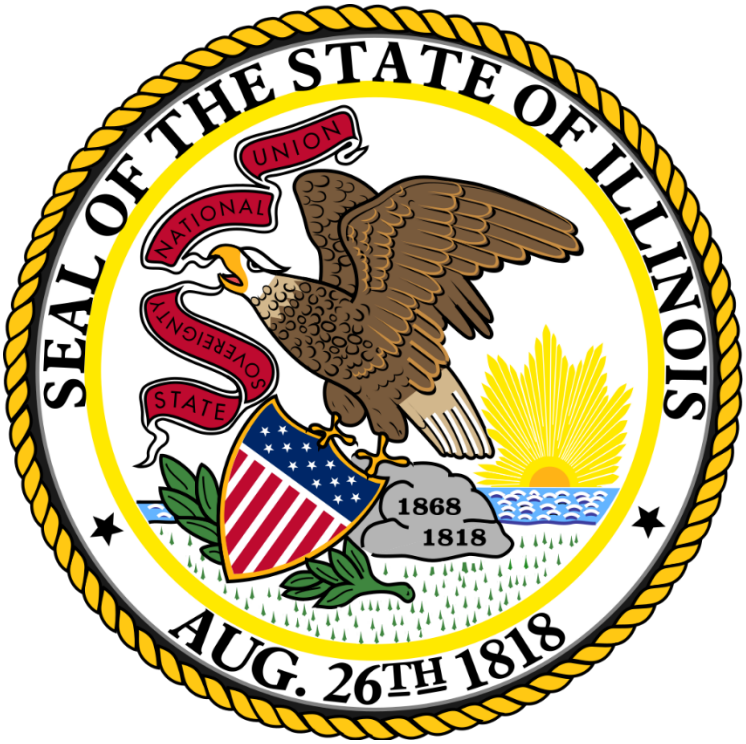
LEGISLATIVE AUDIT COMMISSION



Review of
Department of State Police
Two Years Ended June 30, 2020

622 Stratton Office Building
Springfield, Illinois 62706
217/782-7097

REVIEW: 4516
DEPARTMENT OF STATE POLICE
TWO YEARS ENDED JUNE 30, 2020

FINDINGS/RECOMMENDATIONS – 32

IMPLEMENTED – 6
PARTIALLY IMPLEMENTED – 26

REPEATED RECOMMENDATIONS – 11

PRIOR AUDIT FINDINGS/RECOMMENDATIONS – 14

This review summarizes the auditors' report of the Department of State Police (ISP) for the two years ended June 30, 2020, filed with the Legislative Audit Commission May 4, 2021. The auditors conducted a compliance examination in accordance with State law and *Government Auditing Standards*.

ISP was established on January 1, 1970. ISP's responsibility is to maintain order as mandated by statute, while safeguarding the rights and privileges of all citizens of the state.

ISP had been divided into four divisions: Operations, Forensic Services, Administration and Internal Investigation all under the direction of the Director of the Department. ISP was re-organized in 2019 and now consists of 7 divisions:

- Patrol;
- Criminal Investigation;
- Forensic Services;
- Justice Services;
- Internal Investigation;
- Academy and Training; and
- the Office of the Statewide 9-1-1 Administrator.

The reporting metrics for the Public Accountability Report (PAR) mirror the Department structure prior to the re-organization in 2019.

1. The Division of Operations (now the Divisions of Patrol and Criminal Investigation) provides police service to the residents and visitors of Illinois and is dedicated to improving highway safety and solving and preventing crime.
2. The Division of Forensic Services mission is to deliver accurate and timely forensic services in the collection and analysis of physical evidence from crimes and assist with the identification and prosecution of offenders and the exoneration of the innocent.
3. The mission of the Division of Administration (now the Division of Justice Services) is providing administrative and technical support to the employees of the Illinois

State Police and statewide law enforcement, in addition to delivering reliable, accurate, and credible information to empower effective public safety decision-making.

4. The mission of the Division of Internal Investigation is through education and swift and impartial investigations of all allegations, to reduce the incidence of misconduct within ISP and within the executive branch, maintaining a high level of trust in ISP and in public office.

During the examination period, Mr. Leo Schmitz was Department Director from July 1, 2018 to January 20, 2019. Brendan F. Kelly was appointed Acting Director from January 21, 2019 to October 29, 2019. The Illinois Senate unanimously confirmed Director Kelly's appointment on October 30, 2019 and he continues to serve in that capacity. Mr. Kelly graduated from the University of Notre Dame and the Saint Louis University School of Law. Mr. Kelly served as a prosecutor and an elected State's Attorney for eight years prior to his appointment to the Director of ISP.

The following presents the average number of full-time employees by function at June 30:

	FY18	FY19	FY20
Operations	1,437	1,582	1,476
Internal Investigations	56	64	69
Forensics	359	357	362
Administration	96	106	124
Academy	110	65	71
Statewide 911	-	-	138
Special Funds	368	316	342
Total Full-Time Equivalent Employees	**2,426**	**2,490**	**2,582**

According to the Analysis of Overtime provided to the LAC on September 30, 2021, ISP paid $6.3 million for 120,444 hours of overtime and compensatory time in FY20 and paid $6.7 million for 133,607 hours of overtime and compensatory time in FY19.

The following presents a comparison of activities and performance by division for the fiscal years noted:

Division of Operations (Patrol and Criminal Investigation)	**FY18**	**FY19**	**FY20**
Number of Impaired Driving/Zero Tolerance Citations	4,801	5,040	4,230
Number of Speeding Citations	106,087	104,517	36,486
Number of Motor Carrier Inspections	88,482	91,103	60,962
Number of Criminal Investigative Cases Opened	1,428	1,275	650
Number of Criminal Investigative Cases Closed	580	423	201
Number of Fatal Crashes	951	914	956

Percentage of Criminal Cases Resulting in Arrests	31%	33%	31%

The significant reduction in the enforcement statistics of these services was due to COVID-19 restrictions. In addition, the Department undertook additional "community caretaking" activities in order to ensure compliance with the Executive Orders issued by the Governor to mitigate the spread of COVID-19.

(Source: Analysis of Operations in the Compliance Examination on pages 84 and 85 of the audit report)

Division of Administration (Now Justice Services)	**FY18**	**FY19**	**FY20**
Number of Inquiry Transactions Processed (LEADS)	96,276,476	95,440,682	90,435,040
Number of Court Orders to Expunge or Seal Records	N/A	16,625	19,766

(Source: Analysis of Operations in the Compliance Examination on page 86 of the audit report)

Division of Forensic Services	**FY18**	**FY19**	**FY20**
Number of DNA Cases Worked	6,394	10,801	15,888
Number of Forensic Cases Worked in All Disciplines	66,126	63,074	64,543
Number of Crime Scenes Processed	3,849	3,597	3,365
Number of Firearm Owner's Identification (FOID) Applications Processed	228,448	313,483	279,878
Number of Identification Inquiries (Name-based and Fingerprint-based Checks)	1,104,809	1,178,886	984,675
DNA Case Backlog	3,745	8,776	6,093
Case Backlog of All Forensic Cases	12,916	23,109	14,671
Number of Property Crime Scenes Processed	1,488	1,271	884
Number of DNA Profiles Uploaded to the Combined DNA Indexing System (CODIS)	26,445	21,110	16,217
Number of Revoked FOID Cards	10,871	10,703	10,278
Percentage of DNA Cases Worked in 30 Days	8%	21%	29%
Percentage of Forensic Cases Worked in 30 Days	50%	41%	32%
Percentage of Crimes Against Persons Responded to Within One Hour	91%	92%	82%

(Source: Analysis of Operations in the Compliance Examination on page 85 of the audit report)

Division of Internal Investigation	FY18	FY19	FY20
Number of Division of Internal Investigation Cases Opened	228	198	670
Number of Employment Background Checks (ISP and Other Criminal Justice Agencies)	903	888	1,282
Number of Criminal History Analyses Conducted at Nursing Homes	3,197	3,148	2,662
Percentage of ISP Personnel Complaints Cleared	11%	8%	20%
Percentage of Complaints Against Officers that are Sustained	85%	56%	80%

(Source: Analysis of Operations in the Compliance Examination on page 86 of the audit report)

Adverse Opinion Expressed by Auditors

Due to the significance and pervasiveness of the findings described within the [Compliance Examination] report, [the auditors] expressed an **Adverse Opinion** on the Illinois State Police's compliance with the specified assertions which comprise a State compliance examination. The Codification of Statements on Standards for Attestation Engagements (AT-C § 205.72) states a practitioner "should express an adverse opinion when the practitioner, having obtained sufficient appropriate evidence, concludes that misstatements, individually or in the aggregate, are both material and pervasive to the subject matter."

In particular, findings 1-12 are each considered to represent material deviations with specified audit requirements.

(Source: Introduction in the Summary Report Digest of the Compliance Examination on page 1)

Changes in Independence Requirement

Due to changes in independence requirements effective June 30, 2020, the Office of the Auditor General (OAG) now requires auditees, without auditor assistance, to prepare the report components comprising the Supplementary Information for State Compliance Purposes, **usually** found within the OAG's compliance reports. To help facilitate this

change, the OAG published guidance on its website for auditees to follow in preparing these report components. While the auditors do not express an opinion, a conclusion, or provide any assurance on these report components, they read them to identify potential errors. If errors are identified, auditors present them to the agency for correction or to demonstrate why the disclosure was complete and accurate.

Though ISP submitted the required Supplementary Information, auditors noted discrepancies between ISP records and the records of the Illinois Office of the Comptroller (IOC) and did not provide all the necessary explanations for significant variations in their financial data. As the result of the unresolved doubts and noted omissions concerning report components, the report components were omitted from the ISP Compliance Exam. See finding no. 12 for more detail.

LAC staff requested the Supplementary Information for State Compliance Purposes that was not published with the audit report. That information was received from ISP on September 30, 2021. LAC staff does not express an opinion, a conclusion or provide any assurance on these report components; however, a brief analysis is provided based on the report components provided by ISP. This information is provided in a supplementary packet with this review for the purposes of analysis and to supplement the findings laid out in the audit report.

Expenditures From Appropriations

Data for this section is based on the Schedule of Appropriations, Expenditures and Lapsed Balances by Fund for FY19 and FY20 that was submitted to LAC staff on September 30, 2021. Total expenditure data for these schedules matched the IOC records; however, LAC staff does not express an opinion, a conclusion or provide any assurance on these report components

ISP was appropriated $663.4 million in FY19 and $690.9 million in FY20, an increase of $27.58 million, or 4.1%. ISP expended $555.3 million and $571.5 million appropriated funds in FY19 and FY20, respectfully. Expenditures increased $16.2 million from FY19 to FY20, representing an increase of approximately 3%. ISP lapsed $108.2 million in FY19 and $119.5 million in FY20. The top five funds with the largest lapsed balances in FY20 were the following: Statewide 9-1-1 Fund ($20.6 million), State Police Services Fund ($13.4 million), State Police Operations Assistant Fund ($12.3 million), State Police Whistleblower Reward and Protection Fund ($11.1 million) and State Police Law Enforcement Administration Fund ($10 million). The following funds had no expenditures in FY20: the Medicaid Fraud and Abuse Prevention Fund, the Sex Offender Investigation Fund, the State Police Law Enforcement Administration Fund and the Firearm Dealer License Certification Fund.

According to ISP, significant variations in expenditures in FY20 compared to FY19 were as follows:

- $4 million increase in the State Crime Laboratory Fund due to increased lab equipment and supplies.
- $3.1 million increase in the State Police Firearm Services Fund to increase staffing levels to process increased FOID Card applications.
- $2.4 million increase in the State Police Vehicle Fund for increased number of vehicles purchased to replace high mileage, unsafe vehicles.
- $500,000 decrease in the State Asset Forfeiture Fund due to the fund's cash balance being low in FY20. Expenditures are limited to available cash for this fund.
- $1.3 million increase in the State Police Whistleblower Fund resulting from unexpected COVID-19 necessary supplies and PPE.

Cash Receipts

Based on reviews of previous audit reports, it appears that the schedules of receipts submitted to LAC staff on September 30, 2021 were incomplete compared to previous reports; however, LAC staff does not express an opinion, a conclusion or provide any assurance on these report components. Analysis is provided based on the information submitted to the LAC by ISP.

According to the Comparative Schedule of Receipts, Disbursements and Fund Balances, the Statewide 9-1-1 Fund, receipts decreased $11.1 million, or 5.5%, from $203.9 million in FY19 to $192.8 million in FY20. However, total disbursements increased $8.6 million, or 4.6%, from $186.2 million in FY19 to $194.8 million in FY20. Total cash balances were $40.3 million and $38.3 million in FY19 and FY20, respectively. Notably, these balances are only representative of July 1 through June 30 for the respective fiscal years, and omit $32.3 million and $32.7 million expended during the lapse period for FY19 and FY20, respectively.

For the Wireless Carrier Reimbursement Fund, total receipts decreased approximately $1 million, or 36.7%, from $2.6 million in FY19 to $1.7 million in FY20. Disbursements increased slightly by $73 thousand, or $2.8%, from $2.653 million in FY19 to $2.727 million in FY20. Resultantly, the total cash balance decreased approximately $1 million, or 58%, from $1.8 million in FY19 to $0.8 million in FY20. Notably, these balances are only representative of July 1 through June 30 for the respective fiscal years, and omit $0.8 million and $0.2 million expended during the lapse period for FY19 and FY20, respectively.

During FY16, the Statewide 9-1-1 Fund and the Wireless Carrier Reimbursements Fund were transferred from the Illinois Commerce Commission to the Department of State Police effective January 1, 2016. According to the Department of State Police & Illinois Commerce Commission Comparative Schedule of Cash Receipts for Fiscal Years Ended June 30, 2017, 2018 and the Six Months Ended June 30, 2016, the Statewide 9-1-1 Fund and the Wireless Carrier Reimbursements Fund had a irreconcilable difference of $5.3 million at the end of FY18. The significance of the irreconcilable differences is noted in

finding no. 1 in the Department's Compliance Exam for the Two Years Ended June 30, 2018.

