



VIRGINIA STATE POLICE

REPORT ON AUDIT

FOR THE YEARS ENDED

JUNE 30, 2012 AND JUNE 30, 2013

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350



AUDIT SUMMARY

Our audit of the Virginia Department of State Police (State Police) for the fiscal years ended June 30, 2012, and June 30, 2013, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth Accounting and Reporting System and Oracle;
- matters involving internal control and its operation necessary to bring to management's attention; and
- instances of noncompliance with applicable laws and regulations or other matters that are required to be reported.

We have detailed our specific findings related to State Police's Information Technology environment and other matters involving internal controls below in two sections, titled "Risk Alert" and "Audit Findings and Recommendations." State Police has not taken adequate corrective action on prior year audit findings. They continue to have significant deficiencies related to their information technology environment and have made limited progress on improving financial management system controls. Therefore, we have repeated these findings in the sections referenced above. Findings with an asterisk (*) next to the heading indicate that the issue has been addressed in previous audits. Previous audit reports have also made recommendations for process improvements; however, State Police has made limited progress on these due to budgetary constraints. Therefore, these recommendations are not repeated in this audit report.

–TABLE OF CONTENTS–

	<u>Pages</u>
AUDIT SUMMARY	
RISK ALERT	1-2
AUDIT FINDINGS AND RECOMMENDATIONS	3-11
AGENCY HIGHLIGHTS	12-14
INDEPENDENT AUDITOR’S REPORT	15-16
AGENCY RESPONSE	17
AGENCY OFFICIALS	18

RISK ALERT

Effective law enforcement will increasingly require the capability to securely and simultaneously access data from multiple locations. Over the last several years, our audits have identified significant deficiencies related to State Police's information technology (IT) environment, primarily due to resource constraints. The results of our current audit revealed that State Police continues to face substantial challenges in this area. At the forefront of our concerns regarding State Police's IT environment is the lack of progress and stagnation in their negotiations with the Virginia Information Technologies Agency (VITA), regarding whether a portion of their critical infrastructure should be transitioned and managed by VITA. These negotiations have been ongoing since 2006 and have further strained limited State Police IT and management resources. Transformation has not taken place because of legal requirements that mandate that the Superintendent of State Police retain management control of the Virginia Criminal Information Network (VCIN).

Currently, State Police has over 50 existing applications. While State Police has upgraded or retired some of their legacy applications, they still continue to rely on outdated legacy database technologies to support applications that contain sensitive data, including criminal firearms, evidence tracking, human resources, and other information. The age of these technologies and the lack of available vendor and IT resources to support them represent a substantial risk to the agency.

Additionally, State Police has very limited IT resources. Current staffing is not sufficient to manage projects that are underway, maintain existing applications, embark on replacing the remaining legacy systems, or proactively address the information technology demands of the future. Furthermore, State Police does not have the staff, hardware, or software to adequately secure the data that the agency is charged with protecting.

*Develop a Secretary Level Transformation Strategy for State Police and VITA**

State Police and VITA have yet to successfully come to an agreement on if and how the State Police's IT infrastructure should be transformed. Additionally, due to the ineffective collaboration between the two agencies, as well as the complexity of the necessary solution, over eight years and approximately 26 percent of the allocated man-hour transformational budget has been exhausted since the original Comprehensive Infrastructure Agreement (CIA) became effective across the Commonwealth in July 2006.

Currently, Chapters 981 and 1021 of the 2003 Acts of Assembly requires that executive branch agencies transfer management and operation of their IT infrastructure to VITA. However, due to State Police's unique operations, and the kinds of sensitive systems and data that State Police manages, Section 52-15 of the Code of Virginia requires that the Superintendent of State Police retain management control of the VCIN. The principle of the Superintendent maintaining management control was reaffirmed and emphasized by an official Opinion of the Attorney General, 04-085, in 2006. Based on Section 52-15 of the Code of Virginia and the Opinion of the Attorney General, 04-085, in 2013, State Police and VITA signed a Memorandum of Understanding which specifies that a significant portion of the State Police IT environment is out of scope and is not to be managed by, or

