LEGISLATIVE AUDIT COMMISSION

Review of
Department of Innovation and Technology
620 Stratton Office Building
Springfield, Illinois 62706
217/782-7097

REVIEW #4559:
DEPARTMENT OF INNOVATION AND TECHNOLOGY
TWO YEARS ENDED
JUNE 30, 2022

RECOMMENDATIONS – 26
PARTIALLY IMPLEMENTED - 19
IMPLEMENTED – 6
UNDER STUDY - 1
ACCEPTED– All

REPEATED RECOMMENDATIONS – 23

PRIOR AUDIT FINDINGS/RECOMMENDATIONS – 28

This review summarizes the first audit report of the Department of Innovation and Technology for the two years ended June 30, 2022 filed with the Legislative Audit Commission on March 23, 2023. The auditors performed a compliance examination in accordance with *Government Auditing Standards* and State law.

The Department of Innovation and Technology (DoIT) was created in 2016 via Executive Order 2016-01, which took effect in March of 2016, with the mission to "deliver best in-class innovation and technology to client agencies to foster collaboration among client agencies, to empower client agencies to provide better service to residents of Illinois, and to maximize the value of taxpayer resources."

Agency Narrative:
The mission of DoIT is to empower the State of Illinois through high-value, customer-centric technology by delivering best-in-class innovation to client agencies, fostering collaboration, and empowering employees to provide better services to residents, businesses, and visitors. DoIT delivers statewide information technology and telecommunication services and innovation to state government agencies, boards, and commissions as well as policy and standards development, life-cycle investment planning, enterprise solutions, and privacy and security management.

Program Goals and Objectives:
- Use technology effectively to reduce administration costs.
- Encourage agencies to upgrade and replace legacy mainframe systems.
- Continue consolidation of state agencies into the shared data center to reduce capital investment and operating expenses for the state.
- Support the rollout of the statewide ERP system, and ensure successful integration with existing applications.
- Continue to measure and improve reliability, security, and availability of services.

- Standardize service offerings to provide consistent, cost-effective services to all state agencies.
- Expand the reach of the Illinois Century Network (ICN) to provide service to additional schools and units of local government.

The audit was performed when Brandon Ragle was Acting Secretary. Previous Secretary Jennifer Ricker left DoIT in January 2023.

The current Secretary of DoIT is Sanjay Gupta, a national IT leader with private and public sector experience. Gupta has served in major roles across the public and private sectors, including running the federal government's pandemic aid portals for small businesses and serving as a board member of the federal Technology Modernization Fund.

Previously, Gupta was the Chief Information Officer for the Justice Department's Executive Office for Immigration Review. He also served for more than four years as Chief Technology Officer of the U.S. Small Business Administration, where his efforts to modernize the agency allowed it to process more than $1 trillion in loans for the nation's largest economic recovery effort.

Prior to his career in public service, he spent nearly 20 years in management and as a consultant and analyst in leading global technology organizations, including several companies based in Illinois.

Gupta holds a Bachelor of Science from Punjab Engineering College, a Master of Science from Wayne State University, and a Master of Business Administration from the University of Michigan. He and his wife raised their two daughters in the suburbs of Chicago, where they lived for more than two decades.

Expenditures From Appropriations

	FY21 Expend	FY21 Headcount	FY22 Expend	FY22 Headcount
Innovation & Technology	**$656,500,100**	**1,203**	**$706,088,700**	**1,181**

For comparison, The total operational budget for DoIT in FY24 is $1,095,311,600. Of which $27 million is GRF. DoIT also has $178 million in Capital that is separate from operations. The estimated headcount in FY24 is over 1,700.

Key Performance Indicators

Indicator	FY20 Actual	FY21 Actual	FY22 Actual	FY23 Project
State employee users supported	55,477	68,668	68,863	69,000
Email users supported	61,430	66,185	78,780	79,000
Websites supported	141	149	140	150
Statewide apps supported	68	68	68	70
Service desk calls answered	166,350	139,938	142,553	150,000
Virtualized servers managed	3,884	3,915	4,495	4,500
Enterprise data storage managed (PB petabytes)	16.8	9	5.6	6
Security: current risk assessments	10	9	18	18
Cybersecurity training	61,700	60,500	63,000	65,000
Devices w/up to date virus protection	52,100	57,400	57,800	58,000
Agencies utilizing ERP	54	65	65	73
Agencies transferred to Illinois.gov email	92%	99%	100%	100%
Network data circuits managed	2,230	3,485	2,850	3,200
ICN anchor institutions	3,685	4,150	4,2,75	4,600
Wireless devices managed	32,790	36,000	31,160	32,000
Annual telecom orders (TSR)	9,100	8,130	8.865	8,000
Phone lines managed	67,500	69,400	68,850	70,000
Mainframe transactions complete within 1 second	99%	99%	99%	99%

Mainframe system availability	99%	99%	99%	99%
Systems w/disaster recovery services	100%	100%	100%	100%
Service desk customer satisfaction	88%	86%	94%	95%
Avg bandwidth in Mbps (all customers)	458	778.5	921	1,000
Network availability	99.99%	99.99%	99.99%	99.99%
Mainframe transactions completed within 2 seconds (per Gartner Group Research)	98%	98%	98%	98%

Source: Comptroller's Public Accountability Report.

Emergency Purchases

The Illinois Procurement Code (30 ILCS 500/) states, "It is declared to be the policy of the state that the principles of competitive bidding and economical procurement practices shall be applicable to all purchases and contracts…." The law also recognizes that there will be emergency situations when it will be impossible to conduct bidding. It provides a general exemption when there exists a threat to public health or public safety, or when immediate expenditure is necessary for repairs to state property in order to protect against further loss of or damage to state property, to prevent or minimize serious disruption in critical state services that affect health, safety, or collection of substantial state revenues, or to ensure the integrity of state records; provided, however that the term of the emergency purchase shall not exceed 90 days. A contract may be extended beyond 90 days if the chief procurement officer determines additional time is necessary and that the contract scope and duration are limited to the emergency. Prior to the execution of the extension, the chief procurement officer must hold a public hearing and provide written justification for all emergency contracts. Members of the public may present testimony.

Notice of all emergency procurement shall be provided to the Procurement Policy Board and published in the online electronic Bulletin no later than five business days after the contract is awarded. Notice of intent to extend an emergency contract shall be provided to the Procurement Policy Board and published in the online electronic Bulletin at least 14 days before the public hearing.

A chief procurement officer making such emergency purchases is required to file a statement with the Procurement Policy Board and the Auditor General to set forth the circumstance requiring the emergency purchase. The Legislative Audit Commission receives quarterly reports of all emergency purchases from the Office of the Auditor General. The Legislative Audit Commission is directed to review the purchases and to comment on abuses of the exemption.

The LAC has recorded the following for DoIT:

- FY22 Quarter 1 - $17.2 million – 13 EP;
- FY22 Qtr 2 - $29.1 million – 7 EP;
- FY22 Qtr 3 - $19 million – 8 EP;
- FY22 Qtr 4 - $55.6 million – 13 EP;
- FY23 Quarter 1 - $25.7 million – 9 EP;
- FY23 Qtr 2 - $12.1 million – 6 EP;
- FY23 Qtr 3 - $0; and
- FY23 Qtr 4 - $0.

Accountants' Findings and Recommendations

Condensed below are the 26 findings and recommendations included in the audit report. Of these, 23 are repeated from the previous audit. The following recommendations are classified on the basis of information provided by DoIT, via electronic mail received March 23, 2023.

1. The auditors recommend DoIT work with the agencies to ensure IGAs are timely executed and IGAs are entered into with all transferring agencies.

FINDING: *(Failure to Comply with Executive Order 2016-01) – First reported 2018, last 2020*

DoIT failed to comply with the provisions of Executive Order 2016-01: Executive Order Consolidating Multiple Information Technology Functions into A Single Department of Innovation and Technology.