An analysis of significant variations in receipts cannot be provided due to lack of complete information related to the schedules of receipts for the two years ended June 30, 2020.

Changes in Property

Due to the process and control deficiencies identified in finding no. 1, auditors were unable to conclude whether ISP's population records were sufficiently precise and detailed under the Attestation Standards promulgated by the American Institute of Certified Public Accountants (AT-C § 205.35) in order to test the ISP's controls over state property and equipment.

Status of Previously Conducted Program/Management Audits

Division of Forensic Services

The Management and Program Audit of the State Police's Division of Forensic Services was released in March 2009 and contained 16 recommendations. As of June 30, 2018, fourteen of the audit's recommendations were implemented and two were partially implemented. The partially implemented recommendations were as follows:

#1 Develop a comprehensive plan to address the environmental issues at the forensic labs.

#3 Fully utilize the funds appropriated by the General Assembly for the Division of Forensic Services, including the reduction of backlogs, rather than allowing the funds to be transferred or to lapse.

Firearm Owner's Identification Card Act

The Management Audit of the State Police's Administration of the Firearm Owner's Identification Card Act was released in April 2012 and contained 12 recommendations. As of June 30, 2018, 11 of the audit's recommendations were implemented and one was partially implemented. The partially implemented recommendation was as follows:

#6 Work with vendor to ensure the FOID cards are forwarded to the correct mailing address and ensure enough customer service representatives are available to answer applicants' questions about the FOID card.

State Asset Forfeiture Fund (514)

The Accountant's Report on State Compliance and on Internal Control Over Compliance for the State Asset Forfeiture Funds contains an adverse opinion on compliance and identifies material weaknesses over internal control over compliance.

There were four findings that were all considered material weaknesses and material noncompliance. The findings were:

1. Inadequate Controls Over Receipts and Reconciliations (Recommendation Partially Implemented)

2. Failure to Comply with the Seizure and Forfeiture Reporting Act (Recommendation Accepted and In Progress)

3. Noncompliance with the Seizure and Forfeiture Reporting Act (Recommendation Partially Implemented)

4. Failure to Demonstrate the Completeness and Accuracy of the Report Components for the Compliance Exam Report (Recommendation Accepted and In Progress)

Statewide 9-1-1 Fund (612) and Wireless Carrier Reimbursement Fund (613)

Effective January 1, 2016, the Wireless Emergency Telephone Safety Act (Act) (50 ILCS 751 et seq.) was repealed and the Emergency Telephone Safety Act (50 ILCS 750 et seq) was enacted to create the Office of the Statewide 9-1-1 Administrator (Office) with the Illinois State Police. The Office is responsible for developing, implementing and overseeing a uniform statewide 9-1-1 system for all areas outside of municipalities having a population over 500,000.

The Illinois Commerce Commission was responsible for administering the Wireless Service Emergency and the Act (50 ILCS 751/1 et seq.) through December 31, 2015. The purpose of the Act was "to promote the use of wireless 9-1-1 and wireless enhanced 9-1-1 (E9-1-1) service in order to save lives and protect the property of the citizens of the State of Illinois."

Effective January 1, 2016, ISP became responsible for functions related to the Statewide 9-1-1 Fund (Fund 612) that was previously named the Wireless Service Emergency Fund and the Commerce Commission remains responsible for payments from the Wireless Carrier Reimbursement Fund (Fund 613).

The Accountant's Report on State Compliance, on Internal Control Over Compliance, and on Supplementary Information for State Compliance Purposes for the responsibilities of the Illinois State Police within the Statewide 9-1-1 Fund and the Wireless Carrier

Reimbursement Fund contains a modified opinion on compliance and identifies material weaknesses over internal control over compliance.

There were two findings that were considered material weaknesses and material noncompliance. The findings were:

1. Inadequate Controls Over Receipts and Reconciliations (Recommendation Partially Implemented)

2. Failure to Demonstrate the Completeness and Accuracy of the Report Components (Recommendation Accepted and In Progress)

Accountants' Findings and Recommendations

Condensed below are the 32 findings and recommendations presented in the audit report. There were 11 repeated recommendations. The following recommendations are classified on the basis of updated information provided by Tasso Maton, Chief Financial Officer, Illinois State Police, received via electronic mail on July 9, 2021.

1. The auditors recommend ISP develop procedures to immediately assess if an electronic device may have contained confidential information whenever it is reported lost, stolen, or missing during the annual physical inventory, and document the results of the assessment. The auditors also recommend ISP ensure all equipment is accurately and timely recorded or removed from the property records and ensure accurate reports are submitted to the Comptroller. Additionally, the auditors recommend ISP update its property control manual and strengthen its controls over the recording and reporting of its State property and equipment by reviewing their inventory and recordkeeping practices to ensure compliance with statutory and regulatory requirements.

Furthermore, recommend the Department reconcile its property records to the Comptroller's records and proper reviews are completed.

FINDING: *(Inadequate Control Over Property and Equipment)*

Due to the following process and control deficiencies identified below, the auditors were unable to conclude whether ISP's population records were sufficiently precise and detailed under the Attestation Standards promulgated by the American Institute of Certified Public Accountants (AT-C § 205.35) in order to test the controls over state property and equipment.

Even given the population limitations noted above which hindered the ability of the accountants to conclude whether selected samples were representative of the population as a whole, performed the following tests:

- During review of ISP's discrepancy listings, ISP did not have adequate controls over lost or missing property. 55 of 60 (92%) items listed as lost or missing could possibly have confidential information stored on them. Items included servers, computers, laptops, tablets, and a camera with a memory card.

ISP management indicated they do not have the tools or resources to protect and keep track of all the data placed on equipment.

- When attempting to reconcile the equipment purchase records to the Office of the Comptroller's (Comptroller) record of equipment expenditures, the auditors noted ISP was unable to reconcile the differences noted between the Object Expense/Expenditures by Quarter Report (SA02) and the Agency's Report of State Property (C-15) reports. **During the engagement period, ISP had $81,877,026 in gross equipment and electronic data processing expenditures. However, only $52,300,997 in gross equipment and electronic data processing expenditures were reported.**

ISP management indicated monthly reconciliations of inventory entries to equipment expenditures were not performed due to a lack of resources.

- When attempting to reconcile the ISP's FY20 schedules of additions, deletions, and transfers to the FY20 property control listing, **auditors noted $2,335,955 of unknown activity** which was not reported on ISP's FY20 schedules of additions, deletions, and transfers. ISP was unable to identify the unknown activity.

ISP management indicted the weakness was due to lack of training for new staff and trying to correct the property records the best they could with the limited amount of resources available at the time.

- When testing for accuracy of the C-15 reports filed with the Comptroller, the auditors noted:

    - ISP's property records at June 30, 2020 and 2019 did not agree to the C-15 reports submitted to the Comptroller by approximately $12,466,712 and $692,707, respectively. Management attempted a reconciliation for June 30, 2020 and identified $692,707 of property that should have been recorded to the property records. ISP did not attempt to prepare a reconciliation between the ISP records and the C-15 reports at June 30, 2019.

    - ISP's FY20 and FY19 records of additions, deletions, and transfers did not agree to the C-15 reports submitted to the Comptroller by $628,528 and $17,155,753, respectively. ISP did not attempt to prepare a reconciliation

between the FY19 and FY20 records of additions, deletions, and transfers and the C-15 reports.

- ISP FY20 and FY19 lease activity for both fiscal years was recorded as a $494,854 deletion on the third quarter FY20 C-15 report. As a result, the ending capital lease value reported on the third quarter FY20 C-15 represented the known capital lease value of $108,772, at the time.

ISP management indicated the lack of training for new staff and trying to correct the property records the best they could with the limited amount of resources available at the time resulted in the weaknesses.

- During testing of ISP records for timely acquisition, change, or deletion of equipment items, noted:
  - 37 of 60 (62%) equipment items, totaling $1,671,773, were added to ISP inventory records between 1 and 4,951 days late.
  - 38 of 60 (63%) equipment items, totaling $1,491,310, were deleted from the ISP inventory records between 35 and 1,503 days after the disposal date of the property.

ISP management indicated they were trying to correct the records and recording all activity which was previously unrecorded due to the lack of resources.

- During testing of ISP records for proper recording of transfers and deletions, noted:
  - 4 of 60 (7%) items, totaling $14,746, did not have the correct acquisition cost and did not have the correct purchase date reported on the Surplus Property Delivery form.
  - 3 of 60 (5%) items, totaling $140,616, had the incorrect acquisition cost listed on the Surplus Property Delivery form.
  - 2 of 60 (3%) items, totaling $2,062, were incorrectly removed. The items removed from property were a computer and a radar, but should have been a chair and a preselector totaling $454.

.

ISP management indicated they do not have an efficient process in place to complete and review the equipment deletions and transfers due to the lack of resources.

- During testing of the Annual Certification of Inventory, noted:
  - The FY20 and FY19 Annual Certification of Inventory could be inaccurate based upon failure to perform reconciliations of ISP's property records. The FY20 Annual Certification of Inventory reported 661 missing items totaling

$2,243,766 or 0.72% of the total inventoried items. The FY19 Annual Certification of Inventory reported 626 missing items totaling $1,198,804 or 0.71% of the total inventoried items.

- 7 of 60 (12%) equipment items, totaling $23,344, were reported on both FY20 and FY19 Annual Certification of Inventory as being unable to be located. The seven items were not removed from the June 30, 2020 property records.

ISP management indicated the inaccuracies in the Annual Certifications of Inventory were caused by reconciliations not being performed and not removing items from property records, which were both due to a lack of resources.

- During testing of the equipment leases, noted:
  - 19 of 29 (66%) leases tested were not located on the ISP property listing. ISP did not record FY19 and FY20 capital equipment leases to the ISP property control records. In addition, ISP did not maintain a detailed listing of leased equipment.
  - 18 of 29 (62%) leases tested did not report the correct Fair Value at Inception on the Accounting for Leases-Lessee (SCO-560) form.
  - 4 of 29 (14%) leases tested did not report the leased equipment's total economic life and the remaining life at lease start date on the SCO-560 form.
  - 18 of 29 (62%) leases tested included maintenance cost in the rent per period input on the SCO-560 form.
  - 1 of 29 (3%) leases tested incorrectly reported a bargain purchase amount of $36,450. The lease did not offer a bargain purchase amount.
  - 1 of 29 (3%) leases tested had a Fair Value at Inception reported on the SCO-560, but ISP failed to maintain documentation on how the fair value was determined.
- During testing of ISP's equipment additions, noted:
  - 2 of 2 (100%) Capital Development Board (CDB) transfer additions, totaling $583,935, were not recorded on the Department's property records.
  - 3 of 60 (5%) items, totaling $21,110, did not accurately include shipping cost on the property records. The equipment additions had a total of $230 in shipping cost which was not recorded on the property records.
  - 1 of 60 (2%) items, totaling $36,393, was recorded on the property records at the incorrect value. The item was overstated by $1,872.

ISP management indicated the CDB transfers were not recorded to the Department's property records due to lack of training.

- During review of ISP manuals, the auditors noted the property control manual was last updated on September 1, 2000 and did not reflect the current processes.

- During review of ISP policies and directives, the auditors noted ISP did not have a written policy clearly delineating the categories of equipment considered subject to theft.

ISP management indicated the manuals, policies, and directives had not been updated due to a lack of resources available to complete the task.

This finding was first noted during the examination of the two years ended June 30, 2002. In the subsequent years, ISP has been unsuccessful in implementing a corrective action plan.

RESPONSE:
ISP concurs and realizes that ultimately the responsibility of control over property and equipment is on itself. The PSSSC (Public Safety Shared Service Center) was responsible for property control between 2008 and mid-2019. While inventory was with the PSSSC, the unit was understaffed.

This was part of the reason that, in 2019, property control and several other functions were returned to the ISP. Property control is now housed in the Office of Finance. Beginning April 1, 2019, two new employees were hired to staff this unit. A retired employee formerly providing sole staffing of property control was hired to train Department staff, however this employee only spent a small fraction of the anticipated time working. The transfer back to the Department brought to light the fact that there was a substantial backlog in inventory records being processed (upwards of a 1-year backlog in some cases). This not only included adding new property that had been purchased, but the lack of ability to surplus items that were obsolete.

It was assumed early in this transition that the inventory records could be incorrect. However, it was not until the transition to the ERP system January 1, 2020, that these assumptions were proven. Efforts to clean data prior to the migration were made and enormous efforts to catch up on the backlogs were made. Many low value assets (not required to be inventoried) were also removed in mass quantities. Further, many information technology related assets had never been transferred to their respective owners. This too was cleaned up in mass corrections.

In April of 2020, when preparing to complete the quarterly C-15 reports in a new system, we learned that insufficient reconciliation activities had been conducted since the activity was first moved to PSSSC. Starting, ending, and quarter activity reports were not reconciled back to the previous report or to the legacy inventory system. Therefore, major adjustments needed to be made to the initial C-15 report from the new system. We have

since evaluated the previous errors and have identified ways of rectifying them and keeping them from happening again.

Lack of training, at the time of bringing back property control to the Department, also exacerbated other issues such as but not limited to entering assets costs correctly.

At around the same time as Property Control was brought back from Shared Services, contracts and obligations were also brought back. This function resides in the Procurement Unit. Training for this function completely omitted the concept of leases and their importance to the Property Control Unit. The reporting of leases to the IOC through the SCO560 forms were not only not done timely or accurately, they also were not shared with the Property Control Unit for them to include in the C-15 reports.