transformed to, VITA's service offering. Since the CIA became effective in 2006, State Police has used approximately 4,000 man-hours of their 15,000 hour transformation budget. State Police has spent the majority of these hours on replacing their antiquated local area network hardware to enhance system availability of the VCIN instead of using them to develop an enterprise-wide plan towards transformation. The transformation plans that have been proposed by VITA, according to State Police, have either not met State Police's changing technical requirements, or have resulted in unacceptable cost structures. This has also resulted in State Police proposing an independent enterprise-wide IT solution to the Secretary of Public Safety and Homeland Security. This solution is a proposal to upgrade and manage the State Police's IT environment, including hardware, software, and personnel, independent of VITA.

In its current state, State Police does not have the staff, hardware, or software to adequately secure the data that the agency is charged with protecting. These cumulative weaknesses, exemplified by several of the recommendations identified during our audit, significantly raise the risk that mission critical data will be compromised, incorrect, or unavailable.

State Police and VITA have not been able to agree on even the basic foundations of what an IT transformation solution looks like or whether VITA should transform the State Police. This has resulted from a lack of an established strategy between the Secretary of Public Safety and Homeland Security and the Secretary of Technology.

We recommend that the Secretary of Public Safety and Homeland Security and the Secretary of Technology evaluate all of the options in upgrading the State Police IT environment. This evaluation should include a proposed managed service transformation solution by VITA, as well as solutions where the State Police upgrades and manages its IT environment independently of VITA.

The strategy chosen should be what is best for the Commonwealth as a whole and consider all factors involved. If the Secretaries decide to have VITA transform the State Police IT infrastructure, we recommend that a collaborative cross-agency team be assembled and regularly meet to best implement the related decision. If the Secretaries decide to enable State Police to independently upgrade and manage its own IT environment, the Code of Virginia and the CIA will need to be amended to exclude the State Police, and all related responsibility be reallocated to State Police's management as well as the Secretary of Public Safety and Homeland Security. If the decision is made to exclude State Police from having to transfer management and operations of its IT infrastructure to VITA and the related statute is amended, we recommend that State Police still be held accountable to all other VITA standards.

Regardless of the chosen solution, State Police will need to dedicate significant resources to be able to adequately manage and maintain its IT environment going forward. Additional IT employees are necessary to ensure that the minimum requirements set forth by the Commonwealth's Information Security Standard (Security Standard), SEC 501-08, and State Police's information security program are implemented and continuously enforced for the entire IT environment.

AUDIT FINDINGS AND RECOMMENDATIONS

Information Technology Findings

Improve Motor Vehicle Inspection Program Web Application Security

State Police does not secure the Motor Vehicle Inspection Program (MVIP) web application with some of the minimum security controls required by the Security Standard. MVIP is a web-based system that records information related to the motor vehicle inspection stations and inspectors across the Commonwealth of Virginia and contains sensitive personally identifiable information.

We identified nine control weaknesses that were communicated to management in a separate document marked Freedom of Information Act (FOIA) Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The Security Standard, requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability.

We recommend that State Police dedicate the necessary resources to implement the controls discussed in the communication marked FOIA-Exempt in accordance with the Security Standard and that these controls are implemented in a timely manner.

Remove Excessive Computer Permissions

State Police does not use the principle of least privilege to restrict permissions for end user computers. Allowing excessive computer permissions increases the risk that malware is unintentionally downloaded and installed on employees' computers. Once installed, this malware may propagate throughout State Police's internal computers and can make them unavailable. Certain malware is also designed to collect information processed on infected computers and send it to a server outside the organization; thereby making the confidential data available to unauthorized entities.

We have communicated the details of this finding to management in a separate document marked FOIA-Exempt under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of security controls. We recommend that State Police implement the controls discussed in our recommendation in accordance with the Security Standard.

*Continue to Upgrade Database System Software**

State Police continues to rely on outdated legacy database technologies to support applications that contain sensitive data, including criminal firearms, evidence tracking, human resources, and other information. In its current state, the legacy architecture has not been fully supported by the vendor since 2008, and cannot be kept up-to-date. The last patch was applied over eight years ago, in February 2006. Additionally the entire legacy platform is supported by a single part-time State Police engineer who retired at the end of 2014.

When we first raised this issue with State Police during our audit in April 2010, the State Police presented a five-year plan to migrate its mission critical applications to a new database environment by 2015. Since our last review in 2012, State Police has presented a revised 2016 deadline to complete the project, and has either migrated or decommissioned 17 of the most mission critical of the original 32 applications. State Police currently has active project plans to replace or decommission the remaining administrative systems that contain sensitive information.

It is increasingly risky to keep such antiquated software in use given the limitations on available support. As time passes, fewer experts are available to patch or repair the system when bugs appear, and discontinued vendor product lines cannot depend on support from the vendor in the case of a system failure. Further, it becomes increasingly expensive to maintain software with limited support by the original vendor. Additionally, the system has logical access limitations, including password length and complexity issues, which the State Police must find compensating controls and processes to overcome.

State Police has not been able to retire the entire legacy system to date due to severe resource limitations. Because of these resource constraints, State Police has had to take a phased risk-based approach towards the system's retirement. State Police has either upgraded or retired the legacy applications that are mission critical, and currently are working towards migrating the applications that contain sensitive data, and either migrating or decommissioning the remainder.

We recommend that the State Police dedicate the necessary resources to develop a contingency plan to ensure the continued functioning of the administrative Mapper applications until they can be reasonably migrated or decommissioned by the 2016 project goal. This plan should include immediately securing a technical resource, since the sole part-time supporting Mapper engineer retired as of December 2014. We also recommend that the State Police dedicate the necessary resources to migrate the remaining administrative Mapper applications that contain sensitive data, and work towards either migrating or decommissioning the remaining applications in accordance with the 2016 project goal.

*Continue to Realign Information Security Officer with Industry Best Practices**

State Police continues to silo their Information Security Officers (ISOs) within the Information Technology and the Criminal Justice Information Services (CJIS) Divisions, preventing them from having an enterprise-wide view of the organization and thus limiting the necessary information security oversight and authority to all divisions that handle confidential and mission critical data. Both of the ISOs are reporting to the Information Technology Director and the CJIS Commander, respectively, and currently there is no information security oversight or authority over the Communications Division. This siloed approach has resulted in an inconsistent implementation of the Security Standard, as well as internal Information Security Policies.

The Communications Division of the State Police manages sensitive systems and confidential data, including the maintenance of equipment and hardware for the Statewide Agencies Radio

System (STARS). STARS includes an independent information systems network, mobile data terminals that directly interface with the VCIN, and other sensitive and mission critical systems. Without adequate information security oversight and resources, security controls cannot be effectively managed or consistently implemented across the State Police enterprise. During our review, we identified several technical internal control weaknesses that are symptoms of insufficient or compartmental approaches to information security governance.

- The Motor Vehicle Inspection Program web application is lacking multiple internal controls to be adequately secured, as required by Security Standard and internal information security policy. These weaknesses have been communicated to management in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.
- State Police does not use the principle of least privilege to restrict permissions for end user computers as required by Security Standard and internal information security policy. This weakness has been communicated to management in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.
- State Police is continuing to rely on outdated legacy database technologies to support applications that contain sensitive data. This technology is not vendor-supported, and thus cannot receive security patches as additional bugs and vulnerabilities are identified. Additionally the applications have logical access limitations, including password length and complexity issues, which violates Security Standard Section 8.7 Identification and Authentication, Subsection IA-5.

Not having the information security oversight or the technical information security resources within State Police to implement and enforce the Security Standard and internal security policy consistently across the entire State Police enterprise as well as ensuring the principle of least privilege on sensitive systems increases the risk of a significant data breach. These weaknesses also increase the risk that systems are vulnerable to a denial of service attack making them unavailable for essential business and operational functions.

Each of the above weaknesses are primarily due to State Police being significantly understaffed within its Information Technology and Information Security divisions. During our review we found that State Police does not have the adequate technological and security engineering resources to appropriately implement the controls mandated within the Security Standard and State Police's internal security policy.

We recommend that State Police realign the ISO position in the organization to oversee and enforce its information security policy for the Information Technology, CJIS, and Communications Divisions and report directly to the Deputy Director of the Bureau of Administrative and Support

Services. Additionally, we recommend that State Police dedicate the necessary resources to acquire the technical and information security engineering staff to implement the data controls and safeguards mandated within the Security Standard and State Police's internal security policy.

Other Findings

*Improve Financial Management System Controls**

State Police continues to exhibit weaknesses related to controls over its financial management system (Oracle). As noted in previous audits, the current design of user roles and responsibilities eliminates State Police's ability to have adequate internal control and separation of duties. Our audit found the following deficiencies:

- Various conflicting roles exist that allow employees full access to State Police's general ledger and payables ledger. Individuals with this access have the ability to initiate and approve transactions, update/create vendors, and process payments. Conflicting roles significantly increases the risk of unauthorized and fraudulent transactions in Oracle.
- Information Technology employees continue to have access to multiple financial as well as information security responsibilities. While access to financial responsibilities may be needed temporarily for system administration, access was not removed when those responsibilities were complete. The combination of these roles allows users to enter and approve transactions and delete logs of those transactions from the system.
- Periodic system access reviews are not adequate. Our audit found that an Oracle access review had not been completed since August 2011. We noted that an internal audit of logical access controls completed on April 30, 2013, also determined that system access reviews were not being performed. We found that system owners do not completely understand the functionality of the user responsibilities; therefore, system access reviews are not adequate. Without adequate system access reviews, State Police leaves itself prone to the risk of errors or fraud.
- The individual responsible for producing a report that reviews the initiation and approval of expense and travel vouchers also has the full access to the general ledger and payables ledger. While this report was designed to serve as a compensating control, the effectiveness of the control is reduced because the individual producing the report has the ability to create and approve transactions, as well as, manipulate the results of the report. The lack of adequate segregation of duties during the review process increases the risk that unauthorized transactions could go unnoticed.

- User accounts remained active for an individual who had transferred to another position until after this was brought to management's attention in an internal audit report dated April 30, 2013.

State Police should strengthen its policies and procedures governing system access management controls. System and data owners should determine the necessary user roles for the State Police environment, remove conflicting user roles, and consider the principal of least privilege when assigning responsibilities to its systems. Assigning access based on least privileges will improve the integrity of the data because individuals will only have the access that is necessary for their job responsibilities. Roles and responsibilities within the system should be created in a way that allows the agency to maintain adequate segregation of duties.

State Police should adhere to the Security Standard and deactivate temporary accounts that are no longer required, review accounts and privileges annually, and deactivate accounts of terminated or transferred users. In order to perform a meaningful review of account access, business owners should have a thorough understanding of user roles and responsibilities. State Police should also develop more effective compensating controls if user roles and responsibilities are not assigned based on the principal of least privilege. In addition, State Police should consider completing a conflict matrix to identify conflicting user roles and responsibilities. Although we only tested the financial management system this year, we recommend that State Police consider the above recommendations for all of the agency's applications.

Improve Fixed Asset Internal Controls and Processes

State Police does not have adequate internal controls or processes over their capital assets. Our audit noted the following internal control weaknesses:

- Balances in the Fixed Asset Accounting and Control System and the Commonwealth Accounting and Reporting System are not adequately reconciled. Under State Police's current process, two employees perform a fixed asset reconciliation. One reconciliation does not fulfill CAPP Manual requirements and the other reconciliation, which fulfills CAPP Manual requirements, is not being reviewed. Furthermore, reconciliations are not dated; therefore, there is no audit trail to ensure the timeliness of the reconciliation.
- Assets are entered into four systems: the Fixed Asset Accounting and Control System (FAACS), Material Management System (MAPPER), MCM Motorola Database, and FootPrints. Entering assets into the systems is decentralized to multiple individuals and the systems are not reconciled to ensure completeness.
- Physical inventory of capital assets is not being completed once every two years, even though State Police has a policy that requires inventories to be completed once every two years. The current biennial office inventory is an inventory of office equipment that does not include the agency's capital assets.

- According to State Police's internal policy, Statewide Agencies Radio System (STARS) assets are inventoried every five years or when maintenance is performed on the equipment in the vehicles. During the inventory, MCM Motorola Database information is used and updated, but the results are not compared to information in FAACS.
- Vehicles are visually inspected monthly, but this process does not include a comparison to information in FAACS or MAPPER.
- Land and buildings inventory is verified with the Department of General Services, but there is no comparison to information in FAACS.
- Other capital assets including, but not limited to, computer equipment, x-ray kits and systems, and polygraph equipment are not being inventoried by divisions or area offices.
- FAACS is only updated for the disposal of vehicles. Other items that are disposed of are not removed from FAACS because the Fixed Asset Accountant is not notified of the disposal of these assets.
- The Fixed Asset Accountant only receives documentation of the biennial office inventory. When other inventories are completed, no documentation is provided to the Fixed Asset Accountant.
- The Fixed Asset Accountant does not have a process to periodically reassess asset useful lives.

The Commonwealth Accounting Policies and Procedures Manual (CAPP Manual) requires agencies to establish an adequate system of internal controls over their assets. CAPP Manual, Section 30505 and State Police's internal policies require a physical inventory of capital assets at least once every two years. The CAPP Manual Section 30105 also requires that financial records reflect proper capital asset balances and Section 30605 requires agencies to perform a periodic review and update of asset useful lives to ensure that the useful lives closely mirror the actual lives of the assets. Lack of compliance with this policy can result in a misstatement of assets actually held by the agency and increases the risk of undetected lost or stolen assets.

Managing State Police's assets is decentralized to a number of divisions or area offices; therefore, the responsibility for keeping track of these assets is up to the individual division or area office. State Police's Property and Finance Division includes a fixed asset section; however, they have a limited role in this process. Because of the decentralized nature of the agency, there is a disconnect between the divisions or area offices responsible for assets and the Property and Finance Division, which performs the fixed asset accounting procedures. While State Police has internal policies stating that physical inventories of capital assets must be performed, the policies and current

inventory process focuses on inventories of office equipment and do not adequately address capital asset inventories. Furthermore, under the current structure, State Police has not identified a centralized department or individual to enforce CAPP Manual policies.

State Police should establish internal policies that adhere to CAPP Manual requirements and its own internal policies. Internal policies should be updated to clarify physical inventory requirements and should establish a process for conducting physical inventories of all of State Police's capital assets. State Police should consider designating a centralized department or individual to enforce the CAPP Manual's requirements. The Fixed Asset Accountant should perform duties consistent with CAPP Manual's requirements. Once policies and procedures are updated, fixed asset management training should be provided to all employees responsible for fixed asset management.

Improve Small Purchase Charge Card Controls

State Police is not adequately administering the Small Purchase Charge Card (SPCC) program. Our audit found the following deficiencies:

- One instance in which a cardholder exceeded their single transaction limit with no supporting documentation that the cardholder's limit was increased.
- One instance in which a cardholder exceeded their monthly transaction credit limit with no supporting documentation that the cardholder's limit was increased
- Of the 86 charge cards in fiscal year 2013, 73 had monthly purchasing limits that significantly exceeded the cardholders' actual purchasing needs. These cardholders utilized less than 30 percent of their purchasing authority and in many instances averaged 10 percent or less usage.
- Cardholder supervisors are not adequately reviewing and documenting an annual analysis of cardholder usage and credit limits.
- Eight instances in which cardholder reconciliations were not dated by the reviewing supervisor.

Commonwealth Accounting Policies and Procedures Topic 20355 outlines the policies for administering the SPCC program. Included in those policies is a requirement that program administrators set transaction and credit limits to appropriate levels based on the cardholder's buying needs, ensure that an annual analysis of cardholder's usage and limits is performed and documented, and it requires that supervisors sign and date reconciled statements.

Deficiencies in administering the SPCC program increase State Police's risk of inappropriate or fraudulent activity. State Police should develop internal controls and policies that will ensure compliance with the Commonwealth's policies. State Police should evaluate all cardholder

purchasing activity and adjust the limits as appropriate based on the cardholder's buying needs. Furthermore, State Police should periodically review card usage and cancel those cards that are no longer needed. State Police should also consider revising the SPCC cardholder reconciliation documentation to include the date of supervisory review.

Improve Processes over Work Zone Project Billings

State Police has an Interagency Work Zone Safety Patrol Enforcement Agreement with the Virginia Department of Transportation where State Police officers work paid overtime to patrol and/or monitor traffic within specific construction/maintenance areas. State Police does not adequately track highway construction/maintenance work zone projects to ensure that all projects are being billed. Furthermore, there is no process to ensure that the information obtained from the division offices is accurate and complete. During our audit we found one instance in which four hours of overtime was not billed to the third party. Without a tracking process, or a way to verify information from the division offices, State Police leaves itself prone to errors and risks of billing third parties incorrectly. Specifically, State Police could incur expenses that are not billed to the third party or third parties could be overbilled.

State Police should have internal processes to track the highway construction/maintenance work zone projects to ensure that all projects are being billed appropriately. Furthermore, State Police should develop procedures to verify information from the divisions to ensure that third parties are being billed correctly.

Improve and Adhere to Record Retention Schedules

State Police has inconsistent record retention schedules across divisions and area offices. Our review of the record retention schedules found multiple instances where the same document has different retention periods across divisions and area offices and instances where records were not included consistently in the retention policies for the divisions and area offices. We also found inconsistencies between State Police's record retention policy and their financial procedures manual. Our review found that State Police retains retirement payroll reconciliation reports for only six months, original Vehicle Expense Reports (SP-93) for only 90 days, and the Voyager Receipt for Virginia Department of Transportation Fuel Log (SP-296) for the current year plus an additional year or until audited by the Property and Finance Division.

Updating the record retention schedules is decentralized and the Property and Finance Division is responsible for the financial procedures manual. This decentralization increases the risk that schedules are inconsistent and not updated. The CAPP Manual requires that retirement reconciliation reports be retained for a period of five years or until audited, whichever is later. The CAPP Manual also requires that copies of expense documents be maintained for three years.

State Police should ensure that record retention schedules are consistent with the retention requirements outlined in the CAPP Manual and satisfy the unique functions of the agency. If State Police continues to have multiple record retention schedules, it should ensure consistency across

divisions and areas and with its internal financial procedures manual. State Police should also ensure that record retention schedules are properly updated as changes occur. State Police is scheduled for an upcoming project with the Library of Virginia to update retention policies and procedures related to schedules, series, periods, and acceptable destruction methods. This will provide an opportunity for State Police to update their retention schedules and policies and procedures to ensure that they are consistent with the CAPP Manual. Once finalized, management should consider training staff on the new retention policies and procedures and ensure that all records, physical or electronic, are maintained in accordance with this policy and the CAPP Manual.

AGENCY HIGHLIGHTS

The Department of State Police (State Police) provides statewide law enforcement services to the Commonwealth's citizens and visitors. State Police's administrative headquarters is located in Chesterfield County. There are seven field divisions strategically located throughout the Commonwealth and those divisions are subdivided into 48 area offices. State Police employs over 2,700 employees. State Police provides support to federal, state, and local law enforcement agencies.

The Superintendent is responsible for the overall administration, control and operation of the department. Three bureaus support State Police's mission.

Field Operations

Field Operations is responsible for patrolling over 64,000 miles of state roadways and interstate highways. Personnel provide both traffic enforcement, criminal law enforcement, and aviation support to local agencies. Field Operations is responsible for managing the Motor Vehicle Safety Inspection Program, which enforces motor carrier and commercial vehicle safety regulations, and the Aviation Unit that provides aerial support for law enforcement activities and emergency medical evacuations.

Criminal Investigation

Criminal Investigation investigates all criminal matters mandated by statute and established departmental policy. The Bureau consists of the Criminal Intelligence Division, Support Services Division, Drug Enforcement Section, and General Investigation Section. The Bureau is also responsible for the High Technology Division and the Virginia Fusion Center that receives, analyzes, and disseminates intelligence related to all hazards confronting citizens of the Commonwealth, including terrorism.

Administrative and Support Services

Administrative and Support Services includes the Communications Division, Criminal Justice Information Services Division, Property and Finance, Information Technology Division, Personnel Division, and Training Division.

State Police operates four programs, including capital outlay projects. General fund appropriations primarily fund the agency's operations; however, State Police also collects fees for searches of central criminal records and central registry, firearm transaction program inquiries, state inspection stickers, state and federal asset forfeitures, insurance recoveries and federal grants. Table 1 below shows the budget and expenses for each of State Police's programs.

Table 1

Budgeted and Actual Expenses by Program

	2012			2013		
	Original Budget	Final Budget	Expenses	Original Budget	Final Budget	Expenses
Law Enforcement and Highway Safety Services	\$218,685,769	\$232,617,166	\$219,321,071	\$230,990,533	\$243,843,292	\$233,945,802
Information Technology Systems, Telecommunications and Records Management	53,099,972	48,281,749	41,126,701	52,534,422	47,961,966	46,773,958
Administrative and Support Services	19,935,487	20,217,411	19,910,617	19,168,487	20,841,959	20,728,038
Capital Outlay Projects	540,000	53,424,700	24,476,711	-	30,523,028	6,684,869
Total	<u>\$292,261,228</u>	<u>\$354,541,026</u>	<u>\$304,835,100</u>	<u>\$302,693,442</u>	<u>\$343,170,245</u>	<u>\$308,132,667</u>

Source: Commonwealth Accounting and Reporting System

During fiscal year 2012, State Police's budget increased more than \$62 million. Approximately \$49 million of the increase was the re-appropriation of capital outlay project balances that remained at the end of fiscal year 2011. In addition to capital project balances, State Police also received funds for salaries and benefits, unbudgeted gasoline costs, and highway safety grants. Budget increases also realigned appropriations in the correct programs and fund sources. The majority of the unexpended funds were related to the capital outlay projects that extended to fiscal year 2013.

The fiscal year 2013, Law Enforcement and Highway Safety Services program's original budget increased more than \$12 million. Increases funded retirement and other benefit contribution rate changes, vacant state trooper positions, and positions to monitor sex offenders. During fiscal year 2013, the budget increased more than \$40 million. Approximately \$29 million of the increase was the re-appropriation of capital outlay project balances that remained at the end of fiscal year 2012. Additional budget increases during fiscal year 2013 were non-general fund cash balances used to pay for operating expenses, funds for bonuses, benefit increases, and vehicle equipment purchases.

Table 2 below shows State Police's expenses by type.

Table 2

Expenses by Type

	2012	2013
Personal Services	\$204,642,291	\$217,609,395
Contractual Services	29,536,684	26,494,329
Equipment	25,444,324	29,340,072
Supplies and Materials	18,440,860	16,794,926
Plant and Improvements	15,542,270	5,636,640
Continuous Charges	10,233,800	10,782,182
Transfer Payments	984,871	1,407,809
Property Improvements	<u>10,000</u>	<u>67,315</u>
Total	<u>\$304,835,100</u>	<u>\$308,132,667</u>

Source: Commonwealth Accounting and Reporting System

Total expenses increased by approximately \$3.2 million or one percent in fiscal year 2013. Personal services expenses made up 67 and 71 percent of State Police's expenses in fiscal years 2012 and 2013, respectively. Personal service expenses primarily consist of salaries, retirement contributions, and health insurance premiums. In fiscal year 2012, State Police continued the construction of the Driving Training Complex in Nottoway County, as a result, plant and improvement expenses decreased 63 percent, almost \$10 million in fiscal year 2013. The Driver Training Complex became fully operational in July 2013. Design and construction continues on a firing range complex and a new Bureau of Criminal Investigation office that will replace a leased facility.



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

February 4, 2015

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable John C. Watkins
Chairman, Joint Legislative Audit
and Review Commission

We have audited the financial records and operations of the **Virginia Department of State Police (State Police)** for the years ended June 30, 2012, and June 30, 2013. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Objectives

Our audit's primary objectives were to evaluate the accuracy of recorded financial transactions in the Commonwealth Accounting and Reporting System and Oracle, review the adequacy of State Police's internal controls, test compliance with applicable laws, regulations, contracts, and grant agreements, and review corrective actions of audit findings from prior year reports.

Audit Scope and Methodology

State Police management has responsibility for establishing and maintaining internal control and complying with applicable laws and regulations. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws, regulations, contracts, and grant agreements.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered significance and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following significant cycles, classes of transactions, and account balances.

- National Motor Carrier Safety Program Compliance
- Contractual services expenses
- Payroll expenses
- Small purchase charge card expenses
- Inventory and Fixed Asset Management

Information System Security System Access Controls

We performed audit tests to determine whether the State Police's controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements. Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of the State Police's operations. We tested transactions and performed analytical procedures, including budgetary and trend analyses.

Conclusions

We found that the State Police properly stated, in all material respects, the amounts recorded and reported in the Commonwealth Accounting and Reporting System and Oracle. State Police records its financial transactions on the cash basis of accounting, which is a comprehensive basis of accounting other than accounting principles generally accepted in the United States of America. The financial information presented in this report came directly from the Commonwealth Accounting and Reporting System.

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts and grant agreements that require management's attention and corrective action. These matters are described in the sections entitled "Risk Alert" and "Audit Findings and Recommendations."

State Police has not taken adequate corrective action on prior year findings. The prior year finding entitled "Upgrade Unreliable and Unsupported Infrastructure Devices" was partially repeated this year in the section titled "Risk Alert." Further, State Police has made limited progress on other findings included in the prior year report. Therefore, we have repeated these findings in the section titled "Audit Findings and Recommendations." Findings with an asterisk (*) next to the heading indicate that the issue has been addressed in previous audits. In addition, while previous audit reports have made recommendations for process improvements, State Police has only made limited progress on these recommendations due to budgetary constraints. Therefore, these recommendations are not repeated in this audit report.

Exit Conference and Report Distribution

We discussed this report with management on March 13, 2015. Management's response to the findings identified in our audit is included in the section titled "Agency Response." We did not audit management's response and, accordingly, we express no opinion on it.

This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

AUDITOR OF PUBLIC ACCOUNTS

LJH:alh



COMMONWEALTH of VIRGINIA
DEPARTMENT of STATE POLICE

Colonel W. S. (Steve) Flaherty
Superintendent

(804) 674-2000

Lt. Colonel Robert B. Northern
Deputy Superintendent

February 19, 2015

Martha S. Mavredes, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Mavredes:

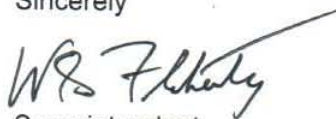
We appreciate the opportunity to review the Department of State Police's (Department) Fiscal Years 2012-2013 Audit Report. Thank you for the recommendations on our financial accounting and control operations as well as the professionalism of your staff throughout engagement. We have responded to the specific items mentioned under separate detailed correspondence throughout the course of your review.

With regard to the four Information Technology Findings: The Department is actively pursuing opportunities to comply with the Commonwealth's Information Security Standards SEC501-08 (Security Standards). We generally concur with your recommendations; the exception is transferring supervisory responsibility of the Department's *Information Security Officer*.

With regard to the five Other Findings: Again, the Department is most interested in fully complying with the Security Standards. We generally concur with your recommendations; the exception is arbitrary adjustment of credit limits related Improving *Small Purchase Card Controls* (SPCC). The Department is an emergency services organization whose employees may be required to perform "no notice" duties, to include procurement functions in times of crisis. Our mindset is the SPCC credit limits are closely matched to possible requirements of the employee's position and function.

We give your comments the highest level of consideration as we continue to improve our practices and compliance with the Commonwealth's Fiscal Policies, Regulations, Laws, and Security Standards. We are making satisfactory progress, and remain committed to focusing staff and resources prudently as we execute the Department's Public Safety mission.

Sincerely



Superintendent

WSF/CCW/jml

C: The Honorable Brian J. Moran
Secretary of Public Safety and Homeland Security

DEPARTMENT OF STATE POLICE

Brian J. Moran
Secretary of Public Safety and Homeland Security

Colonel W. Steven Flaherty
Superintendent

Lieutenant Colonel Robert G. Kemmler
Director of Bureau of Administrative and Support Services