During their testing, auditors noted 42 agencies had transferred their Information Technology (IT) functions to DoIT. However, they noted DoIT had not entered into Intergovernmental Agreements (IGA) with six (14%) and seven (17%) agencies FY21 and FY22, respectively.

Additionally, of the agencies statutorily required to transfer their IT functions to DoIT, the IGAs were not executed in a timely manner during the examination period. Specifically,

- 35 of 36 (97%) FY21 IGAs were not executed timely.
- 35 of 35 (100%) FY22 IGAs were not executed timely.

The IGAs were executed 168 to 998 days after the effective date of the agreement.

This finding was first reported during the period ended June 30, 2018. In the subsequent years, DoIT has been unsuccessful in implementing appropriate corrective action or procedures to remedy this deficiency.

DoIT management indicated the lack of resources has delayed the transfers and the execution of the IGAs.

Failure to timely and fully consolidate IT functions, employees, assets, and funds is a violation of the Executive Order and the Act.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. DoIT has not completed the transfer of all personnel and property for agencies identified in the statute and continues to work with agencies to complete the transfer of personnel and property as required by the Executive Order and Department of Innovation and Technology Act (20 ILCS 1370).

UPDATED RESPONSE:
Partially Implemented. For FY23, DoIT sent draft IGAs to all transferring agencies on June 3, 2022, so that they could be executed by July 1. Despite DoIT's follow up, not all agencies executed by the deadline. The failure to have all IGAs timely executed is outside the control of DoIT.

2. The auditors recommend DoIT implement controls to ensure all property is accounted for in accordance with the Illinois Administrative Code and the Statewide Accounting Management System Manual. In addition, DoIT should ensure the reporting to CMS and the Office of Comptroller is accurate and reconciled to DoIT's records.

FINDING: *(Failure to Maintain Controls over Property) – First reported 2018, last 2020*

DoIT failed to maintain controls over its property and related records.

Agency Report of State Property
During their testing of the Agency Report of State Property (Form C-15) filed with the Office of Comptroller, they noted:

- DoIT did not provide evidence of review for 16 of 16 (100%) quarterly C-15 Reports required to be filed during FY21 and FY22. As such, auditors were not able to determine whether these reports were reviewed prior to submission.

- DoIT did not consistently classify equipment subject to theft. Equipment totaling $5,627,655 and $4,829,016 was not classified as subject to theft and not reported in the C-15 and Annual Inventory Certification reports in FY21 and FY22, respectively. Additionally, equipment totaling $128,915 and $87,089 was not

classified as subject to theft in FY21 and FY22, respectively, although these properties were within the scope of DoIT's high-theft property definition under Section 2.1b of the property control procedure.

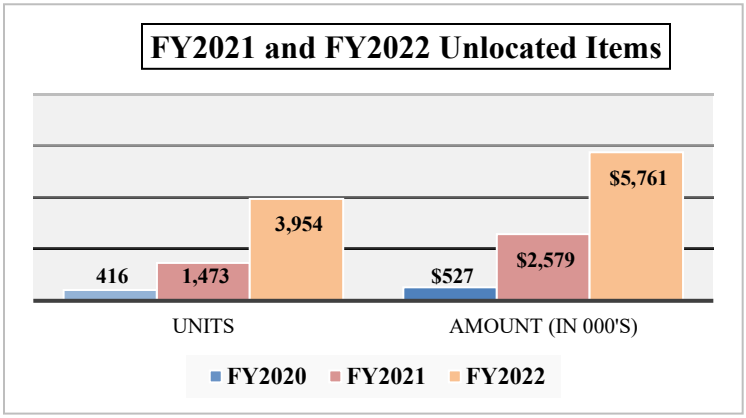
- For the FY21 C-15 Reports:
  - Equipment, totaling $558,393,343 at June 30, 2021, did not agree with DoIT's property listing. The discrepancy totaled $6,526.
  - Property additions did not agree with the detailed list of additions provided by DoIT. The discrepancies totaled $1,586,204. Additionally, properties added to the ERP were overstated by $186,051 and $219,040 for the Technology Management Revolving Fund (Fund 0304) and Government Funds (General Fund (Funds 0001) and Capital Development Fund (Fund 0141)), respectively.
  - Property deletions did not agree with the detailed listing of deletions provided by DoIT. The discrepancies totaled $2,033,000. Additionally, properties removed from the ERP were understated by $21,540.
  - Net transfers did not agree with the detailed list of net transfers provided by DoIT. The discrepancies totaled $1,709,947.

- For the FY22 C-15 Reports:
  - Equipment, totaling $402,731,172 at June 30, 2022, did not agree with DoIT's property listing. The discrepancy totaled $8,195.
  - Property additions did not agree with the detailed list of additions provided by DoIT. The discrepancies totaled $4,112,081. Additionally, properties added to the ERP were overstated by $315,884 for the Technology Management Revolving Fund (Fund 304).
  - Net transfers did not agree with the detailed list of net transfers provided by DoIT. The discrepancies totaled $4,112,571.
  - Property deletions totaling $146,840,965 were incorrectly reported as adjustment to additions.

Annual Certification of Inventory

During their testing of the Annual Inventory Certification Reconciliation filed with CMS, auditors noted:

- Properties totaling $211,651,503 and $46,845,799 were not reported in the Annual Inventory Certification submitted to CMS during FY21 and FY22, respectively.
- 544 and 520 property items reported to CMS during FY21 and FY22 did not have a reported cost.
- DoIT reported an astronomical increase in the number and value of unlocated items during FY21 and FY22. The number of the unlocated items increased by 1,057 or 254% and 2,481 or 168%, during FY21 and FY22, respectively. The value of the unlocated items increased by $2,051,683 or 389% and $3,181,792 or 123%, during FY21 and FY22, respectively. The chart below documents the increase over the past three fiscal years.



- During FY22, one DoIT location code understated the value of the missing properties in the Annual Inventory Certification by $302,171. During FY21, three DoIT location codes overstated the value of the missing properties in the Annual Inventory Certification by $32,557.

Population Completeness

Auditors requested DoIT to provide the population of its property in order to determine if property had been properly recorded. In response to the request, DoIT provided a population; however, given the noted exceptions above they were unable to conclude the Department's population records were sufficiently precise and detailed under the Professional Standards promulgated by the American Institute of Certified Public Accountants (AT-C § 205.36).

Even given the population limitations noted above, the auditors performed testing on a sample of the property population.

Detailed Testing

Property Additions

- Four of 60 (7%) property additions, totaling $1,054,583, were recorded 344 to 753 days late.
- DoIT did not record on its property listing and did not report on annual inventory report submitted to CMS a voucher for the purchase of equipment totaling $1,929,406.
- Three of 60 (5%) property additions, totaling $142,036,908, were not properly recorded in the ERP, resulting in an overstatement of $26,339,417.

Property Deletions and Unlocated Computers

- Eleven of 60 (18%) property deletions, totaling $11,925, were recorded 32 to 1,815 days late.
- Three of 60 (5%) property deletions, totaling $75,417, were recorded with improper transaction codes.

- Thirteen of 60 (22%) unlocated computers, totaling $28,660, were reported as missing items in the Annual Inventory Certification, although these items were still active and in use.
- Six of 60 (10%) Certificates of Media Sanitization (Certificates) tested were not properly completed. The Certificates had incorrect tag numbers, serial numbers, and were not dated.
- DoIT did not provide documentations to determine if:
  - Six of 60 (10%) property deletions totaling $10,417, were properly processed, approved, supported, and timely recorded;
  - Nine of 60 (15%) computers disposed of, totaling $10,488, had confidential data and were properly wiped; and
  - Forty-five of 60 (75%) unlocated computers, totaling $76,165, had confidential information stored and were properly wiped.