The transition to the ERP system created an opportunity to create a new process whereby assets would be entered way earlier in the process, therefore eliminating any timeliness issues. Assets purchased by ISP are now entered in prior to the invoice being paid. This is a major change from the way it had been done in the past. This allows us to have checks and balances when the invoice is paid to only approve if it has been reported to Property Control and been added to inventory.

The process of being able to remove an asset if it has not been located for two years was not a process that the PSSSC adhered to. It was only when we moved to ERP that this was made known to us. Now that we have substantially cleaned up the data and have a good way to adhere to this process, we have started to apply it.

We agree that at the time of audit, ISP did not have the manual updated, but prior to the draft findings being delivered these were completed and posted to the ISP intranet.

ISP will continue to evaluate processes and the accuracy of data so that these infractions will not be prevalent again.

UPDATED RESPONSE:

Partially Implemented. ISP concurs with the recommendation. For electronic assets reported lost, stolen, or missing, a field report or memorandum should be completed that identifies any of the aforementioned assets. This report should have an explanation of what the asset was used for and what type of data was stored on it. This process should be completed as soon as it has been identified as lost, stolen or missing. This would not have to wait until annual inventory. It is assumed, the majority of the documents reported in the past had to do with the old inventory system and most of those had in fact not been lost but surplussed. ISP anticipates the number of such occurrences to be drastically lower now. In addition, the Department of Innovation and Technology (responsible for all electronic devices) uses technology from Microsoft called BitLocker. It is used specifically for securing hard drives. All Windows 10 PCs have this technology enabled in the ISP environment. Windows 7 PCs should be fully retired by August 2021 which means all ISP PCs will have BitLocker technology enabled. If a hard drive is removed from the PC,

it cannot be read in a different PC. A custom security key would have to be entered in order to read the hard drive. These keys are kept securely by ISP DOIT staff.

While this does not prevent items from being lost, stolen or missing it does eliminate the possibility of confidential information being seen or removed by a non-ISP employee. When ISP went live with the property control (PC) module in SAP, we implemented a process where at the time of receipt of asset, the custodian requests tags. When they request tags, they have to provide the serial number of the asset. This then gets uploaded into the system. As a further measure we have a process where an invoice to pay for an asset will not be approved until there is sufficient proof that PC has been involved and that a tag has been provided. This process is in place and requires no further steps. Transfers are done by the custodians (or delegate) within SAP. The receiving location approves the receipt of the asset within 30 days or the central PC group will approve it on their behalf. This process is in place and requires no further steps. The Comptroller reports have now been submitted on time now that we have new C-15 procedures locked down. This is implemented and requires no further steps. The new process for electronic devices will help ensure the timely entry/change of these types of assets. When a new batch of computers comes in and the custodian is ready to request a tag, the words "never assigned" will be entered in the 'type name' field in the SAP upload document and sent to PC. Central PC will then assign a tag and upload it into SAP and send the custodian the tags. This will ensure we know these assets are awaiting installation. As installations/assignments take place, another upload document will be created. This will be done on a weekly basis by the DoIT custodian. The new file will include the name of the person who was given the asset along with their respective location code. This will be sent to PC via email with 'inter-agency transfer and assignment' as the subject. PC will upload to reflect the change in the location code and user. This will eliminate the receiving location code custodian from having to 'receive' in SAP and will allow for a more timely documentation of changes. As electronics are turned back in (no longer needed by user for one reason or another) then a separate upload document will be sent in to show the asset. Similar to the new assets above, there will be a change to the 'type name' field to some predefined terminology that will indicate it is back in the warehouse and that the electronic asset complied with SRV-225. This procedure is for certification of hard drive destruction. (This SRV-225 was implemented in 2/2021).

ISP went live with the new SAP ERP system in January 2020. This drastically changed the processes central property control (PC) follows. We acknowledge that going into the 'go-live' phase of ERP our procedures were extremely out of date. However as of February 2021 we have completely rewritten the PC manual to reflect these changes. ISP has committed to keeping a running log of any process modifications that occur. As either new processes are developed or changes to existing ones occur, they will be logged and evaluated monthly. If changes are necessary to the manual, they will be made and posted to the ISP intranet. This process is considered implemented and no further steps are necessary.

Prior to the ERP system, the starting, ending and activity amounts for the C-15 reports were not reconciled to each other. Beginning with quarter ending 3/31/2020, ISP began

using the reports from the ERP system. This first reconciliation had adjustments applied to bring the aforementioned amounts in synchronization. The next quarter had another substantial reconciling adjustment that allowed subsequent reconciliations to balance. At this point the quarterly C-15 reports are in sync and it is anticipated they will continue to be. This finding is considered implemented as of 7/1/2020 and no further steps are necessary.

2. The auditors recommend ISP maintain accurate and detailed records of all billings and the corresponding collections to facilitate proper reporting of accounts receivable activity and also recommends ISP strengthen procedures and allocate necessary resources to properly post accounts receivables and associated payments. Lastly, the auditors recommend ISP file reports timely in accordance with SAMS.

FINDING: *(Inadequate Controls Over Accounts Receivable)*

ISP did not properly maintain accounts receivable records and failed to accurately report accounts receivable on the Quarterly Summary of Accounts Receivable Reports (reports) to the Office of the State Comptroller (Comptroller).

During testing of accounts receivable records, noted:

- ISP was unable to provide detailed individual accounts receivable records for GRF, Road Fund (11), State Garage Revolving Fund (303), Illinois State Toll Highway Authority Fund (455), Over Dimensional Load Police Escort Fund (652), Drug Traffic Prevention Fund (878), and State Police Services Fund (906).

- During the analytical review of ISP accounts receivable activity, billings and collections were largely identical. ISP stated they were recording accounts receivable at the time of receipt of payments instead of when the claim for future cash was reasonably estimable and measurable.

- ISP was unable to provide policies or procedures for handling and reporting its accounts receivable, tracking and monitoring complaints received, posting delinquent accounts receivable into the Comptroller's Illinois Debt Recovery Offset System or pursuing other debt collection procedures, and writing off uncollectible receivables.

- 13 of 64 (20%) fund Report filings tested were filed between 57 to 149 days late.

As a result of the noted weaknesses, auditors were unable to conduct detailed testing of the Department's accounts receivable.

This finding was first noted during the examination of the two years ended June 30, 2010. In the subsequent years, ISP has been unsuccessful in implementing a corrective action plan.

ISP management indicated the incomplete records were due to payments not being entered into their system since 2008, when a staff position became vacant and was no longer funded. Additionally, ISP management indicated the late reports were due to transition in personnel during the examination period.

Failure to maintain accurate and detailed accounts receivable records and timely report accounts receivable balances could lead to the failure to properly collect amounts owed to the State and inaccuracies in statewide financial statement reporting.

RESPONSE:
ISP concurs the quarterly accounts receivable forms (C-97) should be filed timely with the Comptroller. ISP previously filed C-97s on several funds that are not ISP funds, Road Fund (11), Illinois State Toll Highway Authority Fund (455) and Garage Revolving Fund (303). These accounts have been cleaned up and are no longer on the list of C-97s the Department files. Additionally, accounts receivable balances for General Revenue Fund (0001) have been written off and are no longer on the list of C-97s filed by the Department. While Over Dimensional Load Police Escort Fund (0652) and State Police Services Fund (0906) are still being prepared and filed manually, if we can maintain staffing levels our goal is to use ERP to file these quarterly accounts receivable reports starting July 1, 2021. While we do not have staff levels to have a collections unit, State Police Services Fund (0906) staff has been working with the Comptroller's Illinois Debt Recovery Offset System (IDROP). Our goal is to continue to work with the accounts receivable procedures and processes to become compliant in this area.

UPDATED RESPONSE:
Partially Implemented. ISP concurs with the recommendation. The Office of Finance (OOF) is working with an outside audit firm to determine is any funds have receivables that are not being captured. If accounts are identified a process will documented for accurate records. Additionally, OOF and the division are working on the cleanup of Fund 652 receivables in preparation of utilizing SAP to maintain accurate and detailed records of all billings and collections. With additional staff, the division will post accounts receivables timely for Fund 612.

3. The auditors recommend ISP establish proper segregation of duties over the receipts process, establish procedures to properly reconcile receipts, and maintain accurate documentation to support receipt activities and related reviews performed.

FINDING: *(Inadequate Controls Over Receipts)*

REVIEW: 4516 (Compliance) and 4517 (Management of FOID/Concealed Carry)

During testing, auditors requested ISP provide the population of cash receipts received by ISP during FY19 and FY20 in order to test compliance applicable to those receipts. In response to the request, ISP provided a listing of cash receipts. The auditors noted the following problems with the ISP's population:

- The population of cash receipts did not agree to the ISPs Revenue Status Report (SB04) reconciliations for FY19 or FY20.
- The Department's June 2019 and June 2020 reconciliation contained unknown reconciliation discrepancies between the Office of the Comptroller (Comptroller) records and ISP records. The discrepancies totaled a net amount of $8,893,621 and $1,814,649 for FY19 and FY20, respectively.

Due to these conditions, auditors were unable to conclude ISP's population records were sufficiently precise and detailed under the Attestation Standards promulgated by the American Institute of Certified Public Accountants (AT-C § 205.35) to test the Department's compliance relative to cash receipts.

Even give the population limitations noted above which hindered the ability of the accountants to conclude whether selected samples were representative of the population as a whole, auditors performed testing, noting:

38 of 60 (63%) receipts, totaling $659,809, and ten of 12 (83%) refunds, totaling $13,522, did not include documentation to support the date the check was received. Therefore, timeliness of the deposit could not be determined.

In addition, the auditors noted ISP did not maintain proper segregation of custody and recordkeeping duties over receipt collection and processing. One employee was responsible for:

- Preparing a log of receipts received;
- Recording receipts in the receipts ledger; and
- Depositing funds into the State Treasury.

ISP management indicated the lack of segregation of duties over processing of receipts and refunds, and lack of supporting documentation being maintained were due to staffing shortages.

Failure to maintain proper segregation of duties may result in theft or misappropriation of assets which may not be prevented or detected. Lack of controls over the preparation and review of receipts may lead to inaccurate records and the submission of inaccurate financial information to the Comptroller.

RESPONSE:
ISP concurs procedures are necessary for proper segregation of duties, reconciliations and documentation. Procedures have been implemented segregating the duties of opening checks, logging checks and making deposits. Furthermore, ISP has been diligently working to ensure the reconciliations have proper supporting documentation. The legacy receipts system had issues that were not able to be resolved effective January 2018 which remained unresolved at December 2019 when data was converted to ERP. Unfortunately, this resulted in inaccurate data in the conversion. Staff has been diligently working on cleaning up the FY18, FY19 and FY20 issues to obtain correct figures which should have been used for the ERP conversion. FY21 reconciliations are monitored with issues being resolved in a timely manner.

UPDATED RESPONSE;
NOTE: This response also refers to both findings #2020-005 and #2020-001 (9-1-1 Fund) - Inadequate Controls Over Receipts and Reconciliations

Partially Implemented. ISP concurs with the recommendation. The duties of collecting, stamping and logging receipts has been successfully segregated from the duties of depositing and recording receipts. The SB04 reconciliations need to be reconciled within 60 days of month-end with all variances being accurately identified.

4. The auditors recommend ISP implement procedures and allocate necessary resources to properly report and fully pursue collections on delinquent accounts receivable. The auditors further recommend all eligible delinquent accounts be referred to the Comptroller's Offset System.

FINDING: *(Delinquent Accounts Not Pursued)*

ISP did not aggressively pursue the collection of accounts receivable and did not properly refer delinquent accounts receivable to the Office of the Comptroller's (Comptroller) Offset System.

ISP is owed money from various individuals and companies for items such as drug fines, over-dimensional load police escorts, property vehicles, forfeited items, licenses, and other miscellaneous items.

During testing, ISP wrote off old uncollectible or erroneous accounts receivable balances in the amount of approximately $505,000 for receivables dating as far back as 1999. However, ISP had not undertaken collection efforts for delinquent accounts receivable during FY19 or FY20. Auditors also noted ISP did not have a formal written policy for the collection of accounts receivable balances.

This finding was first noted during the examination for the two years ended June 30, 2012. In the subsequent years, ISP has been unsuccessful in implementing a corrective action plan.

ISP management indicated the collection attempts have not been accomplished due to shortage of staff. The position responsible for collection attempts has been vacant since 2008 and is no longer funded.

Failure to aggressively pursue the collection of accounts receivable through all reasonable means is noncompliance with the Illinois State Collection Act of 1986 and failure to refer all eligible delinquent accounts to the Comptroller's Offset System is noncompliance with SAMS. Further, the failure to pursue collections reduces funds available for the Department's operations.

RESPONSE:
ISP concurs collection procedures should be implemented. However, we do not have adequate staff to consistently accomplish this. ISP is diligently working on this and State Police Services Fund (906), our largest accounts receivable fund, has implemented procedures to use the Comptroller's Illinois Debt Recovery Offset System (IDROP) system. ISP will continue to work on collection procedures.

UPDATED RESPONSE:
Partially Implemented. ISP concurs with the recommendation. ISP currently have three funds with accounts receivable. Fund 906 does and has reported delinquent accounts to the Comptroller's Offset System however as most of the customer's do not receive funds from the state it is not effective. In Fund 612, three penalty notices are sent before delinquent accounts are sent to ISP Legal. ISP Legal has informed the division they work with the Office of the Attorney General for collection therefore the Comptroller's Offset System is not used. ISP is currently working on cleaning up the delinquent accounts in Fund 652 and any unresolved will either be referred to the Comptroller's Offset System or referred to the Office of the Attorney General for write-off as uncollectable.

