

Audit Report

**Department of Budget and Management
Office of the Secretary and Other Units**

October 2019



OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

Joint Audit and Evaluation Committee

Senator Craig J. Zucker (Senate Chair)	Delegate Shelly L. Hettleman (House Chair)
Senator Adelaide C. Eckardt	Delegate Steven J. Arentz
Senator George C. Edwards	Delegate Andrew P. Cassilly
Senator Guy J. Guzzone	Delegate Mark S. Chang
Senator Katie Fry Hester	Delegate Keith E. Haynes
Senator Cheryl C. Kagan	Delegate Michael A. Jackson
Senator Benjamin F. Kramer	Delegate David Moon
Senator Cory V. McCray	Delegate April R. Rose
Senator Douglas J.J. Peters	Delegate Geraldine Valentino-Smith
Senator Justin D. Ready	Delegate Karen Lewis Young

To Obtain Further Information

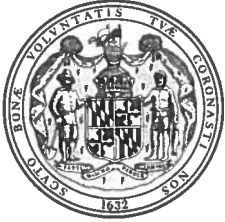
Office of Legislative Audits
301 West Preston Street, Room 1202
Baltimore, Maryland 21201
Phone: 410-946-5900 · 301-970-5900 · 1-877-486-9964 (Toll Free in Maryland)
Maryland Relay: 711
TTY: 410-946-5401 · 301-970-5401
E-mail: OLAWebmaster@ola.state.md.us
Website: www.ola.state.md.us

To Report Fraud

The Office of Legislative Audits operates a Fraud Hotline to report fraud, waste, or abuse involving State of Maryland government resources. Reports of fraud, waste, or abuse may be communicated anonymously by a toll-free call to 1-877-FRAUD-11, by mail to the Fraud Hotline, c/o Office of Legislative Audits, or through the Office's website.

Nondiscrimination Statement

The Department of Legislative Services does not discriminate on the basis of age, ancestry, color, creed, marital status, national origin, race, religion, gender, gender identity, sexual orientation, or disability in the admission or access to its programs, services, or activities. The Department's Information Officer has been designated to coordinate compliance with the nondiscrimination requirements contained in Section 35.107 of the United States Department of Justice Regulations. Requests for assistance should be directed to the Information Officer at 410-946-5400 or 410-970-5400.



DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Victoria L. Gruber
Executive Director

Gregory A. Hook, CPA
Legislative Auditor

October 29, 2019

Senator Craig J. Zucker, Senate Chair, Joint Audit and Evaluation Committee
Delegate Shelly L. Hettleman, House Chair, Joint Audit and Evaluation Committee
Members of Joint Audit and Evaluation Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the Department of Budget and Management's (DBM) Office of the Secretary, which includes the Central Collection Unit (CCU), and certain other units of DBM for the period beginning July 15, 2014 and ending October 19, 2017. DBM assists the Governor in the preparation and monitoring of the State's annual operating and capital budgets. CCU is responsible for collecting delinquent debts owed to the State, except those excluded by law (such as taxes and child support) and its collections totaled \$131.2 million during fiscal year 2018.

Our audit disclosed several deficiencies relating to procedures and controls at CCU. Specifically, we found that numerous employees had unnecessary access to CCU's debt collection and cash register systems or access that resulted in inadequate segregation of duties. We also found certain deficiencies within the debt collection system that resulted in CCU's failure to assess required collection fees of at least \$17.8 million and the rejection of certain valid debts submitted by State agencies for collection. Furthermore, CCU did not periodically review existing deviations from State regulations granted to State agencies regarding the submission of delinquent accounts to CCU to ensure that the deviations were still warranted. At the time of our review, there were 117 active deviations held by 35 State agencies for various types of accounts, dating back to 1979.

Regarding CCU's collection efforts, we noted that potential wage garnishments were not always pursued as a means to collect outstanding debts—a condition that we have commented upon since 1997—and there was a lack of controls over the abatement of accounts which generally results in the cessation of collection

efforts. During the audit period, CCU abated 24,000 accounts valued at \$39.1 million. We also found that certain CCU system omissions and errors resulted in the exclusion of certain significant debts from the State Tax Refund Intercept Program (TRIP), which is administered by the Comptroller of Maryland and is one of CCU's most effective collection methods. For example, our test of 30 debtor accounts totaling \$74.7 million determined that \$73.1 million from 28 accounts had not been submitted for TRIP. Finally, CCU collected TRIP revenues totaling \$11.6 million for a private entity after the law authorizing these collections for this entity was repealed in 2005.

Our audit also disclosed that the ability to view personally identifiable information (PII), such as names and related social security numbers, stored within CCU's debt collection system was not adequately restricted. Our analysis as of January 2018 identified approximately 5.8 million debtor accounts (which may include multiple accounts for the same debtor) in which PII was visible to system users, including CCU employees, State agency employees, and CCU's external collection firm.

Similarly, vendor PII (including social security numbers for individual vendors) was not restricted in the State's Financial Management Information System (FMIS). PII for 398,000 Statewide vendors was displayed in plain text and was visible to 5,204 State employees. It should be noted that responsibility for restricting access to PII in FMIS is shared by DBM, the Comptroller of Maryland, and the State's Department of Information Technology.

Also, with regard to systems security and control, DBM did not have a complete disaster recovery plan for recovering computer operations, and we noted network security risks as a result of certain access granted to information technology contractors. We also noted certain deficiencies regarding DBM's oversight of interagency agreements between State agencies and local community colleges, as well as its monitoring of the State's motor vehicle fleet.

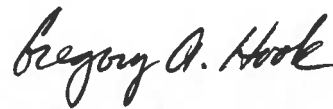
Finally, our audit included a review to determine the status of the two findings contained in our preceding audit report. We determined that DBM did not satisfactorily address these findings; therefore, both findings are repeated in this report.

DBM's response to this audit is included as an appendix to this report. In accordance with State law, we have reviewed the response and, while DBM generally agrees with the recommendations in this report, we identified certain instances in which statements in the response conflict with or disagree with the report findings. In each instance, we reviewed and reassessed our audit

documentation, and reaffirmed the validity of our finding. In accordance with generally accepted government auditing standards, we have included “auditor comments” within DBM’s response to explain our position. We will advise the Joint Audit and Evaluation Committee of any outstanding issues that we cannot resolve with DBM.

We wish to acknowledge the cooperation extended to us during the audit by DBM and its willingness to address the audit issues and implement appropriate corrective actions.

Respectfully submitted,

A handwritten signature in black ink that reads "Gregory A. Hook". The signature is written in a cursive style with a large, prominent initial 'G'.

Gregory A. Hook, CPA
Legislative Auditor

Table of Contents

Background Information	6
Agency Responsibilities	6
Central Collection Unit Operations	6
Debt Manager System	8
Status of Findings From Preceding Audit Report	8
Findings and Recommendations	9
Central Collection Unit (CCU)	
System Controls	
Finding 1 – CCU did not perform a periodic review of user access to its debt collection and cash register systems, and did not adequately restrict access to those systems.	10
Finding 2 – The Department of Budget and Management (DBM) did not ensure that access to personally identifiable information (PII) stored in its debt collection system, such as names and related social security numbers, was restricted. We noted that PII for approximately 5.8 million accounts was not adequately restricted.	11
Finding 3 – Deficiencies in CCU’s debt collection system resulted in the failure to assess collection fees of at least \$17.8 million and the improper rejection of certain valid debts.	12
Collection Efforts	
* Finding 4 – CCU did not adequately pursue potential wage garnishments from debtors.	13
Finding 5 – CCU did not have adequate controls over the abatement of accounts, which totaled approximately \$39.1 million during our audit period.	15
Finding 6 – CCU did not perform a periodic review of existing deviations from State regulations previously granted to State agencies regarding the submission of delinquent accounts to CCU.	16
* Denotes item repeated in full or part from preceding audit report	