Physical observation of equipment
During testing, auditors noted:

- Twenty eight of 60 (47%) items, totaling $92,742, were not found at the location indicated on the Department's property listing.
- Thirteen of 60 (22%) items, totaling $55,924, were assigned an incorrect location code.
- Sixty of 60 (100%) surplus items had not been recycled, issued, or reported as transferable property to CMS.
- Ten of 61 (16%) items were not recorded in the property records as well as in the Annual Inventory Certification submitted to CMS.

This finding was first reported during the period ended June 30, 2018. In the subsequent years, DoIT has been unsuccessful in implementing appropriate corrective action or procedures to remedy this deficiency.

DoIT management indicated the exceptions noted were due to lack of resources, lack of staff preventing the Department's ability to be more proactive, and conflicting priorities.

Failure to maintain controls over the property and related records has resulted in the Department's property records and subsequent reporting to CMS and the Office of Comptroller being inaccurately reported.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. Both the accounting and property control departments are working independently and together to streamline processes.

UPDATED RESPONSE;
Partially Implemented. DoIT has a property control policy in place. Also, based on additional asset information that is now being collected in ServiceNow, the accuracy of DoIT's C-15 reports is improved.

3. The auditors recommend DoIT work with the agencies to ensure risk assessments are conducted for all State agencies to comply with the Act and maintain documentation demonstrating the population of risk assessments is complete.

FINDING: *(Failure to Conduct Risk Assessments for All State Agencies) - New*

DoIT failed to conduct risk assessments for all state agencies as required by the Illinois Information Security Improvement Act (Act).

Auditors testing of DoIT's risk assessment documentation noted:

- Five of eight (63%) risk assessments identified as completed in fact had not been completed during FY21.
- DoIT did not provide documentation demonstrating the population of risk assessments conducted during FY22 was complete and accurate. Therefore, auditors were unable to conduct detailed testing.

DoIT management indicated the lack of resources has delayed completion of the risk assessments for all state agencies and resulted in the inability to provide documentation demonstrating the FY22 population was complete.

Failure to conduct risk assessments for all State agencies is a violation of the Act.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. DoIT is working to add more resources to the Information Security Division to address capacity constraints.

UPDATED RESPONSE:
Partially Implemented. DoIT has posted positions and is currently interviewing candidates for the Risk and Compliance units of the Information Security division. DoIT is currently implementing an Integrated Risk Management (IRM) platform to facilitate risk assessments with state agencies.

4. The auditors recommend the Department:

- **Update the policy to:**
- **establish implementation guidance or detailed procedures to manage user responsibilities,**
- **acceptable use of remote access,**
- **authorization for each type of remote access allowed,**
- **configuration or connection requirements,**
- **compliance to laws, rules and regulations applicable to the Department,**
- **incident/breach notification requirements,**
- **monitor the activities of remote access users, and**
- **perform periodic reviews of users' remote access.**
- **ensure remote access requests are properly documented and authorized.**

- **perform periodic review of remote access users and ensure timely deactivation of users no longer needing access.**

FINDING: *(Inadequate Controls over Remote Access) - New*

DoIT had not documented and implemented adequate procedures governing remote access to DoIT's information systems.

During testing of four remote access users, auditors noted:

- Remote users' access requests did not document the details of the request, such as the reason and duration of remote access.
- Remote access users did not have a documented access request on file and did not acknowledge receipt and understanding of the security policies.

Department management indicated the issues were due to oversight.

Failure to establish and implement adequate procedures related to security and control of remote access increases the risk of unauthorized access and inappropriate usage of Department resources.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. DoIT will develop appropriate standards and documentation related to remote access.

UPDATED RESPONSE:
Partially Implemented. DoIT has implemented additional user security controls addressing remote access and is working to implement improved user authorization tools in conjunction with the SAP Human Capital Management (HCM) HR system. DoIT has implemented remote access user instructions and documentation.

5. The auditors recommend DoIT develop a methodology for determining the administrative markup. Additionally, they recommend DoIT post the current rates on its website and bill for services monthly.

FINDING: *(Lack of Review of Billing Rates) – First reported 2018, last 2020*

DoIT did not review the billing rates utilized to bill agencies for Information Technology (IT) and telecommunication services.

During their testing, auditors noted:

- DoIT adds an administrative mark up to the telecommunication rate; however, DoIT had not developed a methodology to determine the administrative mark up.
- DoIT did not bill for server and the State's Enterprise Resource Planning System (ERP) usages in a timely manner. The server usage was billed annually in FY21 and quarterly in FY22 and the ERP usage was billed semi-annually instead of

monthly.
- There were several IT service rates posted on DoIT's website which differed from DoIT's approved rates. Additionally, the list of IT service rates on DoIT's website included a service no longer being offered.

This finding was first reported during the period ended June 30, 2018. In the subsequent years, DoIT has been unsuccessful in correcting this deficiency.

DoIT management indicated the methodology had not been sufficiently documented due to lack of staff and the other issues were due to oversight.

Failure to review the various rates, establish a methodology for determining rates, and timely bill the agencies, DoIT may be under or over charging agencies for the usage of their services.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. The administrative mark-up to the telecommunication rate has historically been a cost-plus cost methodology, which has been implemented for many years. The mark-up is reviewed and evaluated through the annual SWCAP to determine if there are large over- or under-recovery occurring. To date, there has not been significant overcharges or undercharges occurring in that category.

UPDATED RESPONSE:
Partially Implemented. DoIT is reviewing the telecom rates based on the now completed FY22 SWCAP to determine if the current methodology for determining the markup is still viable. DoIT's current rates are located on the website.

6. **The auditors recommend DoIT ensure complete, accurate, and detailed records are maintained to substantiate its midrange environment. Additionally, they recommend DoIT:**
   - **Upgrade or update servers to current vendor recommended patch or service pack levels;**
   - **Ensure all servers are running antivirus software, with current definition files; and**
   - **Ensure separated individuals' access is timely terminated.**

FINDING: *(Inadequate Security and Control over Midrange Environment) – First reported 2018, last 2020*

DoIT had not implemented adequate security and controls over the midrange environment.

Auditors requested DoIT provide a population of servers utilized in order to determine the controls over the midrange servers. In response, DoIT provided a population; however, the population of servers was incomplete. Due to these conditions, they were unable to conclude DoIT's population records were complete and accurate under the Professional

Standards promulgated by the American Institute of Certified Public Accountants (AT-C § 205.36).

Even given the population limitations noted above, auditors performed testing on the population of servers identified. During their testing, auditors noted:

- Servers running unsupported and outdated operating systems, and;
- Servers without anti-virus software.

In addition, they noted two of 223 (1%) terminated individuals continued to have high level access to the environment.

This finding was first reported in FY18. In subsequent years, DoIT has been unsuccessful in implementing appropriate procedures to improve its controls over midrange security.

DoIT management indicated the issues were due to competing priorities.

Failure to implement adequate security and controls over the midrange environment increases the risk of unauthorized access and heightens the vulnerability to existing or emerging threats.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. DoIT will continue to address outdated legacy systems. Efforts to implement identity and access automation are also underway.

UPDATED RESPONSE:
Partially Implemented. DoIT is continuing to improve the Information Technology Operations Management (ITOM) platform to improve upon the accuracy of the server inventory. DoIT is continuing to upgrade outdated legacy servers and communicate server vulnerabilities to customer agencies. DoIT is continuing to modernize security software deployed on state devices and is working to implement identity and access automation in conjunction with the HCM HR implementation.

7. The auditors recommend DoIT ensure timely deactivation of users no longer needing access.

FINDING: (Weaknesses over System Access) – First and last reported 2020

DoIT had not established adequate controls over system access.

During their testing of the system access controls over the domain, remote access, and the Enterprise Resource Planning (ERP) system, they noted:

- Two of 223 (1%) terminated individuals' access to the Department's domain and remote access system was not revoked, and

- Four of 223 (2%) terminated individuals' access to the Department's ERP was not timely revoked. The terminated individuals' access was revoked 3 to 164 days after separation.