5. The auditors recommend ISP ensure appropriation, cash receipt, cash balance, agency contract, and obligation activity report reconciliations are prepared timely and properly reviewed. In addition, the auditors recommend ISP retain documentation of the completed reconciliations.

FINDING: *(Inadequate Controls Over Monthly Reconciliations)*

During testing of FY20 and FY19 reconciliations between the Office of the Comptroller (Comptroller) records and ISP records, noted:

- Documentation was not retained to support the completion of 3 of 30 (10%) Monthly Appropriation Status Report (SB01) reconciliations.

- Monthly Revenue Status Report (SB04) reconciliations for 1 of 24 (4%) months were not performed within 60 days following the end of the month. The SB04 reconciliation was completed 25 days late.

- The year-to-date SB04 reconciliations for fiscal years ended June 30, 2020 and 2019 contained unexplained reconciliation discrepancies totaling a net amount of $1,814,649 and $8,893,621, respectively.

- SB04 reconciliations for FY20 were not reconciled by receipt account; whereby each Fund was reconciled in total.

- SB04 reconciliations for FY20 and FY19 were not reviewed by an independent person.

- Documentation was not retained to support the completion of 3 of 24 (13%) Monthly Cash Report (SB05) reconciliations.

- Agency Contract Report (SC14) and Obligation Activity Report (SC15) reconciliations for FY20 and FY19 were not completed.

ISP management indicated the lack of documentation of reconciliations and the untimely reconciliation was due to competing priorities. In addition, ISP management indicated they were unaware of the requirement to complete SB04 reconciliations by each receipt account and the SB04 reconciliations were not reviewed by an independent person due to a lack of resources.

Failure to timely reconcile monthly appropriations, cash receipts, cash balances and contract activity in accordance with SAMS could lead to unresolved differences between the Department and Comptroller records, inaccurate financial reporting, and undetected loss or theft.

RESPONSE:
ISP concurs reconciliations should be prepared timely and properly. ISP prepared timely reconciliations in FY21. The reconciliations are saved electronically.

UPDATED RESPONSE:
Partially Implemented. ISP with the recommendation. For cash receipts, please see 2020-003. ISP strives to complete the appropriation, cash balance, contract, and obligation reconciliations within 60 days of month- end; however, we are experience some issues with identifying variances due to SAP issues. We would like to have these reconciliations consistently prepared and reviewed in a timely manner by September 30, 2021. ISP retains documentation in both an electronic and hard copy.

6. The auditors recommend ISP establish controls over reconciliation and conversion of data during system development projects, such as the ERP.

FINDING: *(Lack of Due Diligence over ERP Transition)*

In January 2020, ISP implemented the State's ERP as its business process management system for the tracking of assets, contracts, obligations, and vouchers.

As part of the ISP's transition to the ERP, they converted data from legacy systems. In order to determine if the data had converted correctly, auditors requested the documentation and reconciliations. However, ISP was unable to provide documentation and reconciliations of opening balances in the ERP to ensure the correct balances were transferred.

ISP's lack of due diligence resulted in a lack of assurance over the accuracy of the data converted.

RESPONSE:
ISP concurs data converted from one system to another should be accurate. ISP relied upon the ERP team's expertise when converting data from the legacy systems to the ERP system. During future system development projects, ISP will diligently try to take a larger role in the conversion to ensure accuracy over records.

UPDATED RESPONSE:
Partially Implemented. ISP concurs data converted from one system to another should be accurate. For the fiscal side of ERP conversion, ISP relied upon the SAP team's expertise when converting data from the legacy systems to the ERP system. ISP also did not ensure that all before and after files were coded as such and saved as approved.

While the financial side is already complete and no further steps are necessary, there are future HR related activities still to go live. For these future conversions we will identify a number/naming convention to reflect the starting file for conversion and the approved final files that are loaded in ERP. ISP will document the pre and post files so it will be clear the conversion was tested and passed. ISP will ensure the approval of these conversions are saved and named accordingly so we are not reliant only on the ERP team's processes. The next ERP conversion is set to occur 1/1/22. The starting files will be locked down sometime in December, but the final conversion file would not be able to be validated until after the 1/1/22 cut-over.

7. The auditors recommend ISP allocate the necessary resources to process applications in a timely manner and ensure documentation fees are deposited in accordance with the Acts.

FINDING: *(Failure in processing of FOID and Concealed Carry Applications Timely)*

During testing of FOID applications auditors noted:

- 13 of 15 (87%) FOID applications were not processed within 30 days, with delays ranging from two to 363 days.

- 9 of 15 (60%) FOID card renewal applications were not processed within 60 business days, with delays ranging from ten to 214 days.

- ISP could not provide documentation to demonstrate the FOID card application fees were deposited in accordance with the Act. During FY19 and FY20, ISP reported collecting FOID application and renewal applications fees totaling $3,834,625 and 3,293,655, respectively.

The Firearm Owners Identification Card (FOID) Act (430 ILCS 65/5(a)) requires ISP to approve or deny all FOID card applications, except renewal applications, within 30 days from the date the application is received. The FOID Act also (430 ILCS 65/5(b)) requires ISP to approve or deny FOID card renewal applications within 60 days from the date the application is received.

Additionally, every applicant found qualified by ISP shall be entitled to a FOID Card upon payment of a $10 fee, of which $6 of the fee shall be deposited in the Wildlife and Fish Fund in the State Treasury; $1 of the fee shall be deposited in the State Police Services Fund, and $3 deposited in the State Police Firearm Services Fund. Further, the FOID Act (430 ILCS 65/5(b)) requires the cost for a renewal application to be $10, which shall be deposited into the State Police Firearm Services Fund.

Testing of 30 Concealed Carry applications noted 13 (43%) applications were not processed timely, with delays ranging from 28 to 70 days late.
In addition, ISP could not provide documentation to demonstrate the Concealed Carry application fees were deposited in accordance with the Firearm Concealed Carry Act.

ISP management indicated the Firearm Services Bureau division has not been able to keep up with the volume of applications due to lack of resources. Additionally, ISP indicated deposits are made and can be viewed by pulling information from the Treasurer's portal. However, the auditors noted the information does not provide detail on individuals' specific application fees received to determine if they were deposited into the applicable funds.

Failure to maintain proper internal controls to timely process applications results in untimely issued FOID cards and may result in renewal applicants having an expired license. Additionally, the inability to document where receipts are deposited could result in inaccuracies in deposits and shortages to the applicable funds.

RESPONSE:
ISP concurs. ISP is aware of the importance to process FOID and Concealed Carry applications in a timely manner as required by statute, as well as provide documentation to demonstrate the FOID card application fees are deposited in accordance with the Act. The Division of Justice Services will begin taking the necessary steps to develop an action plan which identifies a solution to rectify these findings and ensure they are resolved.

UPDATED RESPONSE:
Partially Implemented. The Firearms Services Bureau (FSB) will continue to request the necessary resources needed to process applications in a timely manner and ensure documentation fees are deposited in accordance with the Firearms Owners Identification and Concealed Carry Licensing Acts. The FSB began a hiring plan in March 2020 which is still in progress at the time of this finding. From March of 2020 through April of 2021 the FSB has hired 29 Firearms Eligibility Analyst (FEA) to conduct background investigations to approve or deny FOID and CCL permits. The FSB is anticipated to hire another 6 FEA's by the end of FY21 with hiring plan for 20 additional FEA's annually to account for retirements, promotions and separations. In addition to the FEA's the FSB has hired 25 contractual employees to assist FEA's with application processing to address current backlogs. The FSB will work with the State Treasurers Office and the software vendor to determine if there is the ability to document where individual receipts are deposited to ensure they are being sent to the appropriate fund. The FSB will continue to implement process efficiencies as recommended by Illuminative Strategies through a Lean 6 assessment that was conducted in FY 20. To date 32 opportunities to improve have been implemented with 30 more pending review of feasibility and potential development.

8. The auditors recommend ISP issue certificates of licenses to applicants within the timeframe established by the Act. Additionally, ISP should comply with the administrative rules.

FINDING: *(Failure to Comply with Firearms Dealer License Certification Act)*

According to ISP records, beginning May 2019 through June 2020, 1,138 federal firearms licenses were filed for certification. Additionally, ISP records stated the 1,138 federal firearms licenses were in "review status pending."

According to ISP, due to the lack of a definition of what an 'initial certification' was to entail, a compliance letter was sent for each submission. The compliance letter stated ISP was in "receipt of a copy of your Federal Firearms License and affidavit attesting to its validity in compliance with 430 ILCS 68/5-10 of the Firearm Dealer Certification Act". However, auditors could not determine if a compliance letter had been sent to the 1,138 federal firearm licenses within 30 days, due to the lack of information. ISP management further stated the Act allowed the dealers to continue to operate if ISP did not issue an initial certificate of license within the 30 days.

In addition, effective January 3, 2020, emergency administrative rules (20 Ill Admin. Code 1232) were adopted creating a process for the verification of the federal firearms license information submitted for certification. However, ISP did not comply with the emergency administrative rules.

ISP management stated, it was determined the emergency administrative rules, prepared by ISP, were 'unfair' to the dealers; therefore, they were not followed. ISP management

further stated they have subsequently worked with various parties to modify the emergency administrative rules.

The fees for certification were $523,138 for 884 licenses in FY19 and $225,550 for 254 licenses in FY20.

The Act (430 ILCS 68/5-10), effective January 18, 2019, requires a licensee with a valid Federal Firearms License to file with the Department a copy of its license, together with a sworn affidavit, indicating the license is in fact theirs and is valid.

ISP may by rule create a process for checking the validity of the license, in lieu of requiring the affidavit. Upon receipt and review by the Department, the Department is to issue a certificate of license to the licensee, allowing the licensee to conduct business within the State. The Department is to issue an initial certificate of license within 30 days of receipt of the copy of license and sworn affidavit. If the Department does not issue the certificate within 30 days, the licensee is allowed to operate as if a certificate has been granted unless and until a denial is issued by the Department.

ISP's failure to comply with the emergency administrative rule and issue or deny an initial certificate of license to dealer applicants submitting Federal Firearm licenses in a timely manner could result in licensees conducting business in the state that have not been verified by ISP.

RESPONSE:

ISP concurs in part. It is inaccurate to state the ISP's position is the rules were unfair to dealers so the ISP chose to not follow the rules. Rather, because the emergency rules were still subject to change and there could be a significant financial impact to dealers, the ISP chose to postpone enforcing compliance with all of the rules until the final rules were put into place. As of April 5, 2021 the final rules have not been published by the Joint Committee on Administrative Rules with the video surveillance portion of the rules still pending. The video surveillance section of the administrative rules has the potential of having the most financial impact to dealers.

ISP may by rule create a process for checking the validity of the license, in lieu of requiring the affidavit. Upon receipt and review, ISP is to issue a certificate of license to the licensee, allowing the licensee to conduct business within the State. ISP is to issue an initial certificate of license within 30 days of receipt of the copy of license 30 days, the licensee is allowed to operate as if a certificate has been granted unless and until a denial is issued by the ISP.

ACCOUNTANT'S COMMENT

ISP disputes the statement in the finding that ISP did not follow its emergency administrative rules because ISP determined those rules were unfair to the dealers. This information was provided by ISP management to the auditors in a phone conversation on March 26, 2021. Although we understand ISP no longer agrees with this statement the finding accurately represents ISP's position at the time of our fieldwork.

The auditors would further point out that adoption of rules is optional and not necessary for ISP to carry out its responsibilities under the Act and, therefore, the absence of rules does not excuse its non-performance.

UPDATED RESPONSE:
Partially Implemented. ISP concurs with the recommendation. The final administrative rules for firearm dealer licensing were approved in late April 2021. The FSB had preliminarily approved all the dealers prior to the completion of the JCAR rules. The approved rules also included a change in the pay structure for licenses that resulted in the need to provide a refund for the majority of dealers that submitted an application prior to approval of the rules. The FSB is working with the Treasurer's Office and the ISP Finance Office to establish vendor accounts for every dealer to allow for the reimbursement for any overpayment of fees previously submitted. As the dealers are refunded, they will be permitted to renew their certifications at which time they will be approved and issued a certificate of license. It is important to note the fully implemented rules will change many dealers from non-retail to retail locations and will thereby change their fee owed.

9. The auditors recommend ISP comply with the Act by making key information related to the firearms used in the commission of crimes in the State publicly available and to study, compile, or share reports on the number of FOID card checks to determine firearms trafficking or straw purchases patterns.

FINDING: *(Noncompliance with the Gun Trafficking Information Act)*

During testing, noted:

- ISP did not make publicly available, on a regular and ongoing basis, key information related to firearms used in the commission of crimes in the state, as required by the Act.

- ISP did not study, compile, or share reports on the number of FOID card checks to determine firearms trafficking or straw purchases patterns, as required by the Act.

ISP management indicated the information regarding the firearms used in the commission of crimes in the state was not complied with and ISP's reporting regarding FOID card checks was not operational due to a lack of resources. Failure to publicly make available key information and complete studies is a violation of the Act.

RESPONSE:
ISP concurs. ISP understands the importance of transparency with the public and will work across all divisions towards providing the information required by statute 5 ILCS 830/10-5 Gun Trafficking Information Act.

UPDATED RESPONSE:
Partially Implemented. ISP concurs with the recommendation. ISP has been working with DoIT to explore options to create a system that can be utilized by all agencies across the state to compile the data from the number of FOID card checks. Information from this will be posted to an on-line dashboard to make it available to the public. When completed this will meet the requirement to make information involving the use of firearms used in the commission of crimes publicly available. Personnel within the Director's Office are working with legislators to fully identify the needs and requirements within the law as it pertains to the Illinois State Police.