State Tax Refund Intercept Program (TRIP)		
	Finding 7 – Certain significant debt amounts were excluded from TRIP because of CCU system omissions and errors.	18
	Finding 8 – CCU collected TRIP revenues totaling \$11.6 million for a private entity after the law authorizing these collections to be handled by CCU was repealed in 2005.	20
Financial Management Information System		
	Finding 9 – Vendor PII was not adequately restricted in the Financial Management Information System and was visible to 5,204 employees Statewide.	21
Information Systems Security and Control		
*	Finding 10 – Sensitive PII maintained by CCU was stored without adequate safeguards.	23
	Finding 11 – DBM did not have a complete information technology disaster recovery plan for recovering computer operations.	24
	Finding 12 – Network security risks existed from information technology contractors having unnecessary network-level access to the DBM network and the unnecessary assignment of administrative rights on numerous workstations.	24
Interagency Agreements		
	Finding 13 – DBM did not require State agencies to report interagency agreements with local community colleges.	26
Motor Vehicle Fleet		
	Finding 14 – DBM lacked documented justification for excluding certain vehicle types from its annual review of vehicle usage. In addition, DBM’s cost assessments of the need for an agency to retain vehicles when they were not driven the minimum annual miles without adequate justification were not properly calculated.	27
Audit Scope, Objectives, and Methodology		29
Agency Response		Appendix

* Denotes item repeated in full or part from preceding audit report

Background Information

Agency Responsibilities

The Department of Budget and Management (DBM) is primarily responsible for assisting the Governor in the preparation and monitoring of the State's annual operating and capital budgets. The Office of the Secretary coordinates the functions of DBM's divisions which include, in addition to the budget process, overseeing certain Statewide procurements and providing fiscal and personnel services to State agencies. This audit report includes the operations of the following units:

- Office of the Secretary, which includes the Central Collection Unit (CCU)
- Office of Budget Analysis
- Office of Capital Budgeting

DBM's Office of Personnel Services and Benefits (OPSB), which directs the State's personnel policies and administers the health care benefits programs for State employees and retirees, is audited and reported upon separately.

According to the State's records, DBM's expenditures, excluding OPSB, totaled approximately \$24.5 million during fiscal year 2018, of which \$15.2 million related to the operations of CCU.

Central Collection Unit Operations

CCU's primary responsibility is to collect delinquent debts owed to the State, except those excluded by law (such as taxes and child support). Collections on debt, less CCU's assessed collection fees, are generally paid either to the State Treasury or to the unit of State government where the debt originated.

State law authorizes CCU to assess and collect for each debt a fee sufficient to cover all collection and administrative costs, not to exceed 20 percent of the outstanding principal and interest. CCU's collection fee is currently established at 17 percent, which is added to the original amount of the debt. Collection fees received are deposited into the Central Collection Fund, a continuing, non-lapsing special fund used to pay CCU's operating expenses. According to State law, any balance in the Fund at the end of the fiscal year exceeding 15 percent of CCU's actual operating expenses for that year is required to be reverted to the State's General Fund.

During fiscal years 2015 to 2017, according to State records, CCU reverted approximately \$10.4 million to the State’s General Fund. This reversion amount represents a decrease of approximately \$7.1 million from the amount reverted during fiscal years 2012 to 2014, as noted in our preceding audit report, and was the result of increased CCU operating expenses, and ongoing expenses related to its information technology modernization project (Debt Manager System - discussed below). According to CCU’s records, as of July 1, 2017, the balance in the Fund totaled approximately \$2.9 million.

CCU’s operations include its Baltimore headquarters office, and five satellite offices established at select Motor Vehicle Administration (MVA) locations to assist primarily in the collection of uninsured motorist penalty fees assessed by MVA.

According to its records, the balance of outstanding debt referred to CCU was approximately \$2.6 billion as of June 30, 2018, as noted in Table 1 below. A significant portion of the outstanding debt was referred by the Department of Transportation (primarily, the MVA and the Maryland Transportation Authority). The number of debt accounts increased significantly during our audit period because, in fiscal year 2016, the Authority began transferring its delinquent toll violation accounts to CCU rather than collecting them in-house.

Fiscal Year	Outstanding Debts (at June 30)		
	<u>Accounts</u>	<u>Balance</u>	<u>Collections*</u>
2015	2,355,118	\$2,040,385,146	\$140,388,224
2016	4,111,660	\$2,253,677,876	\$134,957,660
2017	6,375,405	\$2,454,518,705	\$157,678,861
2018	8,191,315	\$2,634,687,680	\$131,225,902

*Collections are net of collection fees and account adjustments (such as refunds), and include amounts collected through the State’s Tax Refund Intercept Program.
Source: CCU records

Debt Manager System

In fiscal year 2009, with the assistance of the State Department of Information Technology, CCU initiated an information technology modernization project to establish a new collection system called Debt Manager. Debt Manager is intended to improve CCU's automated collection processes through replacement of peripheral systems, automation of manual business processes, and implementation of system-to-system interfaces with various State agencies. CCU used Debt Manager for limited processing of debtor information during 2017, but the system was not fully implemented until July 2018, subsequent to our audit period.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the two findings contained in our preceding audit report dated April 17, 2015. As disclosed in Table 2, we determined that DBM did not satisfactorily address these findings, both of which are repeated in this report.

Preceding Finding	Finding Description	Implementation Status
Finding 1	CCU did not adequately pursue potential wage garnishments from debtors.	Repeated (Current Finding 4)
Finding 2	Controls over system access and sensitive personally identifiable information were not sufficient.	Repeated (Current Finding 10)

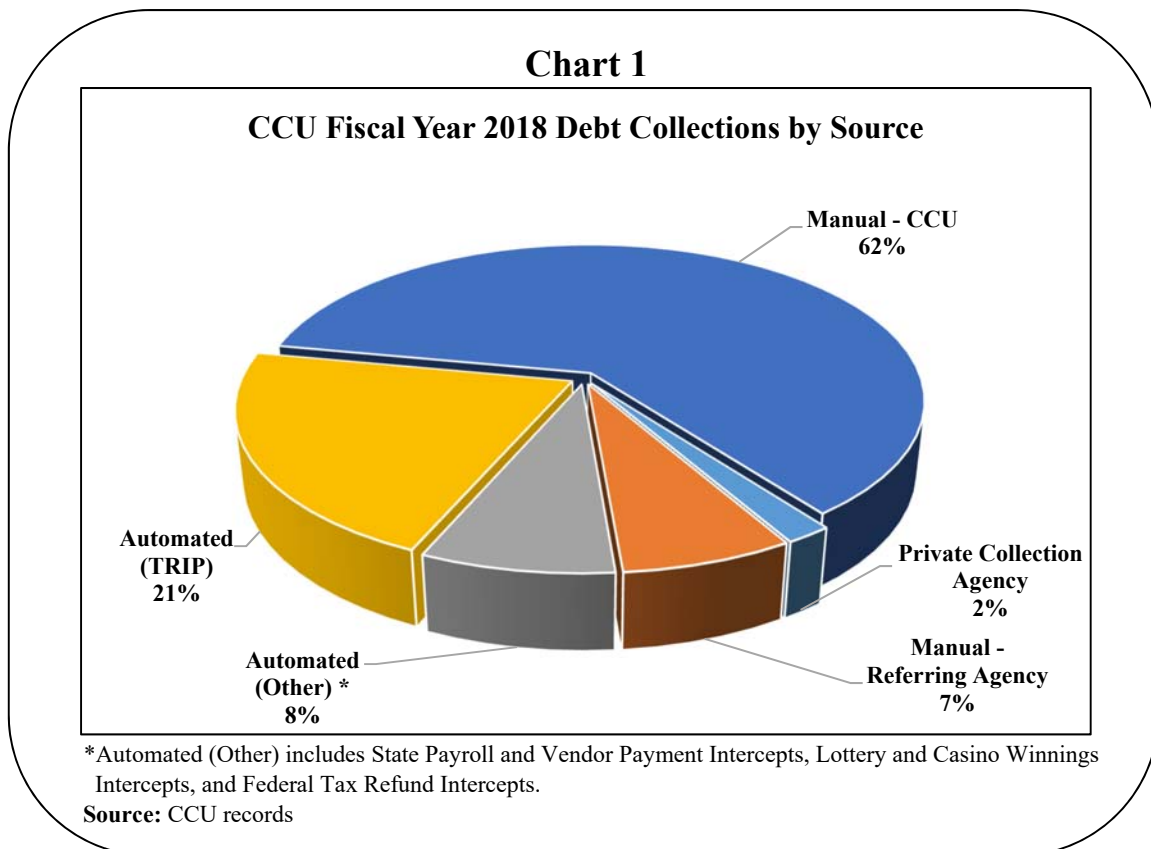
Findings and Recommendations

Central Collection Unit

Background

The Department of Budget and Management’s (DBM) – Central Collection Unit (CCU) uses a variety of methods and resources to facilitate the collection of delinquent accounts, including automated and manual processes, as well as the use of a private collection agency. Automated collection efforts include the use of the State’s Tax Refund Intercept Program (TRIP), which captures debtor State tax refunds, and other automated intercept programs. CCU agents will pursue voluntary payments (such as payment plan agreements) via phone and written correspondence and will also forward selected accounts to the CCU Legal Measures Unit for proactive non-voluntary collection actions, such as wage garnishments and property liens. CCU processes debtor payments received via the internet, mail, or in person as a walk-in, or from the referring agency where the debt originated.

Chart 1 below depicts the details of fiscal year 2018 collections totaling approximately \$131.2 million, by collection method, according to CCU records.



System Controls

Finding 1

CCU did not perform a periodic review of user access to its debt collection and cash register systems, and did not adequately restrict access to those systems.

Analysis

CCU did not perform periodic reviews of employee access to its legacy debt collection system, which was in use during our audit, and to its cash register system to ensure that access to process transactions on these critical systems was properly restricted. Our review disclosed that numerous employees had access to these systems which was either unnecessary for their job duties or incompatible since the access resulted in inadequate segregation of critical duties.

Consequently, unauthorized transactions could be processed on the systems without detection. According to CCU's records, during fiscal years 2015 through 2017, CCU recorded and processed \$433.0 million in transactions to debtor accounts through the debt collection system. In addition, \$93.4 million in debt collections were processed through the cash register system.

Our review of 123 active debt collection system users at CCU headquarters, as of December 6, 2017, identified 51 users with critical access that was either unnecessary or inappropriate. For example, of the 21 employees who had the ability to change a debtor account to inactive, thereby stopping all collection action for that account, only 2 required the access for their job duties. In addition, our review of the 37 active cash register system users at CCU headquarters as of March 7, 2018, disclosed 20 users who had access to process cash receipts and to void the same transactions. CCU headquarters processed voids totaling approximately \$230,000 during our audit period, of which \$14,000 were voided by the user who created the transaction.

Furthermore, we identified nine users with inappropriate access in both the debt collection system and cash register system. Together, such accesses are incompatible when granted to an individual, as it allows a user to process and subsequently void a payment transaction on the cash register system and change the debtor account on the debt system to inactive, concealing any misappropriation or irregularity.

The State of Maryland *Information Technology Security Manual* requires agencies to enforce access controls that provide for separation of duties, and to monitor the controls over their information systems, including periodic reviews of user accounts and access for propriety.

Recommendation 1

We recommend that DBM

- a. perform a documented periodic review of user access to its debt collection system and its cash register system to ensure that access capabilities for critical functions are restricted to employees who require such capabilities to perform their assigned job duties and in a manner that ensures a proper segregation of duties, and**
- b. eliminate the identified unnecessary and incompatible access capabilities.**

Finding 2

DBM did not ensure that access to personally identifiable information (PII) stored in its debt collection system, such as names and related social security numbers, was restricted. We noted that PII for approximately 5.8 million accounts was not adequately restricted.

Analysis

DBM did not adequately restrict user access to PII, such as names and social security numbers (SSN), which is stored in its debt collection system. (See also Finding 10 for comments on CCU's method of storing PII.) In addition to the CCU employees with access to the debt collection system mentioned in Finding 1, an application, through DBM's website, allowed other authorized users with an assigned password to view (not modify) and produce reports containing real-time account information including PII. Although not all accounts in the system included SSNs, our analysis of the CCU debtor account file as of January 2018 identified approximately 5.8 million active accounts¹ with names and SSNs shown in plain text (that is, were not masked or truncated). We also found numerous instances of SSNs unexpectedly appearing in non-SSN fields within the system as a result of the format an agency may have used when submitting the data to CCU.

As of April 2018, there were 2,884 active application user accounts with access to PII in the debt collection system. These users included CCU employees, employees of State agencies using the debt collection system, and employees of CCU's external collection firm. Based on our understanding of the system and its use, in our opinion, very few of these users actually needed access to this PII to perform their job duties. In addition, our review disclosed that 1,303 of the 2,884 user accounts with access to this sensitive information had not been used since they were created, including 974 accounts that were created up to six years prior

¹ A specific debtor might have multiple accounts active at one time. Consequently, although we were not readily able to quantify the number of unique debtors with PII on the system, it should be significantly fewer than 5.8 million.

to our review. Finally, while the majority of user accounts were restricted to debtor accounts applicable to a specific agency, we noted 26 users with Statewide access to all accounts, 18 of which were employed by the external collection firm.

State law defines any record containing an individual's name combined with a SSN as PII. The State of Maryland *Information Technology Security Manual* requires that agencies ensure that access to confidential information is strictly controlled and audited and that it supports the concept of "least privilege" allowing only authorized access to accomplish assigned tasks.

Recommendation 2

We recommend that DBM

- a. to the extent practicable, limit view access to PII, consistent with user needs, by removing or otherwise masking PII data, including SSNs, within the debt collection system;**
- b. search the system and remove SSNs from non-SSN data fields, as feasible, and establish controls to prevent future posting of SSNs to improper data fields; and**
- c. in conjunction with user agencies, remove the unnecessary user access to PII through DBM's website application, including accounts with no user activity.**

Finding 3

Deficiencies in CCU's debt collection system resulted in the failure to assess collection fees of at least \$17.8 million and the improper rejection of certain valid debts.

Analysis

CCU's debt collection system did not apply the required 17 percent collection fee to certain amounts due, resulting in the failure to assess collection fees. For outstanding accounts as of January 2018, we determined that at least \$17.8 million in collection fees were not assessed. In addition, the system improperly rejected certain legitimate debts submitted by State agencies for collection. Consequently, these amounts were not subject to CCU's collection procedures. According to DBM, these conditions occurred because of system programming deficiencies related to the interest component of the debts, which likely have been ongoing since 2002.

The collection fee omission was attributable to instances in which certain agencies, when submitting accounts for collection, reported the interest portion of the debt separately from the principal portion (rather than together as one

amount). For debts submitted in this manner, the system did not apply the 17 percent collection fee to the separately reported interest portion of the debt. Based on debts outstanding, as reflected in the debt collection system as of January 2018, we determined that \$104.5 million in interest charges relating to these accounts was excluded when the 17 percent collection fee was applied, resulting in the failure to assess and collect fees totaling \$17.8 million. Our determination excluded collection fees that were not assessed on accounts collected prior to January 2018.

In addition, the debt collection system did not recognize the separately reported interest on submitted accounts when assessing whether the total amount due from a debtor (principal and accumulated interest) exceeded the \$30 threshold requiring State agencies to submit accounts to CCU. The system was programmed to examine the balance of the principal field only, without considering the combined principal and interest balance. Consequently, the submission was rejected if the principal balance was less than \$30, even if the total debt exceeded \$30. We were unable to readily determine the amount of debt improperly rejected by the system under this condition.

State regulations require CCU to charge the debtor a collection fee (currently 17 percent of the total debt). The regulations also state that delinquent accounts with a balance due (principal and interest) of \$30 or greater can be transferred to CCU for collection. DBM has advised us that implementation of its new Debt Manager system will address these conditions.

Recommendation 3

We recommend that DBM correct these programming deficiencies and ensure that its collection fee is applied to all amounts due, and that the determination as to whether a debt meets the dollar threshold for CCU acceptance from an agency is based on the total amount due.

Collection Efforts

Finding 4

CCU did not adequately pursue potential wage garnishments from debtors.

Analysis

CCU did not always pursue wage garnishments from debtors when viable wages were identified through quarterly computer matches of its accounts with State wage data from the Maryland Department of Labor (MDL). CCU's debt collection policies provide that CCU will generally consider pursuing wage

garnishments on accounts with debts greater than \$750 and for which wages are currently available to attach.

The quarterly wage match queries for the second quarter of 2017 identified approximately 70,500 debtor accounts (each greater than \$750) with balances totaling \$213 million and MDL-reported quarterly wages earned of \$665.3 million, which could have been subject to garnishment based on CCU policies. In January 2018, we reviewed the CCU accounts for 20 debtors appearing on this match, with debts as of September 2017 totaling approximately \$3.9 million and quarterly wages of \$1.3 million. Our review disclosed that 7 debtors had not made any payments, and the remaining 13 had not made payments for periods ranging from 3 to 177 months prior.

We noted a general lack of adequate subsequent collection activity after the wage match in question. Specifically, we noted that CCU's Legal Measures Unit was in the process of establishing a wage garnishment for only 1 of these 20 debtors. The debtor was referred to the Unit in December 2017 and the wage garnishment was still being processed as of February 2018. While 3 debtors tested subsequently paid their debts in full totaling \$8,000, the remaining 16 debtors, with quarterly wages totaling approximately \$798,800, had not made any debt payments nor been referred to the Legal Measures Unit to initiate wage garnishments. Furthermore, for these 16 debtors, there was no documentation as to why these debtors were not referred to the Unit.

We have commented on similar conditions regarding wage garnishments in our seven preceding audit reports dating back to 1997. CCU management advised us that executing a wage garnishment is an expensive and lengthy process, and that it may take months or even years to obtain the required judgments and orders from the courts. CCU further advised us that it uses its limited resources to pursue debts that are likely to produce the best recoveries; however, its policies did not address prioritizing accounts for potential wage garnishments once viable accounts are identified. In our preceding audit report, we noted that CCU management advised that it was in the process of developing such a policy; however, as of February 2018 no such policy had been established.

Recommendation 4

We recommend that DBM

- a. take appropriate action to pursue potential wage garnishments from debtors in a timely manner and document its efforts (repeat), and**
- b. establish guidance on prioritizing accounts for potential wage garnishments within CCU's debt collection policies.**

Finding 5

CCU did not have adequate controls over the abatement of accounts, which totaled approximately \$39.1 million during our audit period.

Analysis

CCU had not established adequate controls over the abatement (generally, the cessation of collection efforts) of accounts. Specifically, there was no procedure in place to ensure that only authorized accounts were moved from an active status to an abated status in the debt collection system. During our audit period, CCU abated approximately 24,000 accounts valued at \$39.1 million.

Accounts that are deemed uncollectible, for example, because of the debtor's death or bankruptcy, are manually compiled on a form, along with supporting documentation, for submission to CCU's abatement committee for review. CCU policy requires approval from its abatement committee for changes in account status from active to abated. There are two levels of abated status: The first level provides for a continuation of only certain passive collection efforts, such as tax refund intercepts, and the second level removes the account from all collection efforts.

Although CCU had previously used a system-generated report to perform an independent review of changes from an active account status to an abated status, as of April 2018, this review had not been performed since at least July 2016. This independent review was necessary because the employee who prepared the manual abatement form also forwarded the committee-approved abatement account list to a second employee to update the account status in the system, and had access to update the account status on the system directly. Accordingly, there was no assurance that all recorded changes to account status were actually approved by the committee.

Our test of 20 accounts abated during our audit period, totaling approximately \$8 million, identified 4 accounts totaling \$349,000 for which there was no evidence of abatement committee approval. Specifically, CCU advised that one account, for \$27,000, was accidentally added to the list of abated accounts after committee approval. The other 3 accounts, totaling approximately \$322,000, were inappropriately changed from the first to the second level of abatement status, removing the accounts from all collection efforts. These 3 account changes were processed by the employee who initially prepared the abatement form, and the system changes were not subject to independent review.

Recommendation 5

We recommend that DBM

- a. establish adequate controls over the abatement process by having an independent employee use system-generated reports to verify that all changes in account status to any type abatement status have been properly authorized;**
- b. investigate and resolve the aforementioned account for which there was no approval from the abatement committee, as well as the three accounts for which there was no approval for a change in abatement status; and**
- c. perform a review of all account changes to abatement status that were made since July 2016 to determine if there are additional unapproved changes in status and take appropriate action.**

Finding 6

CCU did not perform a periodic review of existing deviations from State regulations previously granted to State agencies regarding the submission of delinquent accounts to CCU.

Analysis

CCU lacked an adequate process for monitoring deviations from compliance with State regulations regarding the submission of delinquent accounts to CCU that had been granted to State agencies. At the time of our review, approximately 100 State agencies² were using CCU services, and there were 117 active deviations held by 35 of these State agencies for various types of accounts receivable. These deviations were authorized by CCU, without an expiration date or renewal requirement, during the period between December 1979 and October 2017, the majority (88) of which were established prior to 1999. As of January 2018, the balance of accounts held by CCU that were submitted by agencies with current deviations totaled \$2.3 billion on 6.6 million accounts.

Without an effective monitoring process, there was a lack of assurance that all active deviations remained necessary and effective. For example, a finding on inadequate debt collection efforts in an audit report recently issued by our Office noted that the applicable State agency had been granted a deviation from CCU in 2005 to pursue arbitration with debtors owing less than \$5,000, rather than submit the accounts to CCU for collection. However, our audit report further noted that the agency advised us that it had not participated in arbitration since 2013, calling into question the need for continuing this deviation. In other examples, deviations remained in place even though they were initially granted based on data that may

² This includes 13 Maryland community colleges and 21 Register of Wills offices, none of which hold a deviation from CCU.

no longer be relevant, such as one deviation we noted that was based on cost data from 1985. In our opinion, a process for periodic monitoring, reevaluation, and renewal is necessary to determine if existing deviations are still warranted and effective.

CCU management was aware of this issue, and advised us that it conducted a one-time confirmation of deviations. Specifically, CCU sought confirmation that existing deviations were still required via a letter in January 2016 sent to each agency with an active deviation. However, the confirmation sought limited information, as it only required the agency to check a box indicating if the deviation was or was not still required. Agencies were not required to provide any information regarding the effectiveness of or outcomes attributable to the deviation, such as whether it helped to increase collections and reduce the number of accounts requiring submission to CCU. According to CCU, all agencies confirmed that they still required their respective deviations; however, CCU management acknowledged to us that this process was ineffective in assessing whether the deviations were still warranted.

State regulations generally require State agencies to send the debtor three written demands for payment at 30-day intervals after which the unpaid account is to be submitted to CCU for further collection efforts. With the approval of the Secretary of DBM, however, CCU may grant an agency a deviation from these regulations based on a documented request from the agency. Such requests must include the nature of the deviation, the type of accounts involved, and justification for the deviation. For example, an agency may request and receive approval to extend the period after which accounts must be sent to CCU in order to allow more time for debtors to respond to the agency's own collection efforts.

Recommendation 6

We recommend that DBM establish a formal process for periodically monitoring deviations granted to State agencies to ensure that they remain necessary and effective. For example, DBM could require each agency to periodically renew its deviation and, at that time, provide documentation supporting the need for and the effectiveness of the deviation.

State Tax Refund Intercept Program

Background

State law authorizes CCU to submit certain qualifying debts to the State's Tax Refund Intercept Program (TRIP), which is administered by the Comptroller of Maryland. TRIP redirects a debtor's State tax refund to CCU to pay off all or a

portion of the delinquent balance due. If the refund is greater than the debt owed, the Comptroller will issue a refund to the debtor for the difference.

CCU compiles debts for annual submission to the Comptroller for collection through TRIP, which has consistently been one of the most effective collection methods used. According to CCU's records, TRIP collections for CCU debts were approximately \$28.4 million of the \$131.2 million in total fiscal year 2018 CCU collections.

Finding 7

Certain significant debt amounts were excluded from TRIP because of CCU system omissions and errors.

Analysis

Certain significant debt amounts were excluded from submission to the Comptroller of Maryland for TRIP because of deficiencies in how CCU identified and prepared the accounts for submission. Based on our test of 30 debtor accounts totaling approximately \$74.7 million that were eligible for TRIP for the 2017 tax year, we determined that only debts totaling \$1.6 million were submitted for TRIP because of these deficiencies.

For individual debts exceeding \$100,000 that were eligible for TRIP, CCU submitted only the first \$99,999, and excluded the remaining debt balances. This occurred because CCU had not addressed an account balance limitation in its debt collection system that limited submissions to a five-character length and which should have been corrected in 2004 when the limitation was corrected on the Comptroller's system. To illustrate, as of January 2018, CCU's records included 909 accounts with balances of \$100,000 or more. Under CCU's current submission process, accounts totaling \$90.9 million (909 accounts times \$99,999) would be submitted for TRIP and the remaining balance of these accounts that exceeded \$99,999, totaling \$227.8 million, would be excluded from submission.

Although DBM management asserted that there was no loss of collections resulting from this limitation since income tax refunds rarely exceed \$100,000, this would not relieve CCU of its responsibility to submit the entire account balance for TRIP. Furthermore, information we obtained from the Comptroller indicated that approximately 1,050 refunds were issued during 2018 that exceeded \$100,000, totaling \$348.9 million. The value of actual tax refunds, if any, that were not subject to TRIP because of this account balance limitation was not readily determinable.

We further noted a process error in CCU’s TRIP submissions for tax year 2017. Specifically, CCU used its new Debt Manager system to combine multiple debt accounts for the same individual into a single account for TRIP submission purposes. However, if any one of the multiple accounts was ineligible for TRIP because, for example, it lacked certain necessary identifying information, a programming error in Debt Manager resulted in the combined single account being removed from TRIP eligibility, instead of just the ineligible debt. This process error might have been detected if CCU had performed a review for reasonableness. Specifically, our analysis of the 2017 tax year TRIP submission found that CCU submitted approximately 509,000 accounts with balances totaling \$845 million; this reflected significantly lower activity than the 2016 tax year when CCU submitted 3 million accounts with outstanding debts of \$1.9 billion.

As previously mentioned, our test of 30 debtor accounts totaling \$74.7 million determined that \$73.1 million from 28 accounts was not submitted for TRIP because of these two conditions, while a total of \$1.6 million was submitted for TRIP. The details of our test are shown in Table 3 below.

Count of Test Items	Approximate Value Range of Test Items	Items with Improper TRIP
20	\$600,000 - \$17,000,000	20
10	\$300 - \$700	8
<u>30</u>		<u>28</u>

Source: CCU records

Recommendation 7

We recommend that DBM correct the aforementioned deficiencies in the processes used for submission of delinquent accounts to the Comptroller of Maryland for TRIP. Specifically, we recommend that DBM take the necessary steps to ensure that the total balance of each debtor account and all eligible debtor accounts are submitted for inclusion in TRIP.

Finding 8

CCU collected TRIP revenues totaling \$11.6 million for a private entity after the law authorizing these collections to be handled by CCU was repealed in 2005.

Analysis

CCU collected revenues for a private entity through TRIP after the law authorizing such collections to be handled by CCU was repealed effective July 1, 2005. As of February 2018, CCU had improperly collected \$11.6 million on behalf of this private entity through TRIP and transferred these collections to the entity. Of this amount, \$1.8 million was collected during our audit period.

Specifically, the Maryland Higher Education Loan Corporation (MHELC) was a State-recognized nonprofit corporation that had been responsible for guaranteeing and providing loans for Maryland students for higher education expenses. Under State law, defaulted loans guaranteed through MHELC could be submitted to CCU for collection through TRIP. When MHELC was dissolved in 1996 and its debts and guarantees transferred to a private entity, State law continued to permit defaulted loans initially issued or guaranteed through MHELC, but managed by the private entity, to be submitted to CCU for collection through TRIP. However when this law was repealed effective July 1, 2005, CCU continued to collect debts on behalf of this entity using TRIP. In addition, correspondence sent by CCU after July 1, 2005 to debtors to notify them that their accounts from the private entity had been forwarded to CCU for collection continued to include the repealed State law as a reference during our audit period.

DBM was not aware of this matter until we brought the matter to its attention in January 2018. CCU advised us that it has discontinued forwarding collected funds to the private entity. As of June 2018, CCU represented that collections totaling approximately \$190,000 from the private entity's defaulted loans were being retained pending CCU's determination as to the proper disposition of these collections.

Recommendation 8

We recommend that DBM

- a. ensure that future TRIP submissions exclude debts from this private entity; and**
- b. in conjunction with legal counsel, determine the appropriate course of action regarding the \$11.6 million that we improperly collected on behalf of this private entity, as well as the appropriate disposition for the \$190,000 being retained and any related subsequent collections.**

Financial Management Information System

The Financial Management Information System (FMIS) is an integrated database system that runs on the Comptroller of Maryland's Annapolis Data Center's computers and supports individual agency and Statewide purchasing and accounting operations. According to the State's accounting records, expenditures processed through FMIS for fiscal year 2018, before fiscal year-end closing adjustments, totaled approximately \$34.7 billion (including State agencies that use their own computer systems, but interface with FMIS).

The State implemented FMIS in 1992 to replace separate accounting systems maintained by the Comptroller and DBM. In July 2008, in accordance with State law, the Office of Information Technology was removed from DBM and established as an independent department of the State—the Department of Information Technology (DoIT). Also in July 2008, a memorandum of understanding (MOU) between DBM and DoIT established DBM as the owner of FMIS and required DoIT to provide certain support services to DBM's financial applications, including FMIS.

That MOU was superseded in 2009 by an Operating Agreement between the Comptroller, DoIT, and DBM in which it was agreed that the three control agencies would actively engage in the functional and technical support associated with the enhancement, maintenance, documentation, operation, replacement, and disposition of the State's Relational Standard Accounting and Reporting System, which is one of the two components of FMIS. That Agreement also states that DoIT is responsible for information technology standards and procedures and the management of all system development life cycle tasks, including enhancements and exhibiting control over the system security, and the Comptroller has final approval authority for any core enhancements or modifications of accounting and/or reporting functions. To the extent that third-party reviews, such as those conducted by the Office of Legislative Audits, identify items related to the integrity of system controls, DBM and DoIT are to provide the Comptroller an action plan to resolve such issues and a monthly progress report until all issues are resolved.

Finding 9

Vendor PII was not adequately restricted in FMIS and was visible to 5,204 employees Statewide.

Analysis

DBM, in conjunction with the Comptroller and DoIT, did not ensure that access to vendor PII stored in FMIS was adequately restricted and that this PII was

otherwise safeguarded. Specifically, social security numbers (SSNs) were frequently recorded in FMIS as a vendor's identification number when the vendor was an individual, instead of a corporation. Accordingly, vendor PII—including vendor name, address, and SSNs—was displayed in FMIS in plain text on-line or in reports generated by FMIS.

While we did not perform a comprehensive review, we readily identified at least 9 FMIS screens and 13 FMIS reports containing vendor PII that were available to FMIS users throughout the State. As of August 2018, based on FMIS records, there were 5,204 State employees with access to FMIS and, therefore, depending on their access level, these users potentially had access to the sensitive PII.

The Comptroller's *Accounting Procedures Manual* states that vendor numbers in FMIS be coded with the number "1" followed by the 9-digit vendor federal identification number or SSN. As of May 2019, there were approximately 398,000 Statewide vendors in FMIS with PII, although there could be some duplication of vendors within this total number. The number of Statewide vendors excludes approximately 117,000 vendors who are State employees for which certain restrictions exist to limit access to their PII.

We believe that this situation represents a critical PII issue that requires a collective corrective action plan from the responsible agencies. Consequently, it is incumbent upon the three control agencies (the Comptroller, DoIT, and DBM) to ensure that PII in FMIS is adequately restricted and safeguarded, including determining whether practical alternatives to using PII in FMIS exist. State law defines any record containing an individual's name combined with a SSN as PII. Although the Comptroller's *Accounting Procedures Manual* instructs agencies to create vendor numbers using federal identification numbers or SSNs, it also paradoxically requires agencies to restrict access to SSNs to the extent practical. In addition, the State of Maryland *Information Technology Security Manual* requires that agencies ensure that access to confidential information is strictly controlled and audited and that it supports the concept of "least privilege" allowing only authorized access to accomplish assigned tasks.

We were advised by DBM's legal counsel that, in accordance with the July 2008 law creating DoIT, the responsibility for changes to FMIS, including any changes required to address the PII security issue had been transferred to DoIT. DoIT's legal counsel subsequently advised us that DoIT is required to confer with DBM and the Comptroller prior to any changes that impact FMIS accounting functions, procedures, or business operations.

Recommendation 9

We recommend that DBM, in conjunction with the Comptroller and DoIT, take the necessary steps to adequately restrict and safeguard PII in FMIS.

Information Systems Security and Control

Background

In 2008, DBM began to use certain DoIT Information Technology (IT) services. Throughout our current audit period, DBM used the following DoIT IT support services:

- DoIT maintained network firewalls and IT security services (such as intrusion detection prevention systems operations and maintenance).
- DoIT provided IT service desk assistance, hardware support, and software support (including malware protection support).

DBM utilizes the DoIT operated statewide network services for connections between its two Baltimore remote sites and the Annapolis headquarters location. The statewide network service provides DBM users access to various other information technology functions including email services, internet access, and key applications. DBM, DoIT, and their contractors maintain key applications such as the legacy CCU debt collection system (in use during our audit) and its replacement, the Debt Manager system, which record State of Maryland delinquent financial accounts, outstanding balances for such accounts, and present summaries of collection actions and current collection status for those accounts.

Finding 10

Sensitive PII maintained by CCU was stored without adequate safeguards.

Analysis

Sensitive PII maintained by CCU was stored without adequate safeguards (see Finding 2 for comment on user access to PII). Specifically, we reviewed one application and determined that as of May 2018, one file within CCU's debt collection application contained 1,216,224 unique SSNs stored in clear text along with associated names and addresses. In addition, we were advised that this sensitive PII was not protected by other substantial mitigating controls. This PII is commonly associated with identity theft. Accordingly, appropriate information system security controls need to exist to ensure that this information is safeguarded and not improperly disclosed. A similar condition was commented upon in our preceding audit report. The State of Maryland *Information*

Technology Security Manual requires that confidential data should be protected using encryption and/or other substantial mitigating controls.

Recommendation 10

We recommend that DBM use approved encryption methods or other substantial mitigating controls to properly protect all sensitive PII (repeat).

Finding 11

DBM did not have a complete information technology disaster recovery plan (DRP) for recovering computer operations.

Analysis

DBM did not have a complete information technology DRP for recovering computer operations from disaster scenarios (for example a fire). The State of Maryland *Information Technology Disaster Recovery Guidelines* establish the minimum required elements needed for a DRP. DBM's DRP did not address certain of these minimum requirements. For example, the DRP did not contain required listings of hardware and software and adequate details for restoration of network connectivity. Additionally, the DRP had not been tested. Without a complete and tested DRP, a disaster could cause significant delays (for an undetermined period of time) in restoring information systems operations above and beyond the expected delays that would exist in a planned recovery scenario.

Recommendation 11

We recommend that DBM

- a. develop and implement a comprehensive DRP that is in accordance with the aforementioned *Information Technology Disaster Recovery Guidelines*; and**
- b. periodically test the DRP, document the testing, and retain the documentation for future reference.**

Finding 12

Network security risks existed from IT contractors having unnecessary network-level access to the DBM network and the unnecessary assignment of administrative rights on numerous workstations.

Analysis

Network security risks existed from IT contractors having unnecessary network-level access to the DBM network and the unnecessary assignment of administrative rights on numerous workstations.

- We identified a number of IT contractors with unnecessary access to the DBM network. According to DBM records, as of June 2018, there were 63 contractors working on multiple DBM system development projects and using DBM's internal network. DBM personnel advised us that these contractors only required access to the specific development servers and resources involved with their respective IT projects and certain support servers, such as email servers. However, from our review of the three largest DBM system development projects we determined that 17 of 39 IT contractors involved were granted unnecessary network-level access to the entire DBM internal network as well as to other DBM network segments containing hosted critical servers, such as servers supporting State employee benefits administration and capital budgeting.

The unnecessary access occurred because the network traffic from the contractor workstations was not subject to any filtering. The network-level access by DBM's onsite IT contractors should be limited to only the network devices and ports required for them to perform their contractual duties. The State of Maryland *Information Technology Security Manual* requires an authorization process which specifically grants access to information ensuring that access is strictly controlled, audited, and that it supports the concept of least privilege allowing only authorized access to accomplish assigned tasks.

- We identified 34 user accounts defined on 36 DBM workstations that were assigned local administrative rights even though these users were not system/network administrators. In addition, DBM could not provide documentation that would have authorized and supported the necessity of these assigned administrative rights. Consequently, if the above workstations were infected with malware, the malware would run with administrative rights and expose these workstations to a greater risk of compromise than if the workstations' user accounts operated with only user rights.

Recommendation 12

We recommend that DBM, in conjunction with DoIT

- a. restrict IT contractors' network-level access to only those network devices and ports required for them to perform their duties; and**
- b. limit the assignment of administrative rights on workstations to only system/network administrators and those users specifically allowed such rights, with any such assignments to non-IT administrators being justified, approved, documented, and regularly reviewed to determine whether they are still needed.**

Interagency Agreements

Background

Interagency agreements are used by State agencies to obtain services, such as technical assistance and training, from another State agency, including public institutions of higher education. Interagency agreements are exempt from State procurement laws, including the requirements for competitive procurement, publication of solicitations and awards, and Board of Public Works' approval.

Since fiscal year 2005, State budget law has required agencies to report all interagency agreements between State agencies and public institutions of higher education that are valued at more than \$100,000 to DBM. State budget law also requires that DBM provide direction and guidance to State agencies regarding the reporting of these interagency agreements, including the specific elements to be reported. Finally, DBM is responsible for compiling an annual listing of such agreements and reporting that compiled information to the General Assembly's budget committees.

For fiscal years 2016 and 2017, State budget law established an additional requirement for DBM to review each agreement in excess of \$500,000 to determine why the services could not be provided directly by the State agency, and to provide pre-approval for all new agreements over this dollar limit. For fiscal year 2018, State budget law continued to require DBM to review and approve new agreements in excess of \$500,000. Furthermore, a new State law, effective June 1, 2017, required DBM to review each interagency agreement with actual expenditures of more than \$750,000 that has been in place for three or more years and to report a summary of its findings annually. In fiscal year 2018, 307 interagency agreements, collectively valued at \$405.9 million, were reported by State agencies to DBM, including 108 agreements totaling \$356.0 million, each valued at more than \$500,000.

Finding 13

DBM did not require State agencies to report interagency agreements with local community colleges.

Analysis

DBM did not require State agencies to include their agreements with local community colleges in their annual reporting of interagency agreements. However, we were advised by a Board of Public Works official that a State agency's agreement with a local community college should be considered an interagency agreement and, accordingly, is also exempt from State procurement regulations.

DBM's written instructions to agencies for reporting interagency agreements did not advise agencies that agreements with community colleges were to be considered interagency agreements and should be reported if the \$100,000 threshold was met. Further, our review of the annual interagency agreement list prepared by DBM for fiscal years 2015 through 2018 did not disclose the inclusion of any community colleges except Baltimore City Community College (BCCC), which is a State agency. Consequently, it appears that State agency agreements with Maryland community colleges (other than BCCC) were not being reported to DBM, were not subjected to DBM preapproval if over \$500,000, and were not reported to the General Assembly.

Two audit reports issued by our Office since May 2018 included findings regarding six agreements between the applicable State agencies and community colleges. For example, in one report we noted that the agency had entered into several agreements with a community college to provide staffing for certain services. The report noted that these agreements allowed the agency to avoid using competitive procurement processes for these services, filling existing positions, or seeking additional budgeted positions as necessary. The value of these agreements totaled \$15 million.

Recommendation 13

We recommend that, in its written instructions regarding the reporting of interagency agreements, DBM inform State agencies that agreements with community colleges are considered interagency agreements, and, accordingly, are subject to the aforementioned reporting requirements.

Motor Vehicle Fleet

Finding 14

DBM lacked documented justification for excluding certain vehicle types from its annual review of vehicle usage. In addition, DBM's cost assessments of the need for an agency to retain vehicles when they were not driven the minimum annual miles without adequate justification were not properly calculated.

Analysis

DBM's annual review of State agency compliance with vehicle usage requirements excluded numerous vehicles, and DBM lacked documentation of the justifications used to exclude these vehicles from its review. In addition, DBM's formal cost analysis of vehicles driven less than the annual minimum miles was not properly completed. Under the provisions of State law, DBM is to oversee the

use of motor vehicles by units of the Executive Branch. DBM's *Policies and Procedures for Vehicle Fleet Management*, adopted pursuant to this law, state that vehicles driven fewer than 10,000 miles annually are subject to review to provide assurance that they are being used in the most efficient and effective way.

Our review found that, of the 79 vehicle types used by State agencies, 73 were excluded from DBM's annual review, and certain vehicles were excluded from the 6 vehicle types that were reviewed. The purpose of DBM's annual review is to identify vehicles driven fewer than the required 10,000 miles and to obtain justification from the applicable agencies as to why such vehicles are needed in spite of the lower mileage. Although it may be appropriate to exclude certain vehicles types from this review, such as law enforcement vehicles, DBM had not documented its justification for excluding any vehicle types. Other vehicle types excluded from DBM's review were, for example, midsize sedans and cargo vans. In addition, the 6 vehicle types included in DBM's review included 3,965 vehicles; however, DBM excluded 1,260 of these vehicles from its mileage usage review and could provide no explanation for doing so.

Furthermore, DBM did not use appropriate cost data for each vehicle type when performing its breakeven assessments for vehicles included in its review (such as certain sedans, sport utility vehicles, and passenger vans). These breakeven assessments were performed for vehicles that did not meet the mileage requirement and for which the agency failed to provide adequate justification. The purpose of the assessments was for DBM to determine if the vehicle was driven at least the number of miles necessary to justify the cost of retaining the vehicle. However, we found that this analysis was flawed because it applied cost data and breakeven mileage for a small sedan to all vehicle types, even though maintenance costs are not the same across all vehicles.

Recommendation 14

We recommend that DBM

- a. document its justification for excluding certain vehicle types from its annual review of vehicle usage;**
- b. based on the vehicle types to be reviewed, include all vehicles of that type in its review; and**
- c. use appropriate cost data for each vehicle type when performing its breakeven assessments.**

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the following units of the Department of Budget and Management (DBM) for the period beginning July 15, 2014 and ending October 19, 2017.

Office of the Secretary (including the Central Collection Unit)
Office of Budget Analysis
Office of Capital Budgeting

The audit was conducted 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.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine DBM's financial transactions, records, and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of significance and risk. The areas addressed by the audit included cash receipts, collection practices, accounts receivable, procurement and disbursement activity, payroll, interagency agreements, and vehicle fleet maintenance. Our audit included DBM's administration of the Cigarette Restitution Fund and State Reserve Fund that consisted of the Dedicated Purpose Account, the Revenue Stabilization Account, the Economic Development Opportunities Program Fund, and the Catastrophic Event Fund.

Our audit also included certain support services (such as payroll, maintenance of certain accounting records) provided by DBM's Office of the Secretary to the Office of Personnel Services and Benefits. In addition, it included certain support services (such as legal, internal audit, and budgeting) provided by DBM to the Department of Information Technology. We also determined the status of the findings contained in our preceding audit report.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of DBM's operations and tests of transactions. Generally, transactions were selected

for testing based on auditor judgment, which primarily considers risk. Unless otherwise specifically indicated, neither statistical nor non-statistical audit sampling was used to select the transactions tested. Therefore, the results of the tests cannot be used to project those results to the entire population from which the test items were selected.

We also performed various data extracts of pertinent information from the State's Financial Management Information System (such as expenditure data) and the State's Central Payroll Bureau (payroll data), as well as from the contractor administering the State's Corporate Purchasing Card Program (credit card activity). The extracts are performed as part of ongoing internal processes established by the Office of Legislative Audits and were subject to various tests to determine data reliability. We determined that the data extracted from these sources were sufficiently reliable for the purposes the data were used during this audit.

We also extracted data from DBM's debt collection system in order to perform certain tests related to cash receipts and accounts receivable, including collection practices. We performed various tests of the relevant data and determined that the data were sufficiently reliable for the purposes the data were used during the audit. Finally, we performed other auditing procedures that we considered necessary to achieve our objectives. The reliability of data used in this report for background or informational purposes was not assessed.

DBM's management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records; effectiveness and efficiency of operations including safeguarding of assets; and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings relating to conditions that we consider to be significant deficiencies in the design or operation of internal control that could

adversely affect DBM's ability to maintain reliable financial records, operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes findings regarding significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to DBM that did not warrant inclusion in this report.

DBM's response to our findings and recommendations is included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise DBM regarding the results of our review of its response.



LARRY HOGAN
Governor

BOYD K. RUTHERFORD
Lieutenant Governor

DAVID R. BRINKLEY
Secretary

MARC L. NICOLE
Deputy Secretary

October 17, 2019

Mr. Gregory A. Hook, CPA
Legislative Auditor
Office of Legislative Audits
State Office Building, Room 1202
301 West Preston Street
Baltimore, Maryland 21201

Dear Mr. Hook:

The Department of Budget and Management (DBM) has reviewed your draft audit report on the DBM - Office of the Secretary and Other Units for the period beginning July 15, 2014 and ending October 19, 2017. As requested, attached are our responses to the findings in the report.

If you have any questions or need additional information, you may contact me at 410-260-7041 or Joan Peacock, Audit Compliance Unit Manager, at 410-260-7079.

Sincerely,

A handwritten signature in blue ink, appearing to read "David R. Brinkley", is written over the typed name and title.

David R. Brinkley
Secretary

cc: Secretary Michael G. Leahy, DoIT
Marc Nicole, Deputy Secretary, DBM
Brent Bolea, Principal Counsel
Michael Scott Friedman, Deputy Counsel
Anthony Fugett, Director, Central Collection Unit
Mary Naramore, Manager, Interagency Agreements, DBM
Joseph Consoli, Administrator, State Fleet & Travel Management Unit, DBM
Joan Peacock, Manager, Audit Compliance Unit, DBM

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

System Controls

Finding 1
CCU did not perform a periodic review of user access to its debt collection and cash register systems, and did not adequately restrict access to those systems.

We recommend that DBM

- a. perform a documented periodic review of user access to its debt collection system and its cash register system to ensure that access capabilities for critical functions are restricted to employees who require such capabilities to perform their assigned job duties and in a manner that ensures a proper segregation of duties, and
- b. eliminate the identified unnecessary and incompatible access capabilities.

Agency Response			
Analysis			
Recommendation 1a	Agree	Estimated Completion Date:	October 2019
Corrective Action:	<p>With efforts focused on the implementation of the CCU IT modernization project, periodic reviews of user access were not performed.</p> <p>The actions recommended by the auditors related to the legacy debt collection system are no longer relevant as that system is only being used as a library for viewing of historical information no longer being used by CCU. In CCU's new debt manager system, access is granted by various role types. As the new system evolves and experience is gained, we are working on putting procedures in place to address user roles/access. CCU agrees to review access to its debt manager system periodically, at least on an annual basis, with the first review to be performed October 2019. This review will ensure that access is appropriate (i.e., adequate separation of critical functions exists) and that access assigned to individuals is necessary for the user to perform their job duties. These periodic reviews and follow actions taken to correct access will be documented and maintained.</p> <p>It is important to note that access to the cash register system, particularly at the MVA satellites offices, is driven by some important factors:</p> <ul style="list-style-type: none"> Due to the nature and volume of MVA operations, it is important that service be granted as efficiently and timely as possible as MVA offices are extremely busy. No one wants to spend more time than necessary waiting in line at MVA. In addition, debtors often need to get an account cleared through CCU quickly so that they are not restricted from conducting business with MVA. There are a limited number of CCU personnel at these offices, so an overlap of access is required for backup purposes when staff are not available. <p>Making changes in access to cash register system, which resides on the MDOT/MVA's (not DBM's) network, cannot be performed quickly to address</p>		

Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019

	<p>when CCU satellite staff are absent. With the implementation of phase 2 of the new debt manager system (currently estimated in December 2020), access changes to the cash register system should become easier to process.</p> <p>As an additional control, DBM CCU has in place a process for the MVA satellite offices to ensure the appropriateness of void transactions. The CCU Accounting office independently reviews all voided transactions performed by MVA satellite offices. With the limited resources at the satellite offices and the mission to ensure adequate and appropriate customer service, it is not feasible to establish a procedure where all voids must be independently approved prior to being processed. While performed after voids are processed, the independent review performed by Accounting is adequate to ensure that all voids are appropriate.</p> <p>Beginning October 2019, DBM CCU Satellite Manager and IT staff will perform periodic (i.e., at least annually) reviews of user access to the cash register system to ensure that user access is appropriate and necessary. This review and follow actions taken to correct access will be documented and maintained.</p>		
Recommendation 1b	Agree	Estimated Completion Date:	October 2019
Corrective Action:	<p>The review completed in October 2019 will include a review of all users, including those identified in the finding. The review of user access identified and corrected any users</p> <ul style="list-style-type: none"> • with critical access that was either unnecessary or inappropriate and • with inappropriate access in both the debt collections system and the cash register system. <p>As noted above and specifically for CCU MVA satellite offices, certain users may still have access to process cash receipts and to void transactions. The review of void transactions done by CCU Accounting is a control in place to ensure the appropriateness of these transactions. CCU will periodically re-evaluate whether another process may be established. The CCU will also have an independent review performed by the Internal Auditor for this process.</p>		

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

Finding 2

DBM did not ensure that access to personally identifiable information (PII) stored in its debt collection system, such as names and related social security numbers, was restricted. We noted that PII for approximately 5.8 million accounts was not adequately restricted.

We recommend that DBM

- a. to the extent practicable, limit view access to PII, consistent with user needs, by removing or otherwise masking PII data, including SSNs, within the debt collection system;**
- b. search the system and remove SSNs from non-SSN data fields, as feasible, and establish controls to prevent future posting of SSNs to improper data fields; and**
- c. in conjunction with user agencies, remove the unnecessary user access to PII through DBM’s website application, including accounts with no user activity.**

Agency Response			
Analysis			
Recommendation 2a	Agree	Estimated Completion Date:	Completed
Corrective Action:	<p>The legacy debt collection system has been replaced by the new debt manager system and will remain as a read-only library. In addition, the legacy system’s data has been transferred to a virtual server which is encrypted. The PII currently being retained as part of this data is necessary. We believe adequate restrictions and controls are in place to safeguard and secure this sensitive data</p> <p>As the new debt manager system was being implemented, reviews were completed to determine what PII was necessary to be retained. We have also taken steps during the implementation to ensure that proper safeguards and controls were established to protect improper disclosure of such sensitive data. During the implementation of the debt manager system, users were only given roles that provided access to PII when necessary and required to perform their job duties. Beginning September 2019, access to PII will be reviewed as part of the periodic (i.e., at least annual) reviews of access to the debt manager system.</p> <p>The Statewide access to all accounts granted 26 users, as noted in the finding, is necessary as they are either members of the CCU IT modernization project team or are Private Collection Agency personnel who have cleared background checks and signed non-disclosure agreements.</p> <p>With regard to Debt Manager, specific database fields/tables that contain PII are encrypted at rest. CCU has determined that masking PII data is not a feasible option since this data is needed to conduct business.</p>		

Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019

Recommendation 2b	Agree	Estimated Completion Date:	March 2020
Corrective Action:	CCU will investigate to determine if it is possible or feasible to search the system for SSNs in non-SSN data fields, as well as investigating whether the system can be enhanced to add controls to prevent future posting of SSNs to improper data fields.		
Recommendation 2c	Agree	Estimated Completion Date:	October 2019
Corrective Action:	<p>The application referred to in the analysis (that is accessed through DBM's website and allows authorized users to view and produce reports) was retired December 31, 2018. This application was replaced with a portal to the new debt manager system.</p> <p>Access to the portal is controlled by requiring approval from the designated authorized person at each specific agency along with CCU approval. Beginning in October 2019, CCU will also conduct a periodic (i.e., at least annual) review of access to the portal to ensure access is limited to individual's job duties require such access. Corrective action will be taken for any unnecessary access. This review will be documented and maintained.</p>		

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

Finding 3

Deficiencies in CCU's debt collection system resulted in the failure to assess collection fees of at least \$17.8 million and the improper rejection of certain valid debts.

We recommend that DBM correct these programming deficiencies and ensure that its collection fee is applied to all amounts due, and that the determination as to whether a debt meets the dollar threshold for CCU acceptance from an agency is based on the total amount due.

Agency Response			
Analysis			
Recommendation 3	Agree	Estimated Completion Date:	March 2020
Corrective Action:	<p>With the implementation of the new debt manager system, collection fees are now being assessed on the entire account balance including both principal and interest. Enhancements were made to the new system to ensure that interest assessed after the account is transferred to CCU is accurately recorded in the debtor's account. For non-judgement accounts, this was completed October 2019. Judgement accounts are more complicated and will take more time to address. This should be completed by March 2020.</p> <p>The programming issue present in the legacy debt collection system, that rejected certain valid debts as referred to in the audit analysis, was resolved with the implementation of new debt manager system. The new system looks at the total account balance when performing uploads. We are not aware of any additional programming deficiencies in the new system that would cause similar errors and believe all debts with a total balance due of \$30 or greater will properly be accepted for collection.</p> <p>Additionally, with the implementation of the debt manager system, error reports will be automatically generated and sent to the uploading agency. Training has been provided to State agencies. If there are any concerns are issue with accounts that have been rejected for collection, the State agency is to notify CCU. Training provided also addressed the proper procedures and dollar limits for submitting accounts for collection or abatement.</p> <p>Going forward, CCU will consider additional training and determine whether sending out periodic notifications to remind agencies of dollar limits for submitting accounts for collection or abatement.</p>		

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

Collection Efforts

Finding 4
CCU did not adequately pursue potential wage garnishments from debtors.

We recommend that DBM

- a. take appropriate action to pursue potential wage garnishments from debtors in a timely manner and document its efforts (repeat), and
- b. establish guidance on prioritizing accounts for potential wage garnishments within CCU's debt collection policies.

Agency Response			
Analysis			
Recommendation 4a	Agree	Estimated Completion Date:	TBD
Corrective Action:	<p>DBM CCU agrees that potential wage garnishments from debtors should be adequately pursued in a timely manner. Documentation is currently maintained for all wage garnishments pursued. As noted above, the wage garnishment process is complex, expensive and lengthy.</p> <p>Over the past few years, CCU has continued to increase the number of suits filed in pursuit of potential wage garnishments; however, the problem is an issue of sheer volume. As the number of accounts referred to CCU increase, so will the potential opportunities to pursue wage garnishments. As noted by the auditors, the number of accounts increased significantly during the recent audit period because the Maryland Transportation Authority transferred their delinquent toll violation accounts to CCU rather than collecting in-house.</p> <p>Legislation for a new CCU Lien process was proposed in the 2017 Session that would have simplified the wage garnishment process and was believe to fully address this finding. Unfortunately, it was not passed.</p> <p>CCU will continue to make the best use of its resources to collect from debtors and will ensure that collection efforts are documented. With the implementation of Debt Manager, CCU will be able to gain efficiency through continued automation. This includes taking advantage of current and future automation of the various county courts systems.</p>		
Recommendation 4b	Agree	Estimated Completion Date:	TBD
Corrective Action:	<p>As the wage garnishment process evolves, CCU will consider supplementing its debