant for 60 days.	Selected a sample of monthly reviews to determine if dormant accounts were reviewed.	No deviations noted.
	System Administrators-Midrange		
C5.24	Access to administer the midrange environment is limited to authorized technical support personnel.	Reviewed the midrange environment administrators to determine if their access was appropriate.	No deviations noted.
C5.25	To request access as a system administrator, the Department's access provisioning process is to be followed.	Selected a sample of new system administrators to determine if the Remedy access provisioning process was followed.	The Department did not have a request for a new system administrator. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.
C5.26	On an annual basis, the Department's Security Compliance Team conducts a review of the technical accounts to ensure appropriateness.	Reviewed the annual review to determine if the Security Compliance Team conducted a review of technical accounts.	The annual technical account review controls did not include a defined timeframe for the disabling/deletion of accounts in the event a manager did not respond to the review request.

	Applications		
C5.27	Access to application source code, JCL streams, data files and sensitive application functions are restricted to authorized personnel.	Reviewed administrator access to source code, JCL streams, data files, and sensitive application functions to determine if appropriate.	No deviations noted.
C5.28	Agency Application Administrators are established through ASTR submission of a Remedy service request.	Selected a sample of Agency Application Administrators established during the examination period to determine if a service request was approved by the ASTR.	No deviations noted.
	Network		
C5.29	Mandatory backbone design and configuration standards and guides are defined and maintained.	Reviewed backbone design and configuration standards and guides to determine if they were defined and maintained.	No deviations noted.
C5.30	A security banner serves as a security awareness mechanism and is displayed at initial network connection warning of prosecution for unauthorized access.	Reviewed configurations to determine if a security banner was displayed upon initial connection to the network.	No deviations noted.
C5.31	Modification to the network is restricted to Department authorized technicians and authorized vendors.	Selected a sample of individuals to determine if they were authorized to modify the network.	No deviations noted.

C5.32	Authorization and access rights to a network-attached device by either a Department technician or vendor specialist requires assignment of an Active Directory account, inclusion in a specific access-rights group, and use of a Department issued token before network access is granted.	Selected a sample of individuals with authority to modify the network to determine if they were authorized and utilized a Department issued token.	No deviations noted.
C5.33	Department staff with a business need to access or modify network devices are added to a designated Active Directory access group and setup with a two-factor authentication token.	Selected a sample of individuals with authority to modify the network to determine if they were authorized and utilized a Department issued token.	No deviations noted.
C5.34	Access Control Lists reside on the network device itself and restrict communication to only certain IP addresses or address ranges.	Reviewed configurations to determine if ACLs restrict communications.	No deviations noted.
C5.35	Authentication Servers control access through assignment of access right privileges (read only or update) based on Department-defined group profiles.	Reviewed configurations to determine if Authentication Servers control access.	No deviations noted.
C5.36	Self-monitoring network hardware devices record all events and forwards to multiple logging servers. These servers use filters to automatically generate alerts when a Network Services' configured parameter or condition occurs.	Reviewed hardware devices to determine if they were encoded with filters and if the Network Operations Center were reviewing and resolving alerts received.	No deviations noted.

C5.37	Network diagrams depict common connectivity configurations.	Reviewed network diagrams to determine connectivity configurations.	No deviations noted.
	Local Area Network		
C5.38	The Department has implemented redundancy in Data Center LANs and at agency locations where technically, fiscally, and operationally feasible.	Reviewed configurations to determine if they have been configured for redundancy.	No deviations noted.
C5.39	Network software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. Network hardware and software generates an email to LAN Services Support staff and a console display alert when a predefined event occurs, or a threshold is reached. LAN staff follow up on these alerts and engage operational teams for resolution as necessary.	Reviewed software configurations to determine if emails and alerts were sent when predefined events or thresholds were reached and that LAN Services Support staff followed up on the alerts.	No deviations noted.
C5.40	Authentication Servers record failed login attempts to the network equipment.	Reviewed configurations to determine if failed login attempts were logged.	No deviations noted.
	Agency Wide Area Network		
C5.41	The Department has implemented last mile redundancy where technically, fiscally, and operationally feasible.	Reviewed configurations to determine if they had been configured for redundancy.	No deviations noted.

C5.42	Network software collects and analyzes operational metrics of devices connectivity, traffic bandwidth, and process utilization. Network hardware and software generates an email to the 24x7x 365 Network Operations Center or console display alert when a predefined event occurs, or a threshold is reached. The 24x7x365 Network Operations Center follows up on these alerts and engages operational teams for resolution as necessary.	Reviewed software configurations to determine if emails and alerts were sent to the 24x7x365 Network Operations Center when predefined events or thresholds were reached and the 24x7x365 Network Operations Center followed up on the alerts.	No deviations noted.
C5.43	Authentication servers record failed login attempts to network equipment. Failed attempts automatically generate an email notifications which is forwarded notifications to Network Design & Engineering staff for determination if further action is required.	Reviewed configurations to determine if failed login attempts were logged and if an email notification was sent to Network Design & Engineering staff.	No deviations noted.
C5.44	VPNs provided controlled and trusted connections between devices.	Reviewed VPN configurations to determine if security settings were configured to allow for secure remote connections.	No deviations noted.
C5.45	The Department's Enterprise VPN Standard provides guidance when establishing a VPN connection.	Reviewed the Enterprise VPN Standard to determine if it provided guidance on VPN connections.	No deviations noted.

C5.46	When data travels across a public network, it is encrypted at the access router and while in transit across the public network until it reaches the distribution router and enters the private network.	Reviewed configurations to determine if data traversing the network was encrypted.	No deviations noted.
	Backbone Wide Area Network		
C5.47	The Department has implemented redundancy between Point of Presence sites where technically, fiscally, and operationally feasible and has also installed fiber optic wave transmission technologies to provide high speed backbone transport services.	Reviewed configurations to determine if they had been configured for redundancy.	No deviations noted.
		Reviewed network diagrams to determine if fiber optic wave transmission technologies had been installed.	No deviations noted.
C5.48	Network software collects and analyzes operational metrics of devices connectivity, traffic bandwidth, and process utilization. Network hardware and software generates an email to the 24x7x 365 Network Operations Center or console display alert when a predefined event occurs, or a threshold is reached. The 24x7x365 Network Operations Center follows up on these alerts and engages operational teams for resolution as necessary.	Reviewed software configurations to determine if emails and alerts were sent to the 24x7x365 Network Operations Center when predefined events or thresholds were reached and the 24x7x365 Network Operations Center followed up on the alerts.	No deviations noted.

C5.49	Authentication Servers record failed login attempts to the network equipment. Failed attempts automatically generate an email notification to Network Design & Engineering staff for determination if further action is required.	Reviewed configurations to determine if failed login attempts were logged and if an email notification was sent to Network Design & Engineering staff.	No deviations noted.