DoIT's Access Control Policy requires DoIT to revoke user access when a user is no longer authorized such as user termination, user transfer, or changes to user job responsibilities.

DoIT management indicated the issues were due to oversight.

Failure to timely remove access of terminated individuals increases the risk of unauthorized access to DoIT resources and the risk that confidentiality, integrity, and availability of systems and data will be compromised.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. DoIT will be automating additional identity and access controls in coordination with the implementation of the Human Capital Management solution.

UPDATED RESPONSE:
Under Study. Implementation of this recommendation is tied to the go live of the HCM HR system.

8. The auditors recommend DoIT process proper bills within 30 days of receipt and ensure vouchers are properly supported.

FINDING: *(Voucher Processing Weakness) – First reported 2018, last 2020*

DoIT did not timely submit its vouchers for payment to the Comptroller's Office and ensure vouchers were properly supported and recorded during the examination period.

Due to their ability to rely upon the processing integrity of the Enterprise Resource Planning System (ERP), they were able to limit the auditors voucher testing at DoIT to determine whether certain key attributes were properly entered by DoIT's staff into ERP. In order to determine the operating effectiveness of DoIT's internal controls related to voucher processing and subsequent payment of interest, the auditors selected a sample of key attributes (attributes) to determine if the attributes were properly entered into the ERP based on supporting documentation. The attributes tested were 1) vendor information, 2) expenditure amount, 3) object(s) of expenditure, and 4) the later of the receipt date of the proper bill or the receipt date of the goods and/or services.

The auditors then conducted an analysis of DoIT's expenditures data for FY21 and 2022 to determine compliance with the State Prompt Payment Act (Act) (30 ILCS 540) and the Illinois Administrative Code (Code) (74 Ill. Admin. Code 900.70).

Auditors noted the following noncompliance:

- DoIT did not timely approve 6,267 of 23,709 (26%) vouchers processed during the examination period, totaling $576,052,039. They noted these late vouchers were approved between 1 and 383 days late.
- One of 25 (4%) travel vouchers, totaling $234, was not properly supported.

This finding was first reported during the period ended June 30, 2018. In the subsequent years, DoIT has been unsuccessful in implementing appropriate corrective action or procedures to remedy this deficiency.

DoIT management indicated the delay in approving vouchers was due to the layered approval process prior to vouchering. DoIT management also indicated the other issue were due to oversight.

Failure to timely process bills and ensure vouchers are properly recorded and supported represents noncompliance with the Code.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. DoIT will work to approve invoices quicker to enable timely voucher processing. DoIT will also strive to minimize the human error that resulted in insufficient supporting documentation for one travel voucher.

UPDATED RESPONSE:
Partially Implemented. DoIT has communicated to end users about the urgency for Fiscal to receive approved invoices timely to have sufficient time to process the invoices within the 30 days. In addition, there are now weekly reminders sent to end users when they have pending invoice approvals.

9. The auditors recommend DoIT adopt formal rules for the operation, administration, and accounting of the Department.

FINDING: *(Failure to Adopt Formal Departmental Rules) – First reported 2018, last 2020*

DoIT had not adopted formal rules for the operation, administration, and accounting of the Department.

During their examination, auditors noted DoIT had not drafted or adopted formal rules related to accounting and personnel.

This finding was first reported during the period ended June 30, 2018. In the subsequent years, DoIT has been unsuccessful in implementing appropriate corrective action or procedures to remedy this deficiency.

DoIT management indicated they utilized the CMS' policies and procedures due to limited resources available to establish DoIT rules.

Failure to establish Departmental rules is a violation of State law.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation.

UPDATED RESPONSE;
Implemented. DoIT has adopted formal rules in accordance with the Illinois Administrative Procedure Act and has drafted and implemented procedures related to the operation, administration, and accounting of DoIT.

10. The auditors recommend DoIT ensure planned audits are completed and the two- year internal audit plans are approved by the chief executive officer of DoIT to comply with the Act and Standards.

FINDING: *(Failure to Comply with the Fiscal Control and Internal Auditing Act) – First reported 2018, last 2020*

DoIT failed to comply with the Fiscal Control and Internal Auditing Act (Act).

During their testing of DoIT's internal auditing activities, auditors noted the following:

- Four of eight (50%) audits proposed to be performed in FY21 were not completed. Additionally, they noted reviews of all major systems of internal accounting and administrative control were not conducted on a periodic basis so all major systems were reviewed at least once every two years.
- DoIT's FY21 two-year internal audit plan did not have documentation of the submission date and approval by the chief executive officer DoIT.

This finding was first reported during the period ended June 30, 2018. In the subsequent years, DoIT has been unsuccessful in implementing appropriate corrective action or procedures to remedy this deficiency.

DoIT management indicated lack of resources contributed to the exceptions.

Failure to ensure audits are conducted and internal audit plans are approved is a violation of the Act and Standards.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation.

UPDATED RESPONSE:
Implemented. Since the Department's current Chief Internal Auditor was hired in 2021, DoIT has not had any issues with FCIAA compliance.

11. The auditors recommend DoIT develop and implement procedures and a tracking mechanism to control, monitor, and track software licenses and its

utilization. Furthermore, DoIT should at least annually reconcile their software license inventory to vendor software inventory to ensure software is deployed in accordance with the terms of procurement.

FINDING: *(Failure to Control and Monitor Software Licensing) – First reported 2018, last 2020*

DoIT had not developed procedures for controlling, monitoring, and tracking the use of software licenses. In addition, DoIT could not provide an inventory of software licenses purchased and the number of software licenses that were actually deployed. As a result, they were unable to determine if DoIT was in compliance with contractual licensing agreements.

This finding was first reported in FY18. In subsequent years, DoIT has failed to implement appropriate procedures to improve its controls over software licensing.

DoIT management indicated procedures for monitoring and tracking software licenses were not formalized in writing due to the lack of resources.

Failure to track, control, and monitor software license usage leaves DoIT, and user agencies exposed to possibility of additional costs, including fees, penalties, litigation and possibility of the termination of software usage.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation.

UPDATED RESPONSE:
Partially Implemented. DoIT tracks and performs an annual reconciliation for Adobe and Microsoft licenses--our largest volume for enterprise licenses. In order to implement this recommendation for all software licenses, DoIT will need to increase its personnel levels on the software and procurement teams.

12. The auditors recommend DoIT ensure controls are suitably designed and implemented to protect computer systems and data. In addition, they recommend DoIT maintain complete and accurate populations and implement general IT controls.

FINDING: *(Weaknesses in the IT Internal Control Environment) – First reported 2018, last 2020*

Information Technology (IT) had weaknesses in the implementation and documentation of IT internal controls.

DoIT did not provide complete and accurate populations.

Due to these conditions, auditors were unable to conclude DoIT's population records were sufficiently precise and detailed under the Attestation Standards promulgated by the American Institute of Certified Public Accountants (AT-C § 205.36). As such, they could not perform testing.

In addition, their testing of the Department's IT controls, noted:

Policies and Procedures

- DoIT did not have a policy or procedure documenting the frequency in which policies and procedures published on its website were to be reviewed during FY21.
- DoIT did not ensure compliance with all of the enterprise information security policies.
- The Change Management Guide and the Change Management Process did not document:
    - Change prioritization requirements;
    - Required fields to be completed for each type of change;
    - Documentation requirements for Post Implementation Reviews;
    - Documentation requirements for testing, implementation and backout plans; and
    - The approval process in place.

- DoIT's change management guides and process documents contradicted one another.
- The Application Lifecycle Management Manual did not document the responsibilities of the Change Management Team and the Change Advisory board.
- DoIT did not document the access provisioning requirements in order for staff and vendors to gain access to network devices.
- DoIT had not documented the internal controls over modification and revocation of mainframe access.
- DoIT did not have a policy documenting the required timeframe for revocation of logical access upon termination.

Change Management

- Changes did not have completed change request forms.
- Defects did not have support for testing in the various environments.
- Changes did not always have test plans, backout plans, or implementation plans.
- Changes were not properly approved.
- Not all changes were reviewed monthly.
- Emergency changes did not always have a Post Implementation Review conducted.
- Mainframe application changes were not always properly authorized prior to moving to the code management system.
- Mainframe application changes were not always approved prior to releasing to Library Services.
- eTime changes were not properly approved prior to deploying to the production environment.

- The Endpoint Protection Group did not follow the Department's Change Management Process.

Logical Security

- Documentation demonstrating separated employees' and contractors' midrange logical access was revoked was not provided for all of the instances selected.
- Separated employees and contractors did not have a completed service request in order to remove their logical access, or the service request was completed late.
- Documentation demonstrating access with powerful privileges, high-level access and access to sensitive system functions was restricted to authorized personnel was not provided.
- Documentation demonstrating separated employees' and contractors' mainframe accounts had been revoked was not provided for all of the instances selected.
- Service requests or exit forms were not always completed for separated employees and contractors.
- New requests for access to DoIT's resources were not always properly approved.
- New employees and contractors did not have a completed service request and/or Mainframe Access Request Form in order to request their logical access.
- DoIT did not conduct the Security Software Annual Reconciliation.
- Security settings did not always conform to DoIT's or vendor's standards.

Physical Security

- Physical security controls were not always properly implemented.
- Documentation demonstrating separated or terminated individuals' physical access had been deactivated was not provided.
- New employee and contractor badge request forms were not always properly completed or did not contain documentation of proof of identity.
- New employees' and contractors' access to the data center's secured location was not always approved.
- Individuals were provided inappropriate access to DoIT's buildings.
- The Building Admittance Registers were not always maintained.
- Monitoring of cameras at a DoIT facility was not conducted.

Security Violations

- Thresholds had not been established to determine which violations were followed up on.
- Mainframe monitoring reports were not always completed and distributed monthly.
- The Incident Management Response Process Guide had not been updated to reflect the transition of service management tools and processes.
- Security incidents did not always contain notification to the agency, documentation the Executive Summary or Incident Report was provided to the affected agency, and status updates.

Backups

- Documentation demonstrating the replication between DoIT's data center and alternate data center occurred and the Enterprise Storage and Backup group received an alert if the data was out of sync for a defined period of time was not provided.
- Midrange server backup reports were not provided for all of the instances selected.
- Remediation efforts for specific midrange backups were not documented.

Human Resources

- The specified required background checks were not always completed.

Risk

- Vulnerability scans were not communicated to all Group Chief Information Officers and Agency Chief Information Officers.
- Upon notification of the closure of medium and high priority threats, Executive Summaries were not sent to the Chief Information Security Officer or the Deputy Chief Information Security Officer.
- An agency was not notified of a medium threat in order to determine the impact to users.
- Guidance was not provided to the agencies related to the remediation of identified vulnerabilities.

Network

- Multiple instances where operating system patches were not tested or did not have documentation of testing prior to being pushed to the general population.
- A Network Administrator did not require administrative rights to the environment.
- Device configurations were not backed up for the period of April 5 to April 23, 2021.

Application Edits

- One states' tax rate was incorrect in the CPS tax tables.
- The federal rate for head of household filers was incorrect.

This finding was first reported in the FY18 Compliance Examination Report. DoIT has failed to implement corrective actions to remedy the weaknesses.

DoIT management indicated the weaknesses were due to lack of resources and system limitations.

Failure to provide internal controls that were suitably designed and operating effectively may result in security weaknesses and data integrity concerns.

DEPARTMENT RESPONSE:

DoIT accepts the finding and recommendation. The weaknesses in internal controls in this finding are summarized in DoIT's SOC reports from FY21 and FY22. Those reports contain the detailed corrective action plans that are being implemented by DoIT to strengthen internal controls.

UPDATED RESPONSE:
Partially Implemented. DoIT is continuing to improve the Information Technology Operations Management (ITOM) platform to improve upon the accuracy of the server inventory.

13. The auditors recommend DoIT strengthen its internal controls to monitor employees to ensure all employees complete the required trainings and in a timely manner.

FINDING: *(Trainings Not Completed Within the Required Timeframe) - New*

DoIT employees did not complete all mandatory trainings within the required timeframe.

The auditors reviewed DoIT's training reports for all employees to determine if they had complied with training requirements, noting:

- Two employees did not complete the annual ethics training during the CY 2020 and 2021 training period. Additionally, one employee completed the CY 2020 ethics training five days late. Further, one of 14 (7%) new hires tested completed the initial ethics training 23 days late during the CY 2020 training period.
- One employee did not complete the sexual harassment training during the CY 2021 training period.
- Three employees did not complete the training for employees handling social security numbers during the CY 2021 training period.

DoIT management indicated the lack of workforce resources resulted in the exceptions.

Failure to complete trainings within the required timeframe may lead to employees being unaware of specific requirements for State employees and DoIT and State policies regarding cybersecurity, ethics, sexual harassment, and safeguard of confidential information. As a result, there is a risk DoIT could be exposed to legal and financial risks due to noncompliance with the Act.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. DoIT will continue efforts to ensure that mandatory trainings are completed in a timely manner.

UPDATED RESPONSE:
Partially Implemented. DoIT is increasing messaging to managers to ensure employee compliance with training requirements.

14. The auditors recommend DoIT ensure overtime pre-approval requests are timely submitted, approved in advance, and properly completed.

FINDING: *(Failure to Timely Approve or Submit Overtime Requests) – First reported 2018, last 2020*

DoIT failed to timely approve or submit overtime requests.

DoIT paid $14,054,296 for approximately 116,048 hours of overtime during FY21 and FY22. Based on their testing of a sample of 60 employee overtime pre-approval requests and time report details, auditors noted:

- Four (7%) employees did not submit overtime pre-approval requests in advance of the time to be worked. These requests were submitted one to seven days after the overtime was worked.
- For four (7%) employees, the overtime pre-approval requests totaling 38 hours were not pre-approved by the supervisors. These requests were approved one to four days after the overtime had been worked.
- For one (2%) employee, the actual overtime worked exceeded the approved overtime request by 6.50 hours.

This finding was first reported during the period ended June 30, 2018. In the subsequent years, DoIT has been unsuccessful in implementing appropriate corrective action or procedures to remedy this deficiency.

DoIT management indicated the exceptions were due to employee oversight.

Failure to ensure pre-approved overtime requests are timely submitted and properly approved in advance undermines accountability controls and may result in unnecessary expenditures.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. DoIT will continue efforts to ensure that overtime pre-approval requests are timely submitted by employees and properly approved in advance by supervisors.

UPDATED RESPONSE:
Partially Implemented. DoIT is increasing messaging to managers about overtime approvals to assist in resolving these failures.

15. The auditors recommend DoIT ensure the I-9 forms are maintained in the personnel records to comply with federal laws.

FINDING: *(Inadequate Controls over the Maintenance of I-9 Forms) – First and last reported 2020*

DoIT has not established adequate controls over the maintenance of Employment Eligibility Verification (I-9) forms for employees hired by DoIT.

During their testing of 60 employees' personnel files, auditors noted eight (13%) I-9 forms were not maintained in the employees' personnel files.

Federal law (8 U.S.C. § 1324a) requires an employer to complete and maintain an I-9 form to verify an individual's eligibility for employment in the United States.

DoIT management indicated the referenced I-9 forms were not included in the employee personnel files forwarded to DoIT by the transferring agencies.

Failure to maintain I-9 forms is a violation of federal laws and could expose the Department to penalties.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. Personnel files from transferring agencies were forwarded to DoIT upon legislative transfer of these employees, and some files did not include the I-9 forms.

UPDATED RESPONSE:
Implemented. DoIT is now conducting a pre-review of employee files as part of the transition process when employees are being transferred to department payroll.

16. The auditors recommend DoIT:

- **Ensure formal risk assessments are performed to identify and ensure adequate protection of information (i.e., confidential, or personal information) most susceptible to attack,**
- **Prioritize, evaluate, and implement appropriate risk-reducing controls for the environment,**
- **Ensure all types of data are identified and classified to ensure proper safeguards, and**
- **Ensure all employees complete the required annual cybersecurity training.**

FINDING: *(Weakness in Cybersecurity Programs and Practices) – First and last reported 2020*

DoIT had not implemented adequate internal controls related to cybersecurity programs and practices.

As a result of DoIT's responsibility to provide State agencies with information technology, large volumes of confidential and personal information, such as names, addresses, Social Security numbers, health information, etc., reside at DoIT.

During their examination of DoIT's cybersecurity program, practices, and control of confidential information, they noted the Department:

- Had not ensured formal risk assessments were performed to identify and ensure adequate protection of information (i.e., confidential, or personal information) most susceptible to attack.
- Had not prioritized, evaluated, and implemented appropriate risk-reducing controls for the environment.
- Had not ensured all types of data were identified and classified to ensure proper safeguards.
- Five employees did not complete the annual cybersecurity training timely during the Calendar Year (CY) 2020 training period. These employees completed the training from six to 62 days late. Additionally, two employees did not complete the annual cybersecurity training during the CY 2021 training period.

DoIT management indicated the issues were due to competing priorities and oversight.

The lack of adequate cybersecurity programs and practices could result in unidentified risk and vulnerabilities and ultimately lead to DoIT's volumes of confidential and personal information being susceptible to cyber- attacks and unauthorized disclosure.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation.

UPDATED RESPONSE:
Partially Implemented. DoIT has posted positions and is currently interviewing candidates for the Risk and Compliance units of the Information Security division. DoIT is currently implementing an Integrated Risk Management (IRM) platform to facilitate risk assessments and data classification with state agencies. DoIT will continue to work to ensure all employees complete annual cybersecurity training.

17. The auditors recommend DoIT obtain SOC reports and bridge letters or conduct an independent review in a timely manner. Additionally, we recommend DoIT ensure contracts with service providers are not expired and contain requirements for the service provider to notify DoIT in the event of a security incident or information breach.

FINDING: *(Lack of Adequate Controls over the Review of Internal Controls over Service Providers) – First reported 2018, last 2020*

DoIT lacked adequate controls over the review of internal controls over service providers.

DoIT utilizes service providers for a variety of services; software-as-a- service, hosting services, identity as a service, etc. During their review of DoIT's controls over the service providers, they noted:

- System and Organization Control (SOC) reports and bridge letters were not obtained in a timely manner.
- SOC reports were not obtained or independent review were not conducted.

- Bridge letters were not obtained.
- SOC reports were not timely reviewed.

In addition, it was noted the service providers' contracts did not contain requirements for the service provider to notify DoIT in the event of a security incident or information breach. Further, although 2 of 15 (13%) service providers continued to provide services, the contracts had expired.

This finding was first reported in the Fiscal Year 2018 Compliance Examination Report. DoIT has failed to implement corrective actions to remedy the weaknesses.

DoIT management indicated the exceptions were due to the lack of resources.

Without obtaining and timely reviewing SOC reports, bridge letter, or another form of independent internal control reviews, DoIT does not have assurance the service providers' internal controls are adequate.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation.

UPDATED RESPONSE:
Partially Implemented. DoIT has established procedures for SOC or other independent control reviews. In addition, DoIT will ensure that contracts continue to contain independent review (audit) language.

18. The auditors recommend DoIT implement adequate controls to ensure reconciliations are completed timely and contain documentation of independent review.

FINDING: *(Inadequate Controls over Monthly Reconciliations) – First reported 2018, last 2020*

DoIT did not maintain adequate controls over monthly obligations, expenditures, revenue status, and cash balance reconciliations.

During their testing of the monthly reconciliations between the Office of Comptroller's (Comptroller) records and DoIT records, they noted:

- For the Agency Contract Reports (SC14)
    - Twenty-two of 24 (92%) reconciliations did not contain documentation of the preparer and preparation date; therefore, the timeliness of preparation could not be determined.
    - Twenty-four of 24 (100%) reconciliations did not contain documentation of independent review.

- For the Monthly Appropriation Status Reports (SB01):

  - Six of 32 (19%) reconciliations were not reviewed timely. The reconciliations were reviewed 23 to 162 days late.

- For the Monthly Revenues Status Reports (SB04):
  - Five of 24 (21%) reconciliations did not contain documentation of the preparer and preparation date; therefore, the timeliness of preparation could not be determined.
  - Twenty-four of 24 (100%) reconciliations did not contain documentation of independent review.

- For the Monthly Cash Reports (SB05):
  - Nine of 24 (38%) reconciliations were not prepared timely. The reconciliations were completed in 9 to 252 days late.
  - Twenty-four of 24 (100%) reconciliations did not contain documentation of independent review.

The finding was first reported during the period ended June 30, 2018. In the subsequent years, DoIT has been unsuccessful in implementing appropriate corrective action or procedures to remedy this deficiency.

DoIT management indicated the exceptions were due to lack of staffing and conflicting priorities. The SB04 and SB05 reconciliations were prepared and reviewed by an outside accounting consulting firm during the examination period and the review process was not formally documented.

Failure to timely prepare and review reconciliations increases the risk of undetected loss or theft and could lead to unresolved differences between DoIT and Comptroller records and inaccurate financial reporting.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation.

UPDATED RESPONSE:
Partially Implemented. DoIT is reliant on an outside accounting firm to prepare reconciliations, but is reviewing them in house in a timely manner. DoIT is also documenting the preparation and review process.

19. The auditors recommend DoIT ensure collection letters are sent timely.

FINDING: *(Inadequate Controls over Collection Efforts) – First reported 2018, last 2020*

DoIT did not maintain adequate controls over collection efforts of delinquent accounts.

During their testing of 60 delinquent accounts receivable, DoIT did not provide collection letters to State agencies for 8 (13%) delinquent accounts. Therefore, they could not determine if collection letter had in fact been sent.

This finding was first reported during the period ended June 30, 2018. In the subsequent years, DoIT has been unsuccessful in correcting this deficiency.

DoIT management indicated the issues were due to errors within the Enterprise Resource Planning System (ERP) causing certain state collection letters to not be sent when there were sufficient unused credits on the account to cover past due balances.

Failure to make collection efforts increases the risk of loss of revenues. In addition, failure to establish and maintain adequate controls over accounts receivable is noncompliance with state laws and regulations.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. A unique programming situation in ERP caused certain state collection letters not to be sent in limited situations. The Department became aware of this combination and has submitted two Change Request (CR) tickets to correct the ERP programming to prevent these limited circumstance situations from occurring again, and one ticket has been completed.

UPDATED RESPONSE:
Implemented. The system logic that caused a small number of collection letters in a limited situation not to be sent timely has been remedied through the Change Request tickets.

20. The auditors recommend DoIT ensure:

- **Vehicle maintenance is completed as required by the Code;**
- **Vehicle usage is optimized; and**
- **Accident reports are properly completed and filed timely.**

In addition, they recommend DoIT prepare, maintain, and submit to CMS its vehicle use policy which covers procedures concerning take-home vehicles and daily vehicle use logs and mileage recording.

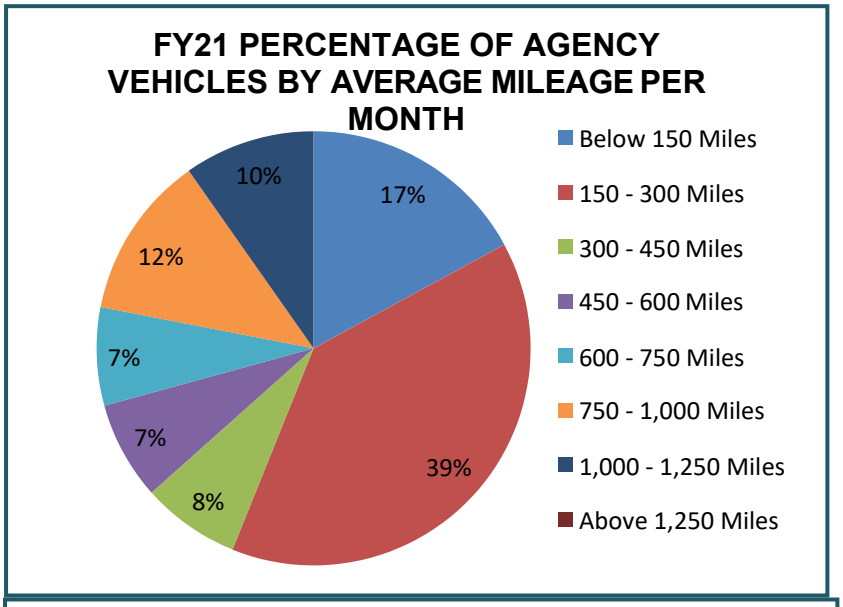
FINDING: *(Inadequate Controls over State Vehicles) – First reported 2018, last 2020*

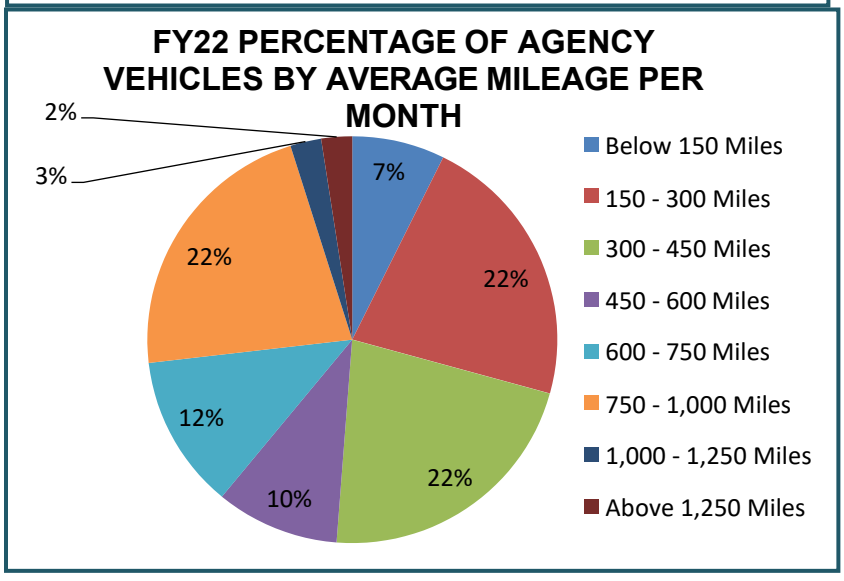
DoIT did not exercise adequate controls over State vehicles.

Maintenance
The Department's fleet consisted of 41 vehicles at June 30, 2022 and 2021.

DoIT did not ensure its vehicles were properly maintained during the engagement period. During their testing of ten vehicle maintenance records, auditors noted one (10%) vehicle did not undergo an annual inspection and oil change.

The auditors analyzed the total activity of the Department's vehicles used during FY21 and FY22. DoIT's vehicles traveled between 468 and 14,509 miles during FY21 and 910 and 32,391 miles during FY22, with the following charts showing the average monthly vehicle utilization:





Auditors noted the following underutilized vehicles during Fiscal Years 2021 and 2022:

Fiscal Year	Year	Make	Odometer at Year End	Total Usage	Average Monthly Usage
FY2021	2006	Ford	74,197	1,694	141
FY2021	2006	Ford	53,519	1,382	115
FY2021	2006	Ford	79,409	659	55
FY2021	2007	Ford	52,137	1,247	104
FY2021	2015	Ford	77,168	468	39
FY2021	2014	Dodge Caravan	40,002	1,349	112
FY2022	2006	Ford	182,868	1,240	103
FY2022	2006	Ford	80,420	910	76
FY2022	2006	Ford	95,021	1,507	126

Accident Reports

During their testing of accidents involving state vehicles, auditors noted:

- Two of seven (29%) vehicle accident reports were not properly completed. One report was not dated therefore, timeliness of completion cannot be determined. The other report did not disclose the driver's policy number and details of the insurance carrier.
- One of seven (14%) vehicle accident report was completed 4 days late.
- One of seven (14%) vehicle accident report was submitted to CMS' Auto Liability Unit 12 days late.

Vehicle Use Policy

Auditors reviewed DoIT's vehicle use policy, noting:

- DoIT utilized CMS' Vehicle Guide and policies, therefore, DoIT has not prepared, maintained, and submitted to CMS its own vehicle use policy.
- The Vehicle Guide and policies used by the Department did not include requirements and procedures concerning take-home vehicles and daily vehicle use logs and mileage recording.

This finding was first reported during the period ended June 30, 2018. In the subsequent years, DoIT has been unsuccessful in implementing appropriate corrective action or procedures to remedy these deficiencies.

DoIT management indicated the issues noted were due to stay at home restrictions and hybrid work schedules implemented within the state as well as competing priorities and oversight.

Failure to properly maintain vehicles may result in low fuel economy and exposure to safety issues. Failure to timely file accident reports and to draft the vehicle use policy are violations of the Code.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. DoIT no longer has individually assigned vehicles.

UPDATED RESPONSE:
Implemented. DoIT has prepared and maintains a vehicle use policy and procedures and has submitted to CMS.

21. The auditors recommend DoIT complete employee performance evaluations in a timely manner as required by the Code.

FINDING: *(Employee Performance Evaluations Not Conducted Timely) – First reported 2018, last 2020*

DoIT did not conduct employee performance evaluations in a timely manner.

Auditors sampled 60 employees to test the performance evaluations conducted during the examination period. A total of 77 evaluations should have been completed, including three-month new hire evaluations, four-month probationary evaluations, six-month probationary evaluations, and annual evaluations. During their testing, auditors noted 32 of 77 (42%) employees' performance evaluations were not completed timely, ranging from 1 to 358 days late.

The finding was first reported during the period ended June 30, 2018. In the subsequent years, DoIT has been unsuccessful in implementing appropriate corrective action or procedures to remedy this deficiency.

DoIT management indicated the lack of workforce resources resulted in the exceptions.

Performance evaluations are a systematic and uniform approach used for the development of employees and communication of performance expectations to employees. Failure to conduct timely employee performance evaluations delays formal feedback on an employee's performance, delays communication of areas for improvement, and delays communication of the next year's performance goals and objectives. In addition, employee performance evaluations serve as a foundation for salary adjustments, promotions, demotions, discharge, layoff, recall, or reinstatement decisions.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. DoIT will continue to enforce efforts to ensure the managers complete evaluations on a timely basis.

UPDATED RESPONSE:
Partially Implemented. DoIT is continuing messaging to managers to assist with resolving these failures. The go-live of the HCM system will assist with tracking and automating communication of these requirements.

22. The auditors recommend DoIT strengthen its controls to ensure the proper completion, and accurate and timely filing of contracts and related documents, including ensuring submission of Late Filing Affidavits when necessary.

FINDING: *(Inadequate Controls over Contractual Agreements) – First reported 2018, last 2020*

DoIT did not have adequate controls over contractual agreements to ensure they were timely filed, properly completed, and accurately reported.

During their testing of 60 contractual agreements, auditors noted:

- Eight (13%) contractual agreements, totaling $9,473,194, were not timely filed with the Office of Comptroller (Comptroller). The contractual agreements were filed four to 271 days late. Additionally, DoIT did not file Late Filing Affidavits.

- For twenty-five (42%) contracts, the Contract Obligation Documents (CODs) were not properly completed. Specifically:
    - Nine CODs, totaling $8,969,127, included incorrect Illinois Procurement Bulletin/Bidbuy publication dates.
    - Five CODS, totaling $7,709,152, indicated terms that were not consistent with the terms of the contracts.
    - One COD, totaling $65,000 has an incorrect Bidbuy reference number.
    - Eighteen CODs, totaling $22,424,854, had vendor addresses different from the addresses stated in the contracts.
    - One COD did not state the correct annual contract amount. The annual amount entered in the COD was $2,000,000, however, the annual amount reported in the SC-14 Report was $500,000.

- Nine (15%) contractual agreements, totaling $11,954,122, did not contain the required conflict of interest disclosure. Two of these contractual agreements also did not have the required disclosure of financial interest statement. Further, one contractual agreement did not contain the standard vendor certification and FEIN document requirement.

The finding was first reported during the period ended June 30, 2018. In the subsequent years, DoIT has been unsuccessful in implementing appropriate corrective action or procedures to remedy this deficiency.

DoIT management indicated the issues noted were due to oversight.

Failure to file contractual agreements in a timely manner and submit late filing affidavits as required is noncompliance with the Code. The lack of proper controls over contract obligation documents may result in inaccurate recording and a lack of accountability by DoIT. Further, failure to contain the material terms of the contract leaves DoIT exposed to liabilities and potential legal issues.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation.

UPDATED RESPONSE:
Implemented. DoIT reviews the contract paperwork at different levels in advance of submitting the contracts to the IOC for filing to ensure a more accurate package being submitted and to reduce errors and speed up the contract acceptance process.

23. The auditors recommend DoIT strengthen its controls to ensure employees' time reports are completed and submitted in a timely manner.

FINDING: *(Employee Time Reports Not Timely Completed) – First reported 2018, last 2020*

DoIT did not implement adequate controls over employee time reporting.

The auditors tested a sample of 174 employees Daily Time Reports, noting 32 (18%) were not completed timely. Completion of the Daily Time Report was one to 53 days late. DoIT expended $136,122,208 and $146,220,100 for payroll during FY21 and FY22, respectively.

This finding was first reported during the period ended June 30, 2018. In the subsequent years, DoIT has been unsuccessful in implementing appropriate corrective action or procedures to remedy this deficiency.

DoIT management indicated, barring extenuating circumstances such as vacations, holidays, illness and/or leaves, this is due to employee oversight.

Failure to maintain adequate controls over employee time reporting increases the risk of DoIT paying for services not rendered by the employees.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation. DoIT will continue efforts to ensure the managers enforce that employee time reports are completed, submitted, and approved timely by supervisors.

UPDATED RESPONSE:
Partially Implemented. DoIT is increasing messaging to managers to remedy these employee delays.

24. The auditors recommend DoIT develop a comprehensive and accurate description which outlines its internal controls for its IT environment.

FINDING: *(Lack of a Comprehensive and Accurate Description of IT Internal Controls) – First reported 2018, last 2020*
DoIT Description of the IT General Controls and Application Controls (Description) was not comprehensive or accurate.

During their examination of DoIT's FY22 Description, auditors noted it contained inaccurate statements. Specifically,

Control stated in the description of system	Actual control in place
DoIT conducts risk assessments for customer agencies.	DoIT was to conduct risk assessments for all agencies, boards, and commissions under the Governor.
DoIT's Division of Information Security is responsible for ensuring Department's compliance with enterprise information security policies.	DoIT did not ensure compliance with all of the enterprise information security policies.
In the event of an emergency, only verbal approval by the appropriate management personnel is required to begin remediation.	The emergency Change Advisory Board (eCAB) approval is required in order for remediation actions to begin.

In addition, DoIT's Description omitted controls related to the recovery activities associated with the midrange environment.

This finding was first reported in the FY18 Compliance Examination Report. DoIT has failed to implement corrective actions to remedy the weaknesses.

The State of Illinois, DoIT's Risk Management Program states the Department is to conduct risk assessments on all agencies, boards, and commissions under the Governor. In addition, the September 16, 2016, Directive from the Governor's Office states DoIT is to conduct an assessment at every agency, board, and commission that reports to the Governor.

DoIT indicated the weaknesses were due to oversight.

Without an accurate description of its IT internal controls, DoIT and user agencies may have unidentified deficiencies and may be unable to rely on the internal controls over the services provided.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation.

UPDATED RESPONSE:
Partially Implemented. DoIT will provide an accurate description of controls in its annual System and Organization Control (SOC) report.

25. The auditors recommend DoIT complete Business Impact Assessments for all transferring agencies and develop and approve disaster recovery plans, business continuity plans and infrastructure plans. Additionally, they recommend DoIT conduct comprehensive testing and document remediation efforts for all issues identified during testing.

FINDING: *(Inadequate Disaster Contingency Planning) – First reported 2018, last 2020*

DoIT did not have adequate disaster recovery plans and had not conducted comprehensive disaster recovery testing.

DoIT provides Information Technology services to over 100 agencies. As a result, DoIT, along with the agencies, have a responsibility for the recovery of the environment and applications. During the examination period, they noted:

- Business Impact Assessments had not been completed for 2 of 35 (6%) transferring agencies.
- Disaster recovery plans had not been developed or were draft for enterprise applications recovery plans, business continuity plans, and infrastructure plans.
- DoIT was unable to provide the Test, Training & Exercise Plans (TT&Es) conducted.

In addition, DoIT was unable to recover all midrange critical applications in the event of a disaster. Further, the mainframe recovery test conducted in April 2022 had to be aborted due to varying issues. DoIT was only able to recover 34 of 146 (23%) identified critical applications.

This finding was first reported in the FY18 Compliance Examination Report. DoIT has failed to implement corrective actions to remedy the weaknesses.

DoIT indicated the lack of resources resulted in the noted weaknesses.

Failure to have disaster recovery plans and conduct testing could result in DoIT and agencies inability to process critical transactions for an extended period of time in the event of a disaster.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation.

UPDATED RESPONSE:
Partially Implemented. DoIT has completed Business Impact Assessments for all transferring agencies and is implementing an integrated risk management tool to track disaster recovery plans and information system contingency plans.

26. The auditors recommend DoIT enter into detailed Agreements with the user agencies documenting each parties' roles and responsibilities. In addition, they recommend DoIT timely execute the Agreements.

FINDING: *(Lack of Agreements to Ensure Compliance with IT Security Requirements) – First reported 2018, last 2020*

DoIT had not entered into detailed agreements with user agencies to ensure prescribed requirements and available security mechanisms were in place in order to protect the security, processing integrity, availability, and confidentiality of user agencies systems and data.

During the examination period, DoIT had not entered into agreements with 13 user agencies. In addition, DoIT executed 35 agreements after the effective date of the agreement.

This finding was first reported in the FY18 Compliance Examination Report. The Department has failed to implement corrective actions to remedy the weaknesses.

DoIT management stated the weaknesses were due to the length of time it takes for each agency to obtain agreement as to the details of the IGAs.

Without detailed agreements, DoIT may not have an understanding of each parties' roles and responsibilities, along with the prescribed requirements and available security mechanisms user agencies require in order to ensure the security, processing integrity, availability, and confidentiality of systems and data.

DEPARTMENT RESPONSE:
DoIT accepts the finding and recommendation.

UPDATED RESPONSE:
Partially Implemented. DoIT added a more detailed description of user agency security roles and responsibilities in the FY23-FY25 IGA with transferring agencies. See comment to 2022-001 regarding the timing on the execution of these agreements.

Headquarters Designations

The State Finance Act requires all state agencies to make semiannual headquarters reports to the Legislative Audit Commission. Each state agency is required to file reports

of all its officers and employees for whom official headquarters have been designated at any location other than that at which official duties require them to spend the largest part of their working time.

As of July 2022, the DoIT had 0 employees assigned to locations others than official headquarters.