10. The auditors recommend ISP identify all service providers and determine and document if a review of controls is required. If required, ISP should:

- **Obtain SOC reports or (perform independent reviews) of internal controls associated with outsourced systems at least annually.**
- **Monitor and document the operation of the Complementary User Entity Controls (CUECs) relevant to ISP operations.**
- **Either obtain and review SOC reports for subservice organizations or perform alternative procedures to satisfy itself that the usage of the subservice organizations' would not impact ISP's internal control environment.**
- **Document its review of the SOC reports and review all significant issues with subservice organizations to ascertain if a corrective action plan exists and when it will be implemented, any impacts to ISP, and any compensating controls.**
- **Review contracts with service providers to ensure applicable requirements over the independent review of internal controls are included.**

FINDING: *(Lack of Controls Over Review of Internal Control Over Service Providers)*

The auditors requested ISP provide the population of service providers utilized in order to determine if ISP had reviewed the internal controls over the service providers. In response to the request, ISP was not able to provide a complete listing of service providers utilized during the examination period.

Due to these conditions, the auditors were unable to conclude ISP's population records were complete and accurate under the Professional Standards promulgated by the American Institute of Certified Public Accountants (AT-C § 205.35). Even given the population limitations noted above which hindered the ability of the accountants to conclude whether the population was complete, during testing of the service providers identified, the auditors noted ISP had not:

- Obtained System and Organization Control (SOC) reports or conducted independent internal control reviews for four service providers.

- Conducted an analysis of the SOC reports, when available, to determine the impact of modified opinions or noted deviations.

- Obtained and reviewed the SOC report for subservice organizations or performed alternative procedures to satisfy itself that the usage of the subservice organizations' would not impact ISP's internal control environment.

- Conducted an analysis of the complementary user entity controls documented in the SOC reports, when available.

- Ensured contracts with service providers include applicable requirements over the independent review of internal controls.

ISP is responsible for the design, implementation, and maintenance of internal controls related to information systems and operations to ensure resources and data are adequately protected from unauthorized or accidental disclosure, modifications, or destruction. This responsibility is not limited due to the process being outsourced.

ISP management indicated they were not aware of the need to perform and document an internal control review of service providers.

Without having obtained and reviewed a SOC Report or another form of independent internal control review, ISP does not have assurance the service providers' internal controls are adequate to ensure personal information is secure.

RESPONSE:
ISP concurs and will work to identify all services providers. Furthermore ISP will document if a review of controls is required.

UPDATED RESPONSE:
Partially Implemented. ISP has identified all service provider contracts and separated them by fiscal year. ISP will review the contracts to determine if a review of controls is required and document them appropriately. If ISP determines the service providers have been delegated any internal controls which have a fiscal/financial nature or deal with information flow software (data) that leads to ISP's financial statement; ISP will either obtain a SOC report or conduct independent reviews using alternative procedures to ensure the internal controls are operating effectively and to check for accuracy.

ISP will obtain SOC reports or conduct alternative procedures at least annually. ISP will also have Divisions or work units monitor and document the operation of Complementary User Entity Controls (CUECs) relevant to ISP operations pertaining to service providers. CUECs are the controls the service provider has included within their system and rely on the Department to implement in order to achieve the service provider's control objectives.

If the service provider ISP has a contract with uses subservice organizations and rely on them to perform one of our internal controls that could impact our financial statements or information flow software (data), then we will request either a SOC report or perform alternative procedures to ensure the internal controls are operating effectively and to check for accuracy. ISP will document its' review of the SOC report or alternative procedures for any subservice organization and any significant issues with them. ISP will review all future service provider contracts to ensure language has been added to include requirements over the independent review of internal controls, if applicable.

11. The auditors recommend that ISP:

- **Maintain documentation of all users for each of their applications.**
- **Ensure application user access is properly authorized and documented,**
- **Ensure application user access is timely deactivated for separated employees; and,**
- **Perform and document annual reviews of user access rights to ensure individual levels of access are appropriate.**

FINDING: *(Failure to Maintain Security Controls Over Computer Systems)*

As a result of ISP's mission to "promote public safety to improve the quality of life in Illinois", ISP collected and maintained a significant amount of confidential information.

The auditors requested ISP provide the population of application users for six applications utilized. In response to the request, ISP was not able to provide complete populations for three (50%) applications.

Even given the population limitations noted above which hindered the ability of the accountants to conclude whether selected samples were representative of the population as of whole, the auditors tested a sample of user access, noting ISP did not provide documentation demonstrating:

- New application users were properly authorized,
- Users access rights were timely deactivated for separated employees; and
- An annual or periodical reviews of access rights had been completed.

This finding was first noted during the examination of the two years ended June 30, 2010. In the subsequent years, ISP has been unsuccessful in implementing a corrective action plan.

ISP management indicated the lack of security controls was due to IT staffing constraints. Failure to properly authorize, timely deactivate, and review user access rights could result in inappropriate access to ISP's systems.

RESPONSE:
ISP concurs. ISP fully understands the importance of maintaining adequate security controls over computer systems to safeguard confidential information. The Division of Justice Services will begin taking the necessary steps to develop an action plan which identifies a solution to rectify this finding and ensure the Fiscal Control and Internal Auditing Act is adhered to.

UPDATED RESPONSE:
Partially Implemented. ISP will create a proper on-boarding, off-boarding and tracking process for user access. This will include the creation of an off-boarding process for the agency that is endorsed by ISP command. Also, ISP will evaluate SAP's role in the on-boarding and off-boarding process. ISP will expand the existing user access form to include all ISP/DoIT applications. Furthermore, ISP will annually review user access rights for proper access by evaluating Sailpoint for possibility of performing annual user account audits.

12. The auditors recommend ISP implement controls to ensure report components are accurately and completely prepared in future compliance examinations.

FINDING: *(Failure to Demonstrate the Completeness and Accuracy of the Report Components)*

During the course of this examination, ISP's internal controls were inadequate to both (1) prepare the report components and (2) demonstrate the report components that ISP management prepared were complete and accurate.

Specifically, noted:

- The *Schedules of Appropriations, Expenditures, and Lapsed Balances* was prepared by ISP management from their own records. However, review of the *Schedules*, noted differences between ISP and the Office of the Comptroller's records.

- The *Comparative Schedule of Net Appropriations, Expenditures, and Lapsed Balances* was prepared by ISP management from their own records. However, review of the *Schedule*, noted differences between ISP and the Office of the Comptroller's records.

- The *Comparative Schedule of Net Expenditures by Major Activity* was prepared by ISP management from their own records. However, review of the *Schedules*, noted differences between ISP and the Office of the Comptroller's records.

- The *Comparative Schedule of Cash Receipts and Deposits into the State Treasury* was prepared by ISP management from their own records. However, review of the

Schedule, noted differences between ISP and the Office of the Comptroller's records.

The *Schedule of Locally-Held Funds* was prepared by ISP management from their own records. However, review of the *Schedule*, noted differences between ISP and the Office of the Comptroller's records.

- The *Schedule of Changes in Property* was prepared by Department management from their own records. However, review of the *Schedule*, noted differences between ISP records and *the Department's Report of State Property* (Form C-15) filed with the Office of the State Comptroller.

- The *Analysis of Significant Variations in Expenditures*, which comments on the underlying cause for why significant variations occurred within various line item expenditures during each fiscal year, as measured by dollar amount or percentage change, omitted several significant variances between FYs19 and 18.

- The *Analysis of Significant Variations in Receipts*, which comments on the underlying cause for why significant variations occurred within various line receipt sources during each fiscal year, as measured by dollar amount or percentage change, omitted several significant variances between FYs19 and 18 and between FYs 20 and 19.

- The *Analysis of Significant Lapse Period Spending*, which comments on the significant Lapse Period expenditures, as measured by dollar amount or percentage change, omitted several significant variances FY20 and omitted several significant variances for FY19.

- ISP provided the *Number of Employees*; however, the information was not in a format to be comparative to the information from FY18.

- ISP did not provide an *Analysis of Overtime and Compensatory Time*.

As a result of the unresolved doubts and noted omissions concerning each of these report components, the report components were omitted from ISP's *Compliance Examination Report*.

ISP management indicated they have experienced difficulties in completing the Report Components for two primary reasons. This is the first time they have been required to complete the schedules and lack expertise in doing so. Additionally ISP is still learning how to pull required information from their new financial system.

Compliance examinations stress the fundamentals of governmental accountability, including providing transparency about ISP's fiscal and administrative controls and whether ISP's resource utilization was efficient, effective, and in compliance with applicable law. Failure to prepare accurate and complete report components hinders the

ability of users of the *Compliance Examination Report* to obtain additional analysis of the ISP's operations.

RESPONSE:
ISP concurs that report components should be accurately prepared for future compliance examinations.

UPDATED RESPONSE:
Accepted. The OOF will work with the auditors during the next audit period to ensure the report components are accurately and completely prepared. ISP will add this to our list of duties to be performed for the audit. A list of required information will be included in the working folder for audits. This information will then be added to the calendar of supervisors to ensure it is obtained.

LAC FOLLOW-UP TO UPDATED RESPONSE

Received by the LAC on 9/30/2021

LAC staff have reviewed ISP's updated response to Finding 12, and would like a little more information, if possible. Is there a process currently in place to timely reconcile Department records with the IOC? Is your agency currently reconciling the ISP's financial records with the IOC's records within 60 days after the end of each month?

ISP: Yes, SB01, SB04 and SB05 are being reconciled within 60 days.

ISP noted in its original response to the LAC that it was "still learning how to pull required information from the new financial system." Has the ISP seen improvement in being able to access the necessary data to address this finding? How is the new financial system working, and is it operating at full capacity at this time?

ISP: ISP has implemented the HANA SB04 rec for FY22 and there appear to be no issues. Other information to be pulled from the new financial system is still in the process of rectified.

13. ISP has the ultimate responsibility for ensuring confidential information is protected from accidental or unauthorized disclosure. Specifically, the auditors recommend the ISP:

- **Perform a comprehensive risk assessment to identify and ensure adequate protection of information most susceptible to attack.**
- **Classify its data to identify and ensure adequate protection of information.**
- **Evaluate and implement appropriate controls to reduce the risk of attack.**
- **Develop a formal, comprehensive, adequate and communicated security program to manage and monitor the regulatory, legal, environmental and operational requirements.**

- **Deploy encryption software on all laptops and data at rest.**
- **Ensure electronic storage media is erased, wiped, sanitized, or destroyed in accordance with the destruction processes required by Act. Additionally, the Department should maintain documentation of such.**

FINDING: *(Weakness in Cybersecurity Programs and Practices)*

As a result of ISP's mission to "promote public safety to improve the quality of life in Illinois", ISP maintains computer systems that contain large volumes of confidential or personal information such as names, addresses, and Social Security numbers of the citizens of the State.

The Illinois State Auditing Act (30 ILCS 5/3-2.4) requires the Auditor General to review State agencies and their cybersecurity programs and practices. During examination of ISP's cybersecurity program, practices, and control of confidential information, the auditors noted ISP:

- Had not performed a comprehensive risk assessment to identify and ensure adequate protection of information (i.e. confidential or personal information) most susceptible to attack.

- Had not classified its data to identify and ensure adequate protection of information.

- Had not evaluated and implemented appropriate controls to reduce the risk of attack.

- Had not developed a formal, comprehensive, adequate and communicated security program (policies, procedures, and processes) to manage and monitor the regulatory, legal, environmental and operational requirements.

- Had not deployed encryption software on all laptops and data at rest.

- Had not ensured electronic storage media was erased, wiped, sanitized, or destroyed in accordance with the destruction processes required by the Data Security on State Computers Act (Act). Specifically, the auditors requested documentation for 60 items disposed of during the examination period; however, the Department did not provide documentation demonstrating the items were disposed of in accordance with the Act.

ISP management indicated the weaknesses were due to IT staffing constraints.

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

RESPONSE:
ISP concurs. ISP fully understands the importance of implementing adequate internal controls related to cybersecurity programs and practices. The Division of Justice Services will begin taking the necessary steps to develop an action plan which identifies a solution to rectify this finding.

UPDATED RESPONSE:
Partially Implemented. ISP will ensure encryption software is installed on all laptops by August 31, 2021. Meanwhile, monitoring and logging of environment is currently being performed at DoIT Security Operations Center (SOC). ISP currently has a Firewall and F5 Load Balancer in place to secure the environment. All logs and activity are sent to DoIT SOC for monitoring and monthly vulnerability scans are performed on servers within the environment. ISP has already begun classifying data on an application basis. ISP and DoIT will investigate the possibility of DoIT Corporate Security performing a risk assessment. If they are unable to perform, ISP and DoIT will procure a vendor to perform the assessment. In order to address the electronic media destruction, ISP has Directive SRV-225 which addresses electronic storage being sanitized and destroyed. An internal process has been defined for performing the destruction and has been utilized since January 2020.

14. The auditors recommend ISP comply with the Act and the Code to ensure vouchers are approved and paid within the required time frame and the required interest is paid. Also, the auditors recommend requests for out of State travel be submitted through eTravel 30 days in advance of the departure date.

FINDING: *(Voucher Processing Weakness)*

ISP did not exercise adequate controls over voucher processing.

During testing, the auditors noted:

- Seventy-two of 251 (29%) vouchers tested, totaling $5,278,527, were approved for payment from 1 to 153 days late.

- Three of 251 (1%) vouchers tested, totaling $32,230, accrued required interest charges of $620 which were not paid by the Department.

- Two of 40 (5%) travel vouchers tested, totaling $4,445, were for travel expenses incurred outside of the borders of the State of Illinois where the Department did not timely request preapproval from the Governor's Office of Management and Budget for the travel. The two requests were approved 23 days prior to and 33 days after the first day of the trip.

This finding was first noted during the examination of the two years ended June 30, 2004. In subsequent years, the Department has been unsuccessful in implementing a corrective action plan.

ISP management indicated late approvals were due to lack of sufficient staffing and prompt payments were not made due to oversight.

Failure to promptly review and approve proper bills resulted in late payment of bills and caused the State to incur interest penalties. Failure to pay interest charges is noncompliance with the Act. Also, failure to exercise adequate control over travel expenditures represents noncompliance with the State's travel regulations.

RESPONSE:

ISP concurs. In June 2019, the Accounts Payable unit was brought back to ISP from the Public Safety Shared Services Center. Staff were hired in June and expected to begin working on FY20 vouchers. However, after training new ISP staff, the PSSSC turned all outstanding vouchers over to them. This included a large backlog of FY19 vouchers that staff had to get caught up on. This caused new FY20 vouchers to sit longer than expected. As soon as FY19 lapse documents were caught up, staff focused again on processing FY20 vouchers in a timely fashion. Then in December 2019 (in anticipation of conversion to the new ERP system) we put a hold on all voucher processing for a few weeks. This was necessary so that no invoice would be lost in the conversion and inadvertently not get sent to the Comptroller. Since converting to ERP, ISP has instituted a 30-day memo process. This requires the end user to have upper management sign a letter explaining any delay that prohibited them from entering the invoice in a timely fashion. This has limited the number of vouchers turned in for approval that are beyond the 30 day window. Central Accounts Payable, who apply level one and two approvals, currently turn around invoices within no more than 72 hours, and usually only 48.

Prompt payment interest has been a very manual process for ISP prior to ERP. Now that ISP is on ERP we anticipate this process to be easier and more timely. in addition the system creates shells with the calculations already applied.

ISP will continue to review out of state travel vouchers thoroughly and look into ways to ensure no voucher is approved without the eTravel documentation.

UPDATED RESPONSE:

Partially Implemented. Since March of 2020, Illinois State Police Accounts payable has been requiring a memorandum signed by, at minimum, the Bureau Chief explaining why any vouchers are processed more than 30 days of the Proper Bill Date. To strengthen this control, Accounts Payable will begin tabulating a list of invoices falling in this category, by Bureau, and will report this number to the Chief Financial Officer or delegate. Once the memorandums are received, the CFO will email each corresponding Colonel and Chief of Staff of the corresponding Division(s) to remind them of the policy violation. This same approach will be used for out of state travel invoices that did not submit through eTravel 30 days in advance of the departure date. These measures are to be in

compliance with the State Prompt Payment Act (Act) (30 ILCS 540/3-2) and reduce prompt pay interest due to late processing of invoices. In addition to requiring the 30-day memorandum, the Office of Finance will periodically remind users about processing invoices in a timely fashion and about the eTravel requirements.

15. The auditors recommend ISP comply with specific statutory mandates and explore options to utilize the financial resources to fund existing and new mandated responsibilities. The auditors further recommend ISP seek legislative remedy to those requirements they determine to be redundant and inefficient.

FINDING: *(Noncompliance with Specific Statutory Mandates)*

During testing, auditors noted:

- ISP did not have six bilingual on-board frontline staff members during FYs19-20 to be in compliance with the State Services Assurance Act of FY2008.

The State Services Assurance Act for FY2008 (5 ILCS 382/3-15) requires ISP to have at least five additional bilingual on-board frontline staff members from the original number of bilingual on-board frontline staff members on June 30, 2007, which was one.

ISP management indicated bilingual staff are in high demand and they have not been able to recruit and retain staff for these positions.

- ISP did not establish a policy to control the acquisition, storage, transportation, and administration of an opioid antagonist, as required by the Substance Use Disorder Act.

The Substance Use Disorder Act (20 ILCS 301/5-23(e)(1)) requires every State agency that employs law enforcement officers to possess opioid antagonists and establish a policy to control the acquisition, storage, transportation, and administration of opioid antagonists.

ISP management indicated the policy amendments are being reviewed by subject matter experts throughout ISP.

- ISP did not prepare or submit quarterly reports on arrest-related deaths to the IL Criminal Justice Information Authority (ICJIA) in accordance with the Uniform Crime Reporting Act.

The Uniform Crime Reporting Act (50 ILCS 709/5-12(1)) requires ISP to submit on a quarterly basis, all information collected from law enforcement agencies regarding arrest-related deaths, to the Illinois Criminal Justice Information Authority (ICJIA).

ISP management indicated arrest related information is sent to ICJIA at the conclusion of the calendar year. Furthermore, ISP management indicated quarterly reports would be incomplete and a burden on the few resources of the Uniform Crime Reporting Division.

- The Department did not prepare or submit annual statistical compilations and related data for the State Board of Education regarding incidents involving firearms or drug related incidents in schools as required by the School Code (Code).

ISP management indicated the data is posted on the Uniform Crime Reporting Program web page and is aggregated by the law enforcement entity reporting the incident. ISP management also indicated sending the data to the State Board of Education is viewed as redundant and inefficient.

- ISP did not enforce the provisions of the Smoke Free Illinois Act (Act) regarding smoking in prohibited areas through the issuance of citations, and did not assess civil penalties pursuant to the Act.

ISP management indicated the opportunity must present itself before they are able to enforce the provisions of the Act.

- ISP failed to notify the Illinois State Library, Government Documents Section in writing of whom was responsible for the distribution of publications during FY19.

ISP management indicated the cause was due to oversight.

- ISP failed to furnish registration information concerning persons who are required to register under the Arsonist Registration Act to the Office of the State Fire Marshal.

ISP management indicated the upcoming Law Enforcement Agencies Data System (LEADS) version 3.0 would be the best system to provide the information; however, the system has not been rolled out statewide.

- ISP did not provide monthly and annual statistical compilations of attacks on school personnel to the Illinois State Board of Education.

ISP management indicated ISBE worked collaboratively with ISP to develop and utilize the School Incident Reporting System maintained by ISBE instead of utilizing the less timely Illinois Uniform Crime Reporting Program maintained by ISP.

Failing to maintain bilingual frontline staff, approve policies to control mandated supplies, notify the Illinois State Library, and to enforce provisions of Acts by issuance of citations, is noncompliance with ISP's mandated responsibilities and may alter the intended effect of the mandates. Additionally, failure to submit reports could result in inaccurate quantification of the achievements of ISP and denies the intended users of necessary

information. Furthermore, failing to provide information to other agencies prevents them from effectively serving the people of the state.

RESPONSE:

ISP concurs. ISP fully understands the importance of compliance with specific statutory mandates. ISP believes it had six bilingual on-board frontline staff members during FY19 and FY20 to be in compliance with the State Services Assurance Act of FY2008. However, ISP is unable to accurately report that information. ISP will develop an efficient and effective way to report on bilingual employees hired during the respective timeframe. ISP also does concur with the finding of failing to enforce the provisions of the Smoke Free Illinois Act (Act) regarding smoking in prohibited areas through the issuance of citations and did not assess civil penalties pursuant to the Act. Regarding the failure to prepare or submit annual statistical compilations for ISBE regarding incidents involving firearms or drug related incidents in schools as required by the School Code (Code), ISP is at the mercy of outside agencies submitting data to ISP to complete this report. With the remaining findings, ISP will begin taking the necessary steps with the Divisions effected by these findings to develop an action plan which identifies a solution to rectify these findings and will work towards meeting the statutory mandates.

UPDATED RESPONSE:

Partially Implemented. ISP has been working with CMS and DoIT to implement a Human Capital Management (HCM) system designed to streamline the application and hiring process, timekeeping, and establish an Employee Central which will be a repository for employee information. Employees will be able to update their own information which will include an area for language skills. This will meet the requirement for identifying and tracking bi-lingual employees. The Division of Patrol (DOP), Protective Services Unit (PSU), will implement a once a day exterior premises check at the Thompson Center in Chicago, for compliance and enforcement of the Smoke Free Illinois Act (410 ILCS 82/40 through 75). These daily checks will be documented on a newly created Excel spread sheet for recording and retention. The log will be kept by the Operations Supervisor. The PSU Shift Commander with assign this task to a police officer with enforcement powers to cite violators of the Smoke Free Illinois Act (410 ILCS 82/40 through 75). The record of the check and possible enforcement of the Smoke Free Illinois Act (410 ILCS 82/40 through 75) will be reported through the Chain-of-Command to the Operation Supervisor and recorded daily. The retentions of this record will show compliance from DOP in reference to enforcing the Smoke Free Illinois Act (410 ILCS 82/40 through 75). The Arsonist Registration Act (730 ILCS 148/60) requires ISP to furnish to the State Fire Marshal the registration information concerning persons who are required to register under the Arsonist Registration Act.

The upcoming Law Enforcement Agencies Data System (LEADS) version 3.0 is the best system to collect and provide the information; however, the system has not been rolled out Statewide. LEADS 3.0 is scheduled to be implemented in the summer 2021. Once implementation activities are complete, attention can be turned to developing an Arsonist Registration file in the new system. The Division of Justice Services will add an annual reminder to the Division's tickler system in order to prompt the Record Retention

Coordinator to notify the Illinois State Library, Government Documents Section, in writing of whom will be responsible for the distribution of publications. Additionally, the Logistics Bureau Supervisor for the Record Retention Coordinator will set an annual reoccurring Outlook email/calendar reminder for the first Monday of each calendar year to ensure the appropriate notification is made.

ISP did not prepare or submit quarterly reports on arrest-related deaths to (ICJIA) in accordance with the Uniform Crime Reporting Act

With the implementation of the Illinois National Incident Based Reporting System (NIBRS) Repository on January 2021, the Illinois Uniform Crime Reporting Program will have the ability to report school incidents in real time. By giving the ISBE their own unique user name and password, they will be able to access the statutorily mandated data when they choose and in any manner they require. A report specific to this statute has been developed and implemented. The Illinois State Police Uniform Crime Reporting Program's Illinois NIBRS Repository will be fully implemented when the current summary reporting site sunsets on December 31, 2022. The ISP will amend policy OPS-040 - Emergency Medical Services/Emergency Medical Responder/Basic Life Support to include the acquisition, storage, transportation, and administration of an opioid antagonists.

16. The auditors recommend ISP make all reasonable efforts to collect the overpayment.

FINDING: *(Failure to Collect Overpayments)*

The Illinois State Police (Department) did not collect an overpayment to an employee. In Fiscal Year 2018, the Department overpaid an employee $51,691. The overpayment was being recovered through payroll deductions; however, $26,860 remained uncollected as of June 30, 2018.

During the current examination, ISP could not provide documentation the remaining overpayment had been collected.

ISP management indicated the overpayment was not collected due to oversight.

Failure to collect overpayments is an abuse of State funds.

RESPONSE:
ISP concurs with the recommendation and any overpayment that is uncollectable by ISP will be referred to the Comptroller for Involuntary Withholding. This specific overpayment has been referred to the Legal Office in an attempt to collect, due to the fact there are additional issues related to the overpayment and this employee.

UPDATED RESPONSE:
Partially Implemented. The Payroll Department will make written contact for collection and repayment agreement within 5 business days and create a dedicated overpayment tracking system for each Code and Sworn employees. The tracker will notate employee name, overpayment amount and type including dates of contact for request of payment and date of completion.

17. The auditors recommend ISP ensure accurate Reports are timely filed with the Comptroller.

FINDING: *(Inadequate Control Over Fee Imposition Reports)*

During testing, auditors noted:

- 16 of 16 (100%) fees reported in FY19 did not agree to ISP records. Total fees reported were $42,063,608; however, total fees per ISP records were $44,685,220, a difference of $2,621,612.

- ISP failed to report the firearm dealer license certification fees in FY19. Department records documented total fees collected of $1,085,242.

- 17 of 17 (100%) fees reported in FY20 did not agree to ISP records. Total fees reported were $31,670,312; however, ISP records documented $32,476,056, a difference of $805,744.

- The FY19 Report was filed on August 7, 2019 and the FY20 Report was filed on August 7, 2020. Both were filed 6 days late.

ISP management indicated the Reports were completed using the latest data available even though ISP's receipts records had not been reconciled to the Comptroller's receipts records.

Filing inaccurate and untimely Reports results in the Comptroller reporting inaccurate fee information to the General Assembly.

RESPONSE:
ISP concurs accurate Reports should be filed timely with the Comptroller. Due to the implementation of a new accounting system, a number of accounts in the financial records were not fully reconciled. Because of this, ISP utilized the Comptroller (IOC)'s receipts, in conjunction with known cash in transit adjustments, both prior year and current year. The unreconciled variances between ISP and IOC's records resulted in a variance in reported amounts on the Fee Imposition Report. With the new accounting system in place, ISP is working on properly reconciling and correcting the receipt records to resolve this issue going forward.

UPDATED RESPONSE:
Implemented. ISP is working as time permits to clean up prior years and FY21 is currently reconciled. We have instituted reminder dates through the calendar software in order to strive for accurate and timely report filings.

18. The auditors recommend ISP ensure policies and procedures are followed and regular maintenance is performed on state vehicles. In addition, ISP should maintain documentation of all maintenance performed.

FINDING: *(Inadequate Control Over State Vehicles)*

Testing of ISP's vehicle maintenance records (vehicles) indicated vehicle maintenance was not performed in accordance with ISP policies and procedures, whereby:

- 47 of 60 (78%) vehicles did not have regular oil changes. Oil changes occurred from 6 to 14,036 miles in excess of 5,000 miles.

- 38 of 60 (63%) vehicles did not have regular tire rotations. Tire rotations ranged from 21 to 14,825 miles in excess of 10,000 miles.

- 33 of 60 (55%) vehicles did not have the fuel and air filter replaced as required. Services were performed from 18 to 15,416 miles in excess of 15,000 miles.

- 6 of 60 (10%) vehicles did not have the automatic transmission fluid and filter replaced every 50,000 miles. Services were performed from 158 to 6,785 miles in excess of 50,000 miles.

- 8 of 60 (13%) vehicles did not have the spark plugs and wires replaced every 60,000 miles. Services were performed from 100 to 1,543 miles in excess of 60,000 miles.

- 6 of 60 (10%) vehicles did not have the cooling system drained, flushed, and filled every 80,000 miles. Services were performed from 57 to 4,137 miles in excess of 80,000 miles.

- 3 of 60 (5%) vehicles did not have PCV valve and rear axle lube replaced every 100,000 miles. Services were performed from 50 to 1,058 in excess of 100,000 miles.

ISP's Vehicle Assignment and Maintenance Directive, EQP-001, requires all operators of state-owned motor vehicles to maintain their assigned vehicle in accordance with the Preventative Maintenance Schedule (Form 2-41). Form 2-41 requires services at the following mileage intervals: change oil and filter every 5,000 miles, rotate tires every 10,000 miles, replace fuel and air filter every 15,000 miles, change transmission fluid and filter every 50,000 miles, replace spark plugs and wires every 60,000 miles, drain and fill

cooling system every 80,000 miles, and have PCV valve and rear axle lube replaced every 100,000 miles. In addition, Section III.F.2.b. of the Directive states oil changes are to be conducted at 5,000-mile intervals.

ISP management indicated many of the maintenance deficiencies identified are the result of record keeping issues rather than a lack of vehicle maintenance being performed.

Failure to perform regular maintenance on State vehicles could result in more significant expenditures related to the repair or replacement of the vehicles.

RESPONSE:
ISP concurs with the finding. Many identified deficiencies are a mix of improper service schedules by vehicle operators and errors in data entry in to the fleet system by the work units. The Office of the Statewide 9-1-1 Administrator, Fleet Services Bureau, is working with DoIT to upgrade the current system, which would include creating the capability for direct uploads of maintenance repairs from CMS directly to ISP the fleet system. While these upgrades are being worked on, the Fleet Services Bureau will continue to remind employees of the importance of strictly adhering to the provided maintenance schedules for ISP-owned vehicles, as written in Illinois State Police Directive *EQP-001, Department Vehicle Assignment and Maintenance* and the Preventative Maintenance Schedule (Form 2-41). In addition, it is important to note that the preventative maintenance schedule is based on exact intervals of mileage rather than ranges. In some instances, interval numbers have to be slightly exceeded based on operational necessity and within an employee's performance of duty.

UPDATED RESPONSE:
Partially Implemented. A Corrective Action Plan has been developed. The Office of the Statewide 9-1-1 Administrator, Fleet Services Bureau will ensure future compliance with recommended maintenance schedules by sending a reminder email to fleet officers in all work units for distribution to appropriate personnel. Additionally, code and contractual personnel with assigned vehicles will receive the same email as a reminder to follow required service intervals prescribed by CMS. Additionally, the FleetFA system will be updated by DoIT to accept automatic service and maintenance updates from CMS. This will negate the need for double entry by CMS and then also by ISP and should result in more accurate maintenance records. System upgrades by DoIT for the CMS systems are expected to begin in June 2021 and be completed by July 2022. Reminder emails are planned to be sent out in May 2021.

19. The auditors recommend ISP ensure employees submit Request for Time Off forms and weekly timesheets in accordance with the Code and ISP Directives. The auditors also recommend ISP maintain documentation of the Request for Time Off and the time sheets. In addition, The auditors recommend supervisors timely review timesheets and approve overtime prior to being worked.

REVIEW: 4516 (Compliance) and 4517 (Management of FOID/Concealed Carry)

FINDING: *(Inadequate Control Over Employee Attendance Records)*

Auditors reviewed a sample of attendance records for employees noting:

- 17 of 60 (28%) employees failed to submit a Request for Time Off forms to their supervisor for approval.

- 39 of 60 (65%) employees Request for Time Off forms were unable to be located.

- 30 of 37 (81%) code employees did not submit weekly timesheets in a timely manner. The weekly timesheets were submitted between nine to 360 days late.

- 3 of 37 (8%) code employees failed to submit weekly timesheets for one or more of the time periods.

- 16 of 37 (43%) code employees submitted weekly timesheets which were not timely approved by a supervisor. Timesheets were approved from 9 to 587 days late.

- 16 of 60 (27%) employees failed to obtain prior approval from a supervisor for overtime hours worked.

ISP management indicated it was not known if the employees failed to submit a Request for Time Off or if the request was not retained by ISP as required. ISP also indicated the untimely submission and approvals of time sheets were due to employee and supervisor oversight. Further, ISP indicated the missing overtime approvals were due to the approvals being made verbally or by email rather than in the attendance system.

RESPONSE:
ISP concurs with the recommendation and all employees will be reminded of the requirement to be compliant with the Personnel Code and Department Directives as it relates to timekeeping and overtime approvals.

UPDATED RESPONSE:
Partially Implemented. The Human Resource Bureau will send out a reminder to all Chiefs of Staff to disseminate the reminder to all employees and supervisors of the requirement for timely submission of Time Off Requests and timely submission of Weekly Time Reports (time sheets). In addition, a reminder will be given that all overtime is to be pre-approved either verbally or email/text and a notation should be made on the overtime request in the comment section. That documentation (email/text) should be maintained in support of the sequence for audit purposes. The Human Resources Bureau will make corrections/changes to the PER-025 Timekeeping Directive to include the timely requirement which is lacking in the current directive. Additional changes will be included.

20. The auditors recommend ISP ensure periodic reviews of the design of major new electronic data processing systems and major modifications to existing systems are performed as required by the Act.

FINDING: *(Noncompliance with the Fiscal Control and Internal Auditing Act)*

ISP did not perform periodic reviews of the design of major new electronic data processing systems and major modifications to existing systems during the period under examination. ISP maintained approximately 68 electronic data processing systems which contained critical, financially sensitive or confidential data during the period under examination.

ISP management indicated the Internal Audit Division has not been able to hire an information systems auditor for several reasons, including budget constraints and other hiring limitations.

RESPONSE:
ISP concurs. The Office of Inspections and Audits completed an information technology security audit within FY21 and will continue its efforts to comply with the FCIAA for information technology reviews in coordination with DoIT.

UPDATED RESPONSE:
Partially Implemented. The Office of Inspection and Audits (I&A) began coordination with ISP command and the ISP DoIT management team to incorporate in the two year audit plan and conduct periodic reviews of the design of major new electronic data processing systems and major modifications to existing systems as mandated by the Fiscal Control and Internal Auditing Act (FCIAA)(30 ILCS 10/2003(a)(3)). The Chief Internal Auditor is apprised of system development projects via email from the DoIT Project and Portfolio Management (PPM) team and attendance at the bi-weekly Agency Proposal Review Committee meeting. The two-year audit plan for Fiscal Years 2022/2023 and future audit plans for Director approval per FCIAA (30 ILCS 10/2003(a)(1) will include and ensure periodic major system reviews as required.

21. The auditors recommend ISP develop and implement a project management framework and tools and a system development methodology to control and provide oversight of IT projects.

FINDING: *(Lack of Project Management over IT projects)*

Since 2010, the auditors have noted ISP had not implemented a project management framework or tools to ensure the state's and ISP's project goals and objectives were met. In addition, ISP had not developed a system development methodology to ensure development projects were properly controlled and met the project's objectives.

ISP was responsible for the development of three new projects during FY19 and FY20 as well as the development of applications in process at the end of FY18. However, ISP did not utilize a project management framework or system development methodology, which would document planning, documentation, testing, and implementation requirements.

This finding was first noted during the examination of the two years ended June 30, 2010. In the subsequent years, ISP has been unsuccessful in implementing a corrective action plan.

ISP management indicated the weakness was due to insufficient resources in order to implement DoIT's standardized project management process.

RESPONSE:
ISP concurs. ISP fully understands the importance of implementing a project management framework, tools, and system development methodology to ensure controls over IT projects. The Division of Justice Services has implemented the project portfolio management system to assist in rectifying this finding and ensure the Fiscal Control and Internal Auditing Act is adhered to**.**

UPDATED RESPONSE:
Implemented. ISP already has a solid project management framework that was put in place in 2017. The correct information to demonstrate this was provided by DoIT, however, due to a miscommunication the auditors did not fully review it. This project management framework was utilized throughout FY19 and FY20 and is available upon request.

22. The auditors recommend ISP update its procedures to ensure it adequately provides for computer system changes to be initiated, planned, developed, tested, and implemented in a controlled environment. Specifically, the auditors recommend ISP enhance its procedures and requirements for:

- **System testing, test scripts, and approval;**
- **User testing, test scripts, and approval;**
- **Requesting and receiving approval to migrate changes into production;**
- **Post implementation reviews; and**
- **Segregating duties between individuals requesting changes, programming changes, testing changes and moving changes to production. If the Department determines that programmer access to the production environment is necessary in some situations, it should establish and enforce compensating controls to ensure appropriate management oversight and approval of changes.**

ISP should fully implement and consistently follow its change management policies and procedures.

REVIEW: 4516 (Compliance) and 4517 (Management of FOID/Concealed Carry)

FINDING: *(Weakness in Change Management of Computer Systems)*

ISP had established computer systems in order to meet its mission and mandate. ISP processed and maintained critical, confidential and sensitive information on its computer systems.

To establish requirements addressing changes to information technology resources utilized by various bureaus; ISP established a Change Management Procedure, along with a Change Request Form and Instructions. However, the Procedures did not provide sufficient guidance to ensure changes were properly controlled and documented.

During the examination, auditors reviewed a sample of 25 changes, noting:

- 8 (32%) changes were moved to the production environment by the developer. In addition, the documentation supporting 16 of the 17 (94%) remaining change requests did not provide sufficient detail to determine if duties were properly segregated.

- 5 (20%) changes did not provide sufficient detail to determine if testing was performed prior to being moved to production.

- All 25 (100%) changes lacked documentation detailing testing performed and associated approvals.

- All 25 (100%) changes lacked documentation indicating changes were approved before being moved to production.

Additionally, the Change Management Procedure in effect during FY19 required the Office of Inspections and Audit to perform semi-annual reviews of the change management practices and provide management any findings and recommendations resulting from the review; however, ISP indicated such reviews were not performed during FY19. The procedures were updated in FY20 and the requirement was removed. Furthermore, the auditors noted the Change Management policies and procedures did not address post-implementation reviews.

This finding was first noted during the examination of the two years ended June 30, 2012. In the subsequent years, ISP has been unsuccessful in implementing a corrective action plan.

ISP management indicated the weaknesses were due to insufficient staff to separate duties and a sprawling infrastructure that spans several decades' worth of technology. These factors have contributed to personnel filling multiple roles across the change management lifecycle.

RESPONSE:
ISP concurs. ISP fully understands the importance of change management regarding computer systems. The Division of Justice Services will begin taking the necessary steps

to develop an action plan which identifies a solution to rectify this finding and ensure the Fiscal Control and Internal Auditing Act is adhered to.

UPDATED RESPONSE:
Partially Implemented. ISP already has a systems development process in place to ensure that the following are completed for each production implementation:

- System testing, test scripts, and approval;
- User testing, test scripts, and approval;
- Requesting and receiving approval to migrate changes into production;
- Post implementation reviews;

Segregation of duties is not possible in some areas because of limited staffing and the nature of the system implementations. DoIT/ISP will work on establishing the proper controls to ensure that management oversight and approval of changes is completed.

Since a system development process is already in place, ISP will now develop a process for ensuring that implementations completed by the developers are controlled and receive management oversight and approval.

23. The auditors recommend ISP continuously review, update, and approve its disaster recovery plan to ensure it reflects the current environment and contains sufficient detail to support ISP's recovery efforts. Additionally, ISP should perform disaster recovery testing at least annually and maintain sufficient documentation supporting the goals, processes, and results.

FINDING: *(Contingency Planning Weakness)*

ISP carries out its mission through the use of IT. Computer systems that support ISP's mission include, among others: Criminal History System (CHRI), ICASE, ICLEAR, Firearms Owner Identification System (FOID), Concealed Carry, and Violent Crime and Gang Tracking System (VITAL).

In June of 2018, ISP implemented the State of Illinois DoIT and ISP's *Information Systems Resiliency Plan* (Plan). However, the Plan did not go into detail on the recovery of the ISP's applications.

During the current examination, the Plan, dated June 1, 2018, was not revised to reflect the implementation of new systems or modifications to existing systems and therefore did not depict the current environment. As a result, the Plan did not adequately prioritize all critical application systems.

ISP had not conducted disaster recovery testing since September 2014.

ISP management indicated the weakness was due to insufficient resources and lack of travel funds to send personnel offsite to perform the testing.

Failure to adequately develop and test a disaster contingency plan leaves the Department exposed to the possibility of major disruptions of services.

RESPONSE:
ISP concurs. ISP fully understands the importance of adequately planning or testing for the recovery of its computer systems. The Division of Justice Services will begin taking the necessary steps to develop an action plan which identifies a solution to rectify this finding and ensure the Fiscal Control and Internal Auditing Act is adhered to.

UPDATED RESPONSE:
Partially Implemented. ISP will perform a Business Impact Analysis (BIA) for all ISP divisions. Once complete, formal contingency plans will be created as appropriate from BIA's. ISP will also create a policy to document Contingency Plan testing, goals and results.

24. The auditors recommend ISP enter into a detailed agreement with DoIT to ensure prescribed requirements and available security mechanisms are in place to protect the security, processing integrity, availability, and confidentiality of its systems and data.

FINDING: *(Lack of Agreement to Ensure Compliance with IT Security Requirements)*

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

During FY19 and FY20, ISP had not entered into an Intergovernmental Agreement which defined roles and responsibilities of both ISP and DoIT, outlined the transfer of assets and staff, and addressed the security, processing integrity, availability and confidentiality of ISP's systems and data.

ISP has the ultimate responsibility to ensure its critical and confidential systems and data are adequately secured. As such, this responsibility is not limited because the information technology functions were transferred to DoIT.

ISP management indicated an Intergovernmental agreement is not yet finalized due to lack of resources.

RESPONSE:
ISP concurs. ISP fully understands the importance of establishing a detailed agreement with DoIT and has already initiated the process by negotiating and providing a draft agreement to DoIT. Once approved the Division of Justice Services will ensure the

agreement is properly vetted through the proper ISP chains of command, to include the Legal Office and the Director's Office.

UPDATED RESPONSE:
Partially Implemented. The agreement is currently sitting with the DoIT Legal Office for final review and signature. Once approved the Division of Justice Services will ensure the agreement is properly vetted through the proper ISP chains of command, to include the ISP Legal Office and the Director's Office.

25. The auditors recommend ISP ensure required documentation of automobile accidents is submitted to CMS within seven calendar days as required by the Code. The auditors further recommend the Department ensure the SR-1 reports are properly completed and submitted to all required parties in a timely manner.

FINDING: *(Untimely Accident Reporting)*

The Illinois State Police (Department) did not properly submit required documentation following automobile accidents. During testing, auditors noted:

- 86 of 497 (17%) accidents did not have the required Motorist's Report of Illinois Motor Vehicle Accident (SR-1) submitted to CMS within seven calendar days of the accident. The documentation was submitted 1 to 334 days late.

- 32 of 60 (53%) SR-1 were either completed untimely or the date of completion was not able to be determined due to incomplete or missing reports. 14 (23%) of the SR-1 reports were completed one to 50 days late and 18 (30%) reports had no date of completion on the accident reports.

- 3 of 60 (5%) accident files were missing the SR-1 report.

ISP management indicated the untimely and incomplete reports were due to late submissions and entry errors by the vehicle operators.

Failure to timely complete and submit accident reports is noncompliance with the Code and the Illinois Self-Insured Motor Vehicle Liability Plan. The noncompliance also increases the risk of forfeiture of coverage under the Self-Insured Motor Vehicle Liability Plan.

RESPONSE:
As a corrective action to this finding, the ISP Fleet Services Bureau will send out correspondence through all Fleet Officers and consider additional ways to bring awareness to this issue (i.e. Shift Briefing, large distribution email, etc.), while providing further direction for officers to ensure they download and print a copy of the completed SR-1 Report prior to submitting the report online. In addition, the Fleet Section will make efforts to more quickly identify instances where a SR-1 Report is omitted from a crash

packet and will ensure timely follow-up with the reporting officer when any such deficiency is identified.

UPDATED RESPONSE:
Implemented. A Corrective Action Plan has been developed. The Office of the Statewide 9-1-1 Administrator, Fleet Services Bureau will require the SR-1 to be included in all crash packets. Fleet staff will check each crash packet to ensure the SR-1 is included. If not included, Fleet staff will send an email request for a copy of the electronic version. If the electronic version is not available, Fleet Services will request a paper copy be completed. Fleet Services has completed the process to provide access to CMS Auto Liability to Fleet personnel and will continue to train additional staff when necessary to assist with entering crash information into the CMS Auto Liability system to ensure timely entries. In addition, Fleet Services has created a checklist to ensure a complete review by the Fleet staff member reviewing any crash packets submitted in the future.

26. The auditors recommend ISP ensure performance evaluations are conducted annually as required by its Directive and the Illinois Administrative Code.

FINDING: *(Untimely Completion of Performance Evaluations)*

Auditors reviewed 60 employee personnel files and noted 16 (27%) employee files did not contain a completed performance evaluation for one of the fiscal years under examination. 7 (12%) employee files contained one or more annual evaluations that were not completed timely ranging from 16 to 291 days late.

ISP management indicated performance evaluations were not prepared or not prepared timely due to the continuation of reduction in staff, causing supervisors to assume additional duties and responsibilities, leaving less time for administrative functions.

RESPONSE:
ISP concurs with the recommendation and Human Resources recently developed and implemented a method to track and notify supervisors 60 days prior to when evaluations are due.

UPDATED RESPONSE:
Implemented. The code transactions process has fully returned to the ISP from the Public Safety Shared Services Center (3/1/2020). ISP transactions staff has developed a spreadsheet to track evaluation due notices. ISP transactions staff will send notice at least monthly, to ISP division liaisons with notification of performance evaluations due. This notice is sent 60 days prior to the evaluation being due and will be monitored by HR transactions staff for compliance. If the performance evaluation is not received by the due date, HR transactions staff will elevate the non-compliance to the HR Manager for follow-up.

27. The auditors recommend ISP implement controls to ensure all employees are paid in accordance with the Act or ISP written policy. Additionally, the auditors recommend ISP maintain support in the employees' files.

FINDING: *(Inadequate Support for Employee Pay) (did not adequately document support for employee pay)*

Auditors reviewed 60 employee personnel files noting 9 (15%) did not have adequate support for the employees' rate of pay.

- Five were sworn officers, who are paid in accordance with the Sworn Salary Schedule. The salary schedule is based on years of service and Officer Rank; however, the employees' pay did not agree to the schedule based on their current rank and years of service; whereby, the auditors noted differences of pay between $1,512 and $16,440 in excess of the schedule.

- Four were code employees whose rate of pay was not documented in their personnel file.

ISP management indicated the lack of support for the employees' rate of pay was not maintained in the files due to oversight by payroll personnel.

RESPONSE:
ISP concurs with the recommendation and designated salary and temporary assignment pay documentation will be maintained in the payroll files to reflect support for the employees' rate of pay.

UPDATED RESPONSE:
Accepted. The Payroll Department will send a directive to staff that all documentation pertaining to employees pay be placed in the employees file immediately after the processing and closing of the payroll each pay period.

28. The auditors recommend ISP comply with their Directive and the Act to document and ensure employees receive the required training to enable them to perform their specific job duties and protect confidential information.

FINDING: *(Inadequate Controls Over Employee Training)*

Auditors tested training records for 60 employees noting:

- Three (5%) employees failed to complete the Department's Mandatory Annual Training during both FY19 and FY20.

- 33 (55%) employees lacked documentation they were either properly trained to protect the confidentiality of social security numbers, or were not subject to this training requirement.

ISP management indicated the deficient training and the lack of documentation to determine if trainings were required to be completed by certain employees were due to oversight.

RESPONSE:
ISP concurs and will work to ensure all training is completed and proper documentation is maintained.

UPDATED RESPONSE:
Partially Implemented. ISP is currently in the process of transitioning to a new LMS system that will rectify this finding. During this time of transition, in addition to a yearly notification that the Division of the Academy and Training (DAT) currently provides, DAT will send out quarterly email reminders to all sworn and applicable code personnel advising them of mandatory training which must be completed. These notifications will remind supervisors to ensure their personnel are completing required training and include instructions on how everyone can check electronic transcripts for assurance that completed training has been properly recorded in the system. Personnel will further be advised to notify their supervisor if they discover completed training has not been properly recorded in the system. Supervisors will then notify a designated DAT staff member who will address the issue and take the proper corrective action. The accountability expectations and measures will be memorialized in correspondences related to this matter.

29. The auditors recommend ISP ensure the Form I-9 (U.S. Citizenship and Immigration Services I-9 Employment Eligibility Verification) is completed and retained for all employees.

FINDING: *(Noncompliance with Federal Regulations)*

Auditors tested the I-9 forms for 60 employees noting:

- I-9 forms could not be located for 36 (60%) employees.
- One (2%) employee's file contained an incomplete I-9 form; whereby, Section II was missing. In addition, Section I was signed by the employee three days late.

ISP management indicated the missing and incomplete I-9 forms were due to oversight.

RESPONSE:
ISP concurs with the recommendation. Human Resources learned the non-code covered sworn employees certified by the Merit Board did not have the Form I-9 completed as required. While citizenship is verified during the background investigation, the Form I-9 was not being completed. ISP has now provided the Form I-9 to the Academy to be

completed at the time the new cadets enter the Academy, during their orientation. The Form I-9 will be forwarded to Human Resources to be maintained in the officer's personnel file. Human Resources will again remind personnel liaisons that the Form I-9 must be complete on the day they begin employment with the agency and must be maintained in the personnel file.

UPDATED RESPONSE:
Implemented. The Form I-9 will be completed within the first three days and forwarded to the Human Resource Bureau to be maintained in the officer's personnel file.

30. The auditors recommend ISP maintain accurate C-25 forms and deduction authorizations to ensure employee withholdings are accurate.

FINDING: *(Inadequate Controls Over Payroll Files)*

Auditors reviewed employee payroll files for 60 employees noting:

- Four (7%) employees' federal and/or state income taxes were withheld at an incorrect rate based upon the employees' *Federal/Illinois W-4 Employee's Withholding Allowance Certificate* (Form C-25).

- Seven (12%) employees were missing signed deduction authorizations, including:

    - deferred compensation withholding authorizations;
    - union dues withholding authorizations; and,
    - other miscellaneous deduction authorizations.

ISP management indicated the weaknesses were due to not maintaining the current or correct C-25 form and deduction authorizations in the employees' payroll files.

RESPONSE:
ISP concurs with the recommendation and will maintain all deduction authorization cards in the payroll files. The Payroll Unit will also maintain accurate C-25 forms.

UPDATED RESPONSE:
Accepted. The Payroll Department will send a directive to staff that all documentation pertaining to employees C-25 forms and deduction authorizations be processed accurately and placed in the employees file immediately after the processing and closing of the payroll each pay period.

31. The auditors recommend ISP maintain adequate documentation to support the timely cancellation or return of cell phones upon termination.

FINDING: *(Inadequate Control Over Cell Phones)*

During testing, ISP could not provide evidence of when the cellular phones were returned from terminated employees; therefore, the auditors were unable to determine if devices were returned or cancelled in a timely manner.

ISP management indicated a lack of internal communication caused the lack of documentation of returned cellular phones.

RESPONSE:
ISP concurs. ISP fully understands the importance of maintaining documentation cellular phones were returned or cancelled in a timely manner. The Division of Justice Services will begin taking the necessary steps to develop an action plan which identifies a solution to rectify this finding.

UPDATED RESPONSE:
Partially Implemented. The Division of Justice Services will have Telecom personnel review ISP directive ADM-019, Wireless Voice/Data Communications Equipment. If corrections or additions are required, then the directive will be sent for corrections and staffing. Once the policy is approved whether by Telecom personnel or through the staffing process the policy will be disseminated to personnel via the Chiefs of Staff. Meanwhile the Telecom personnel will work with the End User Computing work unit to verify current users and create a tracking mechanism that is utilized to accurately track/record and returned/transferred cell phone.

32. The auditors recommend ISP timely file its Form TA-2's.

FINDING: *(Untimely Filing of the TA-2 Reports-Travel Headquarters)*

During testing, auditors noted two of four (50%) Reports were filed 15 and 17 days late to the Legislative Audit Commission (Commission).

Department management indicated the late filing was due to employee oversight.

RESPONSE:
ISP concurs. ISP fully understands the importance of submitting all required (TA-2) reports in a timely manner. The Division of Justice Services will begin taking the necessary steps to develop an action plan which identifies a solution to rectify this finding.

UPDATED RESPONSE:
Implemented. The Division of Justice Services (DJS) will add bi-annual reminders in the Division's tickler system and Outlook calendar to automatically prompt command to request the required information from Divisions throughout the Department one month prior to submitting to the Legislative Audit Commission. Responses will be collected within two weeks of the request and compiled into the final TA-2 Report. Furthermore, DJS will also enter a bi-annual, reoccurring due date to the Division's Outlook calendar

for the final TA-2 report submission to the Legislative Audit Commission prior to the respective due date outlined in the State Finance Act (30 ILCS 105/12-3).

Emergency Purchases

A chief procurement officer making such emergency purchases is required to file affidavits or statements with the Procurement Policy Board and the Auditor General setting forth the amount expended (or an estimate of the total cost), the name of the contractor involved, and the conditions and circumstances requiring the emergency purchase. The Code also allows for quick purchases. 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.

During FY19 the Department filed two emergency purchase statements totaling $369,281.

- Emergency purchase of Augmented Reality Mapping System at $147,110 which was utilized for night vision or enhanced vision assets. This system assists with the detection of explosives, chemical reactions, humans, or any other item which otherwise could be concealed from view.
- Emergency repair of Emergency Vehicle Operations Center driving track. Cadets use this track to train and prepare to use their assigned vehicles during high speed pursuits. If this repair would not have occurred, the cadet class that began in June 2018, would not have graduated on time. (Check audit report. Last paragraph)

ISP did not have any emergency procurements in FY20.

Emergency Purchases Under the Gubernatorial COVID-19 Disaster Proclamations

The Governor, in response to the COVID-19 pandemic, issued sequential Gubernatorial Disaster Proclamations from March 12, 2020, through June 30, 2020. These proclamations allowed ISP to waive the requirements of the Illinois Procurement Code to the extent the requirement (1) would have, in any way, prevented, hindered, or delayed necessary action to cope with the COVID-19 pandemic and (2) was not required by federal law. The following procurements were all processed under this waiver granted by the Governor.

ISP had three emergency purchases related to the COVID-19 pandemic in FY20 totaling $967.859.

- Emergency purchase of 75,000 face masks and 18,000 bottles of hand sanitizer at the beginning of the pandemic. To acquire this personal protective equipment cost $184,041.
- Emergency purchase of 40,000 N95 masks at a cost of $212,000.

- Emergency purchase of simulators as a result of Governor Pritzker's executive order that limited gatherings to no more than 50 individuals. The purchase of the simulators allowed the cadets to complete their training via distance learning technology at a cost of $571,800.

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 of its officers and employees for whom official headquarters have been designated at any location other than that at which their official duties require them to spend the largest part of their working time. ISP reported that 11 employees spent the majority of their work time in locations other than their official headquarters.