Control Objective 6: Controls provide reasonable assurance that application and system processing are authorized and completely and accurately executed in a timely manner and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete and timely manner that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C6.1	The Operations Center utilizes software and the Automated Operations Console in order to continuously monitor the Mainframe and Midrange environment.	Observed the software and the AOC to determine if it monitored the mainframe and midrange environment.	No deviations noted.
C6.2	Problems, issues, and incidents are recorded via the Daily Shift Reports and a Remedy Ticket is created.	Selected a sample of Daily Shift Reports to determine if problems, issues, and incidents were recorded and if a Remedy ticket was	No deviations noted.
C6.3	The Daily Shift Report documents the activity conducted on mainframe production systems and incident calls received at the Operations Center. The Report contains the date, time, system involved in the incident, along with a narrative providing any necessary information regarding the incident. The Report is forwarded to Enterprise Infrastructure management and supervisors for awareness and follow-up of outstanding issues.	Selected a sample of Daily Shift Reports to determine if they documented activity conducted on the mainframe production environment, recorded incident calls received, and were forwarded to the Enterprise Infrastructure management and supervisors for awareness and follow-up.	No deviations noted.
C6.4	The Operator Shift Change Checklist (an action list shared between shifts) is completed at the beginning of each shift to ensure the production systems are operating appropriately and any open items are passed on to the next shift and to identify any changes which need to be made. The Operator Shift Change Checklist are signed off by Operations Center supervisors.	Selected a sample of the Operator Shift Change Checklists to determine if they were completed at the beginning of each shift and reviewed by the Operations Center supervisors.	No deviations noted.

	Mainframe Environment		
C6.5	The mainframe environment is monitored through the z/OS systems console for errors and issues.	Observed the z/OS system console to determine if errors and issues were	No deviations noted.
C6.6	Mainframe system performance and capacity is monitored by System Software programming personnel, via Resource Measurement Facility reports which are run daily and monthly.	Selected a sample of Resource Measurement Facility reports to determine if they were ran daily and monthly and monitored by System Software personnel.	1 of 56 daily Resource Management Facility Reports selected was not provided.
C6.7	Performance and capacity monitoring are documented via internal memorandum distributed via email to Enterprise Infrastructure management monthly.	Selected a sample of internal memorandums to determine if they were distributed monthly to Enterprise Infrastructure management.	No deviations noted.
	Midrange Environment		
C6.8	Midrange availability is monitored by the Operations Command Center via the What's Up Gold system.	Observed What's Up Gold to determine if availability and performance was monitored.	No deviations noted.
C6.9	SQL database serves use the Idera tool set for additional monitoring. The Idera system alerts have been set up to generate emails to SQL support staff.	Observed Idera to determine if monitoring and email alerts were sent to the SQL support staff.	No deviations noted.
C6.10	AD domain Controllers use Microsoft System Center for additional monitoring. System Center alerts have been set up to email alerts to AD support staff.	Observed Microsoft System Center to determine if monitoring and email alerts were sent to AD support staff.	No deviations noted.
C6.11	The Security Operations Center has established Standard Operating Procedures to assist with the detection, analysis and resolution.	Reviewed the Standard Operating Procedures to determine if they provided guidance on detection, analysis, and resolution.	No deviations noted.

C6.12	Upon notification of a threat, the Department follows the Cyber Security Incident Response Plan.	Selected a sample of reported threats to determine if they complied with the Cyber Security Incident Response Plan requirements.	16 of 31 medium and high incidents selected did not have an incident report. 52 of 60 incident reports selected did not document the lessons learned. 57 of 60 incident reports selected did not document the prevention recommendations. 25 of 26 high incident reports selected did not document notification to the CISO and the agency within one hour of discovery. 3 of 5 medium incident reports selected did not document notification to the incident manager and the agency within four hours of discovery. 2 of 29 low incident reports selected did not include documentation of agency notification. 28 of 31 medium and high incident reports selected did not have documentation of status updates to the CISO and the agency.

			18 of 31 medium and high incident reports selected did not have documentation of an executive summary being provided to the deputy CISO and the agency.
C6.13	The weekly activity reports which document a summary of the incidents noted during the week, and their resolutions are available to management.	Selected a sample of weekly activity reports to determine if incidents and their resolutions were documented.	No deviations noted.

Control Objective 7: Controls provide reasonable assurance that the transmission of data between the Department and entities are from authorized sources and are complete, accurate, secure, and timely that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C7.1	The secure, encrypted transfer of mainframe data is achieved using the File Transfer Protocol Secure (FTPS).	Observed the file transfer protocol to determine if the mainframe data was secure and encrypted during transfer.	No deviations noted.
C7.2	The software MoveIt is used to transmit midrange data between servers and applications.	Observed the MoveIt software to determine if midrange data was transmitted between servers and applications.	No deviations noted.
C7.3	The MOVEit software sends email alerts for any failures to Department and agency support staff.	Reviewed MOVEit software configurations to determine if email alerts were sent to Department and agency support staff.	No deviations noted.
C7.4	Access to MOVEit systems are reviewed on an annual basis by the Department’s Midrange Wintel Group.	Reviewed the annual review of access to MOVEIt by the Department's Midrange Wintel Group.	No deviations noted.
C7.5	Another option available to valid Illinois.gov users for the secure transmission of data is the file transfer utility 'FileT'.	Observed FileT to determine the security over the transmission of the data.	No deviations noted.

C7.6	This utility (FileT) uses random key generation to access files stored on a server.	Reviewed file transfer protocol configurations to determine if random key generation was utilized.	No deviations noted.
C7.7	Files (FileT) are automatically purged from the server after 5 days.	Reviewed file transfer protocol configurations to determine if files were purged after 5 days.	No deviations noted.
C7.8	Sender must acknowledge a warning of unauthorized access message.	Observed the sender must acknowledge a warning of unauthorized access message.	No deviations noted.
C7.9	A valid Illinois.gov address is required to use FileT.	Observed a valid Illinois.gov address was required.	No deviations noted.

Control Objective 8: Controls provide reasonable assurance the environment is configured as authorized in order to support application controls and to protect data from unauthorized changes that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C8.1	The Department has implemented system options to protect resources and data.	Reviewed SETROPTS report to determine if security options were implemented.	No deviations noted.
C8.2	The System Coordinator runs a System Management Facility violation report weekly for review and signs off on the report after resolving any unusual violations.	Reviewed a sample of weekly System Management Facility violation reports to determine if unusual violations were resolved and the reports were signed off on by the System Coordinator.	No deviations noted.
C8.3	The System Administrator and Mainframe manager review a high-level systems programmer user ID listing on an annual basis.	Reviewed the annual review of high-level system programmer user IDs to determine if the System Administrator and Mainframe manager had reviewed.	No deviations noted.
C8.4	The Department has developed the operations manuals to provide staff with instructions for various tasks.	Reviewed the operations manual to determine if instructions were provided for various tasks.	No deviations noted.
C8.5	The End Point Protection Group is responsible for pushing definitions and other antivirus software updates out.	Reviewed antivirus compliance reports to determine if definitions and updates were configured.	The February 10, 2020 compliance report documented 84 systems which did not list a DAT version or AmCore Content version. The February 10, 2020 compliance report documented 4 systems which stated N/A for the AmCore Content version. Of the devices connected on February 10, 2020:

			3 of 583 systems did not have the latest Virus Scan Enterprise Product version. 5 of 583 Windows systems did not have the latest DAT version. 22 of 1,822 Windows systems did not have the latest Endpoint Security Threat Prevention Product version. 1 of 169 non-Windows systems did not have the latest Endpoint Security Threat Prevention Product version. 7,503 of 45,725 operating systems did not have the latest Endpoint Security Threat Prevention Product version. 5,304 of 47,460 systems did not have the latest AmCore Content version. 22 of 169 non-Windows systems did not have the latest DAT version.
C8.6	The tool is used to automatically push virus definition files to all systems after receipt from antivirus vendors.	Observed tools to determine if the virus definitions files were pushed out to all systems after receipt from antivirus vendors.	No deviations noted.

C8.7	The endpoint protection group has tools available to monitor the state of systems and detect systems which fail to load updates and are not running the latest supported version.	Observed tools utilized for antivirus protection.	No deviations noted.
		Reviewed antivirus compliance reports to determine if systems were monitored.	No deviations noted.
C8.8	The Department receives Microsoft Windows patches monthly. The patches are first tested with the technical staff, a pilot group, and then pushed out to the general population. The patch process follows the Department's change management process.	Selected a sample of Microsoft Windows servers to determine if the patches were pushed out monthly, tested, and followed the Department's change management process.	No deviations noted.
C8.9	Linux servers are patched every 90 days, which are reviewed and tested by technicians and followed the Department's change management process.	Selected a sample of Linux servers to determine if patches were pushed out every 90 days, tested by technicians, and followed the Department's change management process.	No deviations noted.
C8.10	VMWare and Unix servers are patched when patches are provided by the vendor, which are reviewed and tested by technicians and follow the Department's change management process.	Selected a sample of VMWare and Unix servers to determine if patches were pushed out when provided by the vendor, tested by technicians, and followed the Department's change management process.	The Department did not provide a complete and accurate population of VMWare patches. For the VMWare patches provided, 2 of 2 patches selected were not tested prior to being pushed to the general population.

Control Objective 9: Controls provide reasonable assurance that applications, data, and the environment is backed up and stored offsite that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C9.1	Data Storage performance and capacity are monitored using EMC Toolsets.	Observed EMC toolset to determine if data storage performance and capacity were monitored.	No deviations noted.
C9.2	When capacity is reached or exceeds 80% automated alerts are sent via email to Data Storage Technicians and management.	Reviewed storage system configurations to determine if automated alerts were configured.	No deviations noted.
C9.3	Mid-Range System Data Backups are monitored by EMC tools and IBM Spectrum Protect.	Observed the EMC tools and IBM Spectrum Protect to determine if midrange system data backups were monitored.	No deviations noted.
C9.4	Data Center firewall and switch configurations have incremental backups performed twice a day that are stored for a minimum of 60 days at the Central Computing Facility (CCF) and Alternate Data Center (ADC).	Reviewed backup schedules to determine if incremental backups were performed twice a day and if the backups were stored at the CCF and the ADC.	No deviations noted.
C9.5	LAN access switch configurations are saved on a network management server, which verifies device configuration revisions daily, and new configurations are backed up when detected.	Reviewed configuration backup schedule to determine if the configurations were saved on a network management server.	No deviations noted.

C9.6	Configurations saved on the network management server are backed up daily to the CCF and the ADC through the midrange backup system.	Reviewed the backup schedule to determine if the network management server was backed up daily to the CCF and the ADC.	No deviations noted.
	Agency Wide Area Network		
C9.7	Device configurations are saved on network management server, which verifies device configuration revisions daily, and new configurations are backed up when detected.	Reviewed configurations backup schedule to determine if the configurations were saved on a network management server.	No deviations noted.
C9.8	Configurations saved on the network management server are backed up daily to the CCF and the ADC through the midrange backup system.	Reviewed the backup schedule to determine if the network management server was backed up daily to the CCF and the ADC.	No deviations noted.
	Backbone Wide Area Network		
C9.9	Device configurations are saved on network management server, which verifies device configuration revisions daily, and new configurations are backed up when detected.	Reviewed configuration backup schedule to determine if the configurations were saved on a network management server.	No deviations noted.
C9.10	Configurations saved on the network management server are backed up daily to the CCF and the ADC through the midrange backup system.	Reviewed the backup schedule to determine if the network management server was backed up daily to the CCF and the ADC.	No deviations noted.

	Mainframe		
C 9.11	Data on mainframe systems are backed up daily and weekly utilizing Virtual Tape Technology (Disk Library Management (DLM)).	Observed the DLM to determine if mainframe backups were performed daily and weekly.	No deviations noted.
C 9.12	The Department utilizes CA Scheduler to schedule and verify the completion of the backups.	Selected a sample of backup schedules to determine if mainframe backups were scheduled and the completion was verified.	No deviations noted.
C 9.13	The Department has implemented backup procedures to assist staff in the event of failures.	Reviewed policies to determine if they outlined procedures in the event of failed backups.	No deviations noted.
C9.14	In the event of a mainframe daily backup job failure, the Operations Center staff records the incident in the Shift Report.	Collaboratively inquired with Operations Center staff.	The Department did not encounter failed backups. Therefore, the Service Auditor was unable to test the operating the effectiveness of the control.
C9.15	The next working day, Storage staff review the Shift Report to identify problems, correct and resubmit the failed portion of the backup job.	Collaboratively inquired with Storage staff.	The Department did not encounter failed backups. Therefore, the Service Auditor was unable to test the operating the effectiveness of the control.
C 9.16	The Storage staff review the output of the weekly backup jobs for success or failure. The failure is researched and corrected, and then the failed portion of the backup job is resubmitted for completion.	Collaboratively inquired with Storage staff.	The Department did not encounter failed backups. Therefore, the Service Auditor was unable to test the operating the effectiveness of the control.

C9.17	Mainframe data replication occurs every 15 minutes between the CCF and the ADC DLM. The monitoring software sends the Enterprise Storage and Backup group an alert if the data is out of sync for more than 24 hours.	Observe the DLM configurations to determine if replication occurs every 15 minutes and that an alert was sent if the data was out of sync for more than 24 hours.	No deviations noted.
C9.18	If there is an issue, a Remedy ticket is submitted to track the Enterprise Storage and Backup group's progress on resolution of the issue.	Collaboratively inquired with Enterprise Storage and Backup staff.	The Department did not encounter failed backups. Therefore, the Service Auditor was unable to test the operating the effectiveness of the control.
C9.19	The DLM Replicated Status log keeps a log of replication between the two DLMs and tracks library replication outcomes for DLM replication activity.	Observe the DLM replication log to determine if the current replication activity was recorded and tracking the replication outcome.	No deviations noted.
	Midrange		
C9.20	Spectrum Protect and Avamar are used to backup the midrange environment.	Observed Spectrum Protect and Avamar to determine if they were used to backup the midrange environment.	No deviations noted.
C9.21	Data Protection Advisor is used to monitor and report on midrange backups.	Observed Data Protection Advisor to determine if it monitored and reported on midrange backups.	No deviations noted.

C 9.22	Spectrum Protect and Data Protection Advisor automatically generate daily reports indicating the backup status of scheduled jobs from the prior day.	Observed that Spectrum Protect and Data Protection Advisor were configured to send daily reports of the backup status for all scheduled jobs from the prior day.	No deviations noted.
C9.23	These daily reports are emailed to the Enterprise Storage and Backup group who then investigates the cause of the failures and works to resolve the problem.	Interviewed Enterprise Storage and Backup staff to determine the actions taken to resolve the failures.	No deviations noted.
C9.24	Backed up server data is written to a Data Domain storage system and then replicated to another Data Domain storage system at the ADC.	Observed the replication of the Data Domain storage system to determine if it was replicated to the ADC.	No deviations noted.
C 9.25	The Data Domain storage system generates a daily status report which is emailed to the Enterprise Storage and Backup group.	Observed the Data Domain was configured to send daily reports of the replication status for all scheduled jobs.	No deviations noted.
C9.26	The Data Domain storage systems also send email alerts to the Enterprise Storage and Backup group when issues arise that may need additional attention.	Observed the configuration of the Data Domain storage system to determine if alerts were sent to the Enterprise Storage and Backup group.	No deviations noted.
C 9.27	The Data Domain systems automatically alert vendor support in the event of hardware to system failures.	Observed the configuration of the Data Domain storage systems to determine if alerts were sent to the support vendor.	No deviations noted.

C 9.28	The database backups are written to the Data Domain storage systems via Common Internet File System or Network File System and then replicated to the ADC.	Observed the replication of the Data Domain storage systems to determine if it was replicated to the ADC.	No deviations noted.
C9.29	A PowerShell script goes through the production SQL servers and creates a report with the latest backup data and it is sent to the SQL team daily.	Observed the SQL configuration to determine if the status of backups was documented daily.	No deviations noted.
C9.30	The SQL team reviews it and follows up for any failures.	Collaboratively inquired with SQL team.	The Department did not encounter failed backups. Therefore, the Service Auditor was unable to test the operating the effectiveness of the control.
C9.31	The SQL team also gets alerts from the SQL servers when backup jobs fail.	Observed the SQL servers to determine if alerts were enabled.	No deviations noted.
C9.32	Additionally, the SQL team receives alerts from the Idera monitoring software if a data base has missed a backup.	Observed the Idera monitoring software to determine if automatic alerts were enabled.	No deviations noted.
C 9.33	Any data, including, but not limited to SQL, Access, DB2 databases, user shared documents and user profiles are located on the Isilon storage device via the Network File System or the Service Message Block shares.	Observed the configuration of the Isilon storage device to determine the nature of the data stored on it.	No deviations noted.

C9.34	The Enterprise Storage and Backup group has policies on the Isilon that take daily snapshots of all shares which are then retained for 60 days.	Observed the Isilon storage device configurations to determine if daily snapshots were taken and maintained for 60 days.	No deviations noted.
C 9.35	The Isilon also has daily synchronization with the ADC to another Isilon storage system.	Observed the Isilon storage device configurations to determine if replicated to the ADC.	No deviations noted.
C9.36	The Isilon generates a daily report showing successful and failed synchronization attempts with the ADC.	Observed the Isilon storage device was configured to send daily reports with the status of replication jobs to the Storage group.	No deviations noted.
C9.37	Enterprise Storage and Backup group investigate failed synchronization attempts until a satisfactory conclusion is reached.	Collaboratively inquired with the Enterprise Storage and Backup group.	The Department did not encounter failed backups. Therefore, the Service Auditor was unable to test the operating the effectiveness of the control.
C 9.38	The Isilon has a call home feature that notifies vendor support. For critical issues, the Isilon call home feature additionally notifies the Enterprise Storage and Backup group.	Observed the Isilon configurations to determine if the call home feature was active.	No deviations noted.

Control Objective 10: Controls provide reasonable assurance that physical access to facilities and data centers is restricted to authorized personnel, that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPAPRTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
	Warehouse		
C10.1	The Department's warehouse physical security is managed by cameras and badge proximity readers that are installed at the front and rear entrances and at the dock doors.	Observed cameras and badge proximity readers at the front and rear entrances at the dock doors.	No deviations noted.
C10.2	Authorized badged individuals may enter the Warehouse or End User Computing (EUC) areas through swiping of a Velocity badge.	Selected a sample of individuals to determine if they were authorized to have access.	1 of 5 individual selected was not properly authorized to have access to the EUC area.
C10.3	A visitor's log captures who enters the building.	Observed visitors were required to sign the visitor's log.	No deviations noted.
	CCF and Communication Center		
C10.4	For the Department's Communication Center and the Central Computing Facility (CCF), security guard monitor 24x7x365, proximity badge readers located at various interior and exterior entry points, security alarms, and cameras.	Observed security guards, proximity badge readers, security alarms, and cameras were present at the CCF and the Communication Center.	No deviations noted.

C10.5	Individuals not registered in the Velocity system (no permanent badge issued) must present proof of identification and sign the visitor register log at the guard station to obtain a visitor badge.	Observed visitors were to present proof of identification and sign the visitor register log in order to obtain a visitor badge.	No deviations noted.
C10.6	Visitors are required to be escorted while in either building.	Observed visitors being escorted while in the buildings.	No deviations noted.
C10.7	For individuals registered in the Velocity system but not having a permanent badge immediately available, guards issue a temporary badge upon proof of identification.	Observed individuals were provided temporary badges.	No deviations noted.
C10.8	Temporary badges are also issued to approved vendors once identification has been validated by the facility security guard.	Selected a sample of the Building Admittance Registers to determine if individuals were provided a temporary badge with appropriate access.	1 individual was not provided the appropriate access.
C10.9	Access to the CCF secured area is limited to a small group of individuals with specific business need and requires special badge permission to exit the elevator or enter through the stairway door.	Selected a sample of individuals with access to the secure area to determine appropriateness of access.	2 of 51 individuals selected did not require access to the secure area.
C10.10	Surveillance is enhanced with additional cameras and door sensors to the CCF secured area.	Observed cameras and door sensors were present in the secure area.	No deviations noted.

C10.11	Midrange Wintel Manager or designee conducts monthly review of individuals who were granted access or removed access from the previous month to the CCF highly secured area to ensure proper access is being granted.	Selected a sample of monthly reviews to determine if the Midrange Wintel Manager had reviewed individuals' access to the CCF highly secured area to ensure the access was proper.	No deviations noted.
C10.12	The Department’s Security team conducts a physical access review each calendar quarter for Communication Center. The first review was conducted in February 2020.	Selected a sample of quarterly access reviews to determine if the Security team had reviewed individuals' access to the Communication Building to ensure access was proper.	No deviations noted.
C10.13	Starting in December 2019, Department’s Security team conducts monthly CCF highly secured area physical access review.	Selected a sample of monthly access reviews to determine if the Security team had reviewed individuals' access to the CCF highly secured area to ensure access was proper.	No deviations noted.

C10.14	Effective January 1, 2020, Physical Access Door Group Review Procedure was created to reflect the current physical access review process.	Reviewed the Physical Access Door Group Review Procedures to determine if the current review process was documented.	The Physical Access Door Group Review Procedures did not document the frequency of the reviews and the door groups that were to be reviewed. Additionally, the Procedures did not document what the process would be if the verification was not completed and the process for the Department's timekeeping and badging division to remove access.
C10.15	To obtain a badge, the DoIT Badging Process is followed. The Department's process requires HR to be in receipt of a DoIT Badge Request form.	Selected a sample of access requests to determine if the DoIT Badge Request form was properly approved and the requested access was granted.	The Department did not provide a listing of individuals who were authorized to approve the DoIT Badge Request form. Therefore the Service Auditor was unable to test the operating effectiveness of the control. 1 of 26 individuals selected did not have a completed DoIT Badge Request form.

C10.16	Valid proof of identity and a photo are required for creation of a new badge.	Selected a sample of new access requests to determine if a valid proof of identity and a photo was supplied.	No deviations noted.
C10.17	For non-state employees, documentation of a clear background check, performed in the last five years, must be provided prior to initial badge issuance.	Selected a sample of access requests for non-State employees to determine if a clear background check had been completed in the last five years and was provided prior to the initial badge issuance.	No deviations noted.
C10.18	Access requested for the CCF highly secured area requires approval from those designated as approvers for the secured area.	Selected a sample of access requests to the CCF highly secured area to determine if proper approval was obtained.	4 of 8 individuals selected did not have proper approval.
C10.19	Badge access is revoked by the Velocity system at badge expiration date.	Observed the Velocity system to determine if badge expiration dates were documented.	No deviations noted.
C10.20	HR deactivates badge access after official notice of separation or termination.	Reviewed Remedy and inquired with staff to determine if badge access was deactivated.	The Department did not provide documentation demonstrating the terminated individuals' access badge had been deactivated. Therefore, the Service Auditor was unable to test the operating the effectiveness of the control.

SECTION V

OTHER INFORMATION PROVIDED BY THE STATE OF ILLINOIS, DEPARTMENT OF INNOVATION AND TECHNOLOGY

Department of Innvoation and Technology
Corrective Action Plan
(Not Examined)

	Report Control	Opinion / Exception	Department Response
1	Opinion1	The Department did not have controls in place to review access to the Communication Building during the period of July 1, 2019 to December 31, 2019.	While the physical access reviews were performed during the above mentioned period, the review procedure was under development, and documentation was not maintained. The Department has developed procedures and implemented controls to perform physical access reviews to the Communication Building.
2	Opinion2	The Department did not have controls in place to review access to the Department's Central Computing Facility (CCF) highly secured area during the period of July 1, 2019 through November 30, 2019.	While the physical access reviews were performed during the above mentioned period, the review procedure was under development, and documentation was not maintained. The Department has developed procedures and implemented controls to perform physical access reviews to the CCF highly secured area.
3	Opinion3	The Department could not provide a population of access modifications to the Department's resources.	The Department will research opportunities to generate reports in the requested format for future audit testing.
4	Opinion4	The Department could not provide documentation of the timely termination of an individual's access to the Department's resources.	The Department now generates a monthly report to record individual access termination information.
5	Opinion5	The Department could not provide a listing of individuals authorized to approve the DoIT Badge Request form.	The Department will review the badge request process.
6	Opinion6	The Department could not provide documentation demonstrating the terminated individual's access badge was deactivated.	The Department will research opportunities to generate reports in the requested format for future audit testing.
7	CE1.6	34 of 38 selected employees' probationary evaluations were completed between 14 to 262 days late.	The Department will continue distributing monthly evaluation tickler reports. It is the supervisor's responsibility and obligation to complete the performance evaluation as required and submit to HR for processing.
8	CE1.7	19 of 22 selected employees' probationary evaluations were completed between 3 and 152 days late.	The Department will continue distributing monthly evaluation tickler reports. It is the supervisor's responsibility and obligation to complete the performance evaluation as required and submit to HR for processing.
9	CE1.8	31 of 60 selected employees' annual evaluations were completed between 6 and 204 days late.	The Department will continue distributing monthly evaluation tickler reports. It is the supervisor's responsibility and obligation to complete the performance evaluation as required and submit to HR for processing.

10	CE1.12	Ethics training was not conducted during the examination period. Therefore, the Service Auditor was unable to test the operating effectiveness of the control. 6 of 1,505 required employees and contractors selected did not complete the Safeguard Disclosure training. 3 of 1,429 required employees and contractors selected did not complete the Security Awareness training. No deviations noted with Sexual Harassment Prevention training.	The Department will continue sending training reminders to the employees.
11	CE1.13	2 of 31 terminated employees selected did not have a Remedy Service Request completed. There were no deviations noted in testing of the Exit form.	The Department will examine this isolated occurrence and remind staff of the offboarding process.
12	C2.1	No deviations noted. 1 of 6 state tax rates were incorrect. The State of Illinois' tax rate was correct.	The Department has corrected the tax rate and will review the process of updating state tax tables.
13	C3.1	The Change Management Process Guide did not contain information on the change freeze process.	The Department will review and update the document.
14	C3.2	4 of 60 significant or extensive changes selected did not contain a test plan. 5 of 60 significant or extensive changes selected did not contain a backout plan. 5 of 60 significant or extensive changes selected did not contain a implementation plan.	The Department will remind staff of the internal process guide.
15	C3.3	2 of 19 emergency changes selected did not have a Post Implementation Review conducted. 1 of 19 emergency changes selected was created and approved by the same individual.	The Department will remind staff of the internal process guide.
16	C3.4	1 of 61 changes selected had a class of "expedited" which was not addressed in the change management policies. 1 of 61 changes selected was improperly categorized as "no impact" instead of "significant."	The Department will remind staff of the internal process guide.

17	C4.4	2 of 6 stolen and missing laptops selected did not have verification of encryption was installed.	The Department subsequently verified the encryption was installed on the missing laptops; therefore, no data was at risk. The Department will review the documentation process.
18	C5.2	3 of 25 selected new employees' and contractors' Remedy service requests were not submitted by an authorized ATSR or Department IT Coordinator. 1 of 26 selected new employees and contractors did not have a Remedy service request submitted to obtain access to the Department's resources. The Department did not provide a complete and accurate population of access modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.	The Department will remind staff of the onboarding process. Regarding the population of access modifications, the Department will research opportunities to generate reports in the requested format for future audit testing.
19	C5.26	The annual technical account review controls did not include a defined timeframe for the disabling/deletion of accounts in the event a manager did not respond to the review request.	The Department will define timelines for disabling / deletion of technical accounts.
20	C6.6	1 of 56 daily Resource Management Facility Reports selected was not provided.	The Department will examine this isolated incident and ensure data integrity during staff transition periods moving forward.
21	C6.12	16 of 31 medium and high incidents selected did not have an incident report. 52 of 60 incident reports selected did not document the lessons learned. 57 of 60 incident reports selected did not document the prevention recommendations. 25 of 26 high incident reports selected did not document notification to the CISO and the agency within one hour of discovery. 3 of 5 medium incident reports selected did not document notification to the incident manager and the agency within four hours of discovery. 2 of 29 low incident reports selected did not include documentation of agency notification. 28 of 31 medium and high incident reports selected did not have documentation of status updates to the CISO and the agency. 18 of 31 medium and high incident reports selected did not have documentation of an executive summary being provided to the deputy CISO and the agency.	The Department will update the internal documents to reflect the current incident response process.

22	C8.5	The February 10, 2020 compliance report documented 84 systems which did not list a DAT version or AmCore Content version. The February 10, 2020 compliance report documented 4 systems which stated N/A for the AmCore Content version. Of the devices connected on February 10, 2020: 3 of 583 systems did not have the latest Virus Scan Enterprise Product version. 5 of 583 Windows systems did not have the latest DAT version. 22 of 1,822 Windows systems did not have the latest Endpoint Security Threat Prevention Product version. 1 of 169 non-Windows systems did not have the latest Endpoint Security Threat Prevention Product version. 7,503 of 45,725 operating systems did not have the latest Endpoint Security Threat Prevention Product version. 5304 of 47,460 systems did not have the latest AmCore Content version. 22 of 169 non-Windows systems did not have the latest DAT version.	The Department will continue to improve data protection efforts by implementing automated discovery and remediation of non-compliant anti-virus services installed on servers and workstations.
23	C8.10	The Department did not provide a complete and accurate population of VMWare patches. For the VMWare patches provided, 2 of 2 patches selected were not tested prior to being pushed to the general population.	The Department will research opportunities to generate reports in the requested format for future audit testing.
24	C10.2	1 of 5 individual selected was not properly authorized to have access to the EUC.	The Department has identified the issue and will work to mature the process going forward.
25	C10.8	1 individual was not provided the appropriate access.	The Department will follow up with the DCMS to ensure that the DCMS follows its badging process.
26	C10.9	2 of 51 individuals selected did not require access to the secure area.	The badges were disabled timely; therefore, there was no physical security risk. The Department will mature the physical access review process.
27	C10.14	The Physical Access Door Group Review Procedures did not document the frequency of the reviews and the door groups that were to be reviewed. Additionally, the Procedures did not document what the process would be if the verification was not completed and the process for the Department's timekeeping and badging division to remove access.	The Department will update the physical access review procedure.
28	C10.18	4 of 8 individuals selected did not have proper approval.	The Department has identified the issue and has updated the process.

Department of Innovation and Technology
Business Continuity and Disaster Recovery
(Not Examined)

Illinois continuously strategizes and benchmarks against commercial, federal, state, and local organizations, ensuring the application of best in class processes. The Department partnered with Illinois Emergency Management Agency (IEMA)/University of Illinois to develop a National Institute of Standards and Technology (NIST) based cybersecurity framework and metrics to measure and ensure continuous improvement. Business impact analyses performed to establish a clear understanding of Illinois critical business processes ensuring recovery priorities, Recovery Time Objectives and Recovery Point Objectives aligned with critical business. Risk assessments measure maturity of each control and alignment of policy and processes to NIST controls to minimize risk. Illinois continuously maintains and updates recovery, backup, retention, data classification, network resources, data encryption, breach notification, facilities access and wireless devices. Resiliency planning model, as well as recovery activation and response plans include network, customer services, incidents and major outages, outline response teams' roles and responsibilities. Disaster Recovery testing includes tabletop, proof of concept, and real-life exercises to educate and learn about procedures, policies, best practices, recovery plans, contracts, communications strategies, key personnel, and feasibility. Application personnel restore data and information systems and verify admin/end-user transactions. FY20 testing involved mainframe and midrange information system contingency plans testing. Testing included 10 agencies, 23 mainframe applications and 13 midrange applications. Annual testing of the State of Illinois Cyber Disruption Plan was also conducted with IEMA, Illinois State Police, Illinois National Guard, and Statewide Terrorism and Intelligence Center.

Illinois utilizes the Illinois Century Network to serve as an Illinois local area network enabling interconnectivity, resource sharing, and access to instate content and cloud resources with 365/24/7 support. Resources are available from the IEMA and Emergency Management Assistance Compact (EMAC) to support an enterprise-wide disaster. The mainframe infrastructure at the Alternate Data Center has ample recovery resources. Systems, sub-systems, application libraries, and user data are backed up locally and replicated to the virtual tape storage system at the Alternate Data Center, along with the implementation of snapshots and Site Recovery Manager (SRM) of the mainframe environment. The midrange environment has also implemented SRM within the hyperconverged hardware and hybrid cloud software to build a geo-diverse private cloud software defined data center (SDDC) spread between both State of Illinois data centers.

Disaster recovery, along with infrastructure and information system contingency plans are published to SharePoint for ease of access and provide clearly defined notification pathways and document test results. An Enterprise Architecture Taxonomy database includes application classification information and attributes, recovery time objectives, prioritized recovery order, confidential data indications, and governing standards (HIPAA, IRS Pub 1075, PII, etc.).

Listing of User Agencies of the Department of Innovation and Technology's Information Technology Shared Services System (Not Examined)

1. Abraham Lincoln Presidential Library and Museum
2. Capital Development Board
3. Chicago State University
4. Commission on Government Forecasting and Accountability
5. Court of Claims
6. Criminal Justice Information Authority
7. Department of Agriculture
8. Department of Central Management Services
9. Department of Children and Family Services
10. Department of Commerce and Economic Opportunity
11. Department of Corrections
12. Department of Employment Security
13. Department of Financial and Professional Regulation
14. Department of Healthcare and Family Services
15. Department of Human Rights
16. Department of Human Services
17. Department of Innovation and Technology
18. Department of Insurance
19. Department of Juvenile Justice
20. Department of Labor
21. Department of the Lottery
22. Department of Military Affairs
23. Department of Natural Resources
24. Department of Public Health
25. Department of Revenue
26. Department of Transportation
27. Department of Veterans' Affairs
28. Department on Aging
29. Eastern Illinois University
30. Environmental Protection Agency
31. Executive Ethics Commission
32. General Assembly Retirement System
33. Governor's Office of Management and Budget
34. Governors State University
35. Guardianship and Advocacy Commission
36. House of Representatives

Provided by the Department of Innovation and Technology

37. Human Rights Commission
38. Illinois Arts Council
39. Illinois Board of Higher Education
40. Illinois Civil Service Commission
41. Illinois Commerce Commission
42. Illinois Community College Board
43. Illinois Council on Developmental Disabilities
44. Illinois Deaf and Hard of Hearing Commission
45. Illinois Educational Labor Relations Board
46. Illinois Emergency Management Agency
47. Illinois Finance Authority
48. Illinois Gaming Board
49. Illinois Housing Development Authority
50. Illinois Independent Tax Tribunal
51. Illinois Labor Relations Board
52. Illinois Latino Family Commission
53. Illinois Law Enforcement Training and Standards Board
54. Illinois Liquor Control Commission
55. Illinois Math and Science Academy
56. Illinois Power Agency
57. Illinois Prisoner Review Board
58. Illinois Procurement Policy Board
59. Illinois Racing Board
60. Illinois State Board of Investments
61. Illinois State Police
62. Illinois State Toll Highway Authority
63. Illinois State University
64. Illinois Student Assistance Commission
65. Illinois Torture Inquiry and Relief Commission
66. Illinois Workers' Compensation Commission
67. Joint Committee on Administrative Rules
68. Judges' Retirement System
69. Judicial Inquiry Board
70. Legislative Audit Commission
71. Legislative Ethics Commission
72. Legislative Information System
73. Legislative Printing Unit
74. Legislative Reference Bureau
75. Northeastern Illinois University
76. Northern Illinois University
77. Office of the Architect of the Capitol
78. Office of the Attorney General

79. Office of the Auditor General
80. Office of the Comptroller
81. Office of the Executive Inspector General
82. Office of the Governor
83. Office of the Lieutenant Governor
84. Office of the State Appellate Defender
85. Office of the State Fire Marshal
86. Office of the State's Attorneys Appellate Prosecutor
87. Office of the Treasurer
88. Pollution Control Board
89. Property Tax Appeal Board
90. Secretary of State
91. Senate Operations
92. Southern Illinois University
93. State Board of Education
94. State Board of Elections
95. State Charter School Commission
96. State Employees' Retirement System
97. State of Illinois Comprehensive Health Insurance Board
98. State Police Merit Board
99. State Universities Civil Service System
100. State Universities Retirement System
101. Supreme Court Historic Preservation Commission
102. Supreme Court of Illinois
103. Teachers' Retirement System of the State of Illinois
104. University of Illinois
105. Western Illinois University

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

1. Department on Aging
2. General Assembly Retirement System
3. Illinois Board of Higher Education
4. Illinois Community College Board
5. Illinois Student Assistance Commission
6. Judges' Retirement System
7. Judicial Inquiry Board
8. Office of the Attorney General
9. Office of the Auditor General
10. Office of the State Appellate Defender
11. Office of the State's Attorneys Appellate Prosecutor
12. State Board of Elections
13. State Employees' Retirement System
14. State Universities Civil Service System
15. Supreme Court of Illinois

Listing of User Agencies of the Department's Central Inventory System
(Not Examined)

1. Department on Aging
2. Office of the Attorney General
3. Office of the State's Attorneys Appellate Prosecutor

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

1. Abraham Lincoln Presidential Library and Museum
2. Capital Development Board
3. Commission on Government Forecasting and Accountability
4. Coroner Training Board
5. Court of Claims
6. Criminal Justice Information Authority
7. Department of Agriculture
8. Department of Central Management Services
9. Department of Children and Family Services
10. Department of Commerce and Economic Opportunity
11. Department of Corrections
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 Innovation and Technology
17. Department of Insurance
18. Department of Juvenile Justice
19. Department of Labor
20. Department of the Lottery
21. Department of Military Affairs
22. Department of Natural Resources
23. Department of Public Health
24. Department of Revenue
25. Department on Aging
26. Environmental Protection Agency
27. Executive Ethics Commission
28. General Assembly
29. Governor's Office of Management and Budget
30. Guardianship and Advocacy Commission
31. Human Rights Commission
32. Illinois Arts Council
33. Illinois Board of Higher Education
34. Illinois Civil Service Commission
35. Illinois Commerce Commission
36. Illinois Community College Board
37. Illinois Council on Developmental Disabilities
38. Illinois Deaf and Hard of Hearing Commission
39. Illinois Educational Labor Relations Board
40. Illinois Emergency Management Agency
41. Illinois Gaming Board
42. Illinois Health Information Exchange Authority

43. Illinois Independent Tax Tribunal
44. Illinois Labor Relations Board
45. Illinois Law Enforcement Training and Standards Board
46. Illinois Liquor Control Commission
47. Illinois Math and Science Academy
48. Illinois Power Agency
49. Illinois Prisoner Review Board
50. Illinois Procurement Policy Board
51. Illinois Racing Board
52. Illinois State Board of Investments
53. Illinois State Police
54. Illinois Student Assistance Commission
55. Illinois Workers' Compensation Commission
56. Joint Committee on Administrative Rules
57. Judges' Retirement System
58. Judicial Inquiry Board
59. Legislative Audit Commission
60. Legislative Ethics Commission
61. Legislative Information System
62. Legislative Printing Unit
63. Legislative Reference Bureau
64. Office of the Architect of the Capitol
65. Office of the Attorney General
66. Office of the Auditor General
67. Office of the Executive Inspector General
68. Office of the Governor
69. Office of the Lieutenant Governor
70. Office of the State Appellate Defender
71. Office of the State Fire Marshal
72. Office of the State's Attorneys Appellate Prosecutor
73. Office of the Treasurer
74. Property Tax Appeal Board
75. Sex Offender Management Board
76. State Board of Education
77. State Board of Elections
78. State Employees' Retirement System
79. State of Illinois Comprehensive Health Insurance Board
80. State Police Merit Board
81. State Universities Civil Service System
82. Supreme Court Historic Preservation Commission
83. Teachers' Retirement System of the State of Illinois

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

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

39. Property Tax Appeal Board
40. State Board of Elections
41. State Employees' Retirement System
42. State of Illinois Comprehensive Health Insurance Board

Listing of User Agencies of the Department's eTime System
(Not Examined)

1. Abraham Lincoln Presidential Library and Museum
2. Capital Development Board
3. Criminal Justice Information Authority
4. Department of Agriculture
5. Department of Central Management Services
6. Department of Commerce and Economic Opportunity
7. Department of Financial and Professional Regulation
8. Department of Human Rights
9. Department of Innovation and Technology
10. Department of Insurance
11. Department of Labor
12. Department of the Lottery
13. Department of Public Health
14. Department of Revenue
15. Department on Aging
16. Executive Ethics Commission
17. Guardianship and Advocacy Commission
18. Illinois Civil Service Commission
19. Illinois Council on Developmental Disabilities
20. Illinois Deaf and Hard of Hearing Commission
21. Illinois Emergency Management Agency
22. Illinois Gaming Board
23. Illinois Labor Relations Board
24. Illinois Liquor Control Commission
25. Illinois Prisoner Review Board
26. Illinois Procurement Policy Board
27. Illinois Racing Board
28. Illinois State Police
29. Illinois Workers' Compensation Commission
30. Office of the Executive Inspector General
31. Property Tax Appeal Board
32. State Employees' Retirement System
33. State of Illinois Comprehensive Health Insurance Board

Listing of Security Software Proxy Agencies
(Not Examined)

1. Abraham Lincoln Presidential Library and Museum
2. Capital Development Board
3. Chicago State University
4. Commission on Government Forecasting and Accountability
5. Coroner Training Board
6. Court of Claims
7. Department of Agriculture
8. Department of Central Management Services
9. Department of Human Rights
10. Department of Innovation and Technology
11. Department of Labor
12. Department of Military Affairs
13. Department of Veterans' Affairs
14. Eastern Illinois University
15. Executive Ethics Commission
16. Governors State University
17. Governor's Office of Management and Budget
18. Guardianship and Advocacy Commission
19. House of Representatives
20. Human Rights Commission
21. Illinois Arts Council
22. Illinois Civil Service Commission
23. Illinois Commerce Commission
24. Illinois Community College Board
25. Illinois Council on Developmental Disabilities
26. Illinois Deaf and Hard of Hearing Commission
27. Illinois Educational Labor Relations Board
28. Illinois Emergency Management Agency
29. Illinois Finance Authority
30. Illinois Health Information Exchange Authority
31. Illinois Housing Development Authority
32. Illinois Independent Tax Tribunal
33. Illinois Labor Relations Board
34. Illinois Law Enforcement Training and Standards Board
35. Illinois Liquor Control Commission
36. Illinois Math and Science Academy
37. Illinois Medical District Commission
38. Illinois Power Agency
39. Illinois Prisoner Review Board
40. Illinois Procurement Policy Board
41. Illinois State Board of Investments
42. Illinois State Toll Highway Authority

43. Illinois State University
44. Illinois Supreme Court Historic Preservation Commission
45. Joint Committee on Administrative Rules
46. Judicial Inquiry Board
47. Legislative Audit Commission
48. Legislative Ethics Commission
49. Legislative Information System
50. Legislative Inspector General
51. Legislative Printing Unit
52. Legislative Reference Bureau
53. Northeastern Illinois University
54. Northern Illinois University
55. Office of the Architect of the Capitol
56. Office of the Attorney General
57. Office of the Comptroller
58. Office of the Inspector General
59. Office of the Governor
60. Office of the Lieutenant Governor
61. Office of the State Appellate Defender
62. Office of the State Fire Marshal
63. Office of the State's Attorneys Appellate Prosecutor
64. Office of the Treasurer
65. Property Tax Appeal Board
66. Secretary of State
67. Senate Operations
68. Southern Illinois University
69. State Board of Education
70. State Board of Elections
71. State of Illinois Comprehensive Health Insurance Board
72. State Police Merit Board
73. State Universities Civil Service System
74. State Universities Retirement System
75. University of Illinois
76. Western Illinois University

ACRONYM GLOSSARY

AD – Active Directory
API – Application Program Interface
AR – Accounts Receivable
ATSR – Agency Technology Service Requestor
CHIRP – Criminal History Information Response Process
CIO – Chief Information Officer
CISO – Chief Information Security Officer
CJIS – Criminal Justice Information Services
CMS – Central Management Services
CO – Controlling
DCMS – Department of Central Management Services
Department – Department of Innovation and Technology
DIM – Department's Identity Management
DoIT – Department of Innovation and Technology
EAT – Expenditure Adjustment Transmittal
ECC – ERP Central Component
ERP – Enterprise Resource Planning
FEIN – Federal Employer Identification Number
FI – Financial Accounting
FM – Funds Management
FTI – Federal Tax Information
GL – General Ledger
GOMB – Governor's Office of Management and Budget
GRC – Governance, Risk, and Compliance
HPQC – Hewitt Packard Quality Control
HR – Human Resources
HRIS – Human Resources Information System
ID – Identification
ILCS – Illinois Compiled Statutes
ILTA – Illinois State Toll Highway Authority
IOC – Illinois Office of the Comptroller
IOCA – Illinois Office of the Comptroller Accounts
IP – Internet Protocol
IT – Information Technology
JE – Journal Entry
LHF – Locally Held Funds
M&O – Maintenance and Operational
MIM – Microsoft Identity Management
MS-ISAC – Multi-State Information Sharing and Analysis Center
NIST – National Institute of Standards and Technology
PAR – Personnel Action Request
PCI – Payment Card Industry
PHI – Protected Health Information
PSC – Personal Service Contractor

PSCD – Public Sector Collection & Disbursements
RDT – Receipt Deposit Transmittal
SAMS – Statewide Accounting Management System
SAP – Systems, Applications and Products
SKF – Statistical Key Figure
SOC – System and Organization Controls
SOD – Segregation of Duties
SRM – Supplier Relationship Management
SSN – Social Security Number
STIL – State of Illinois
WBS – Work Breakdown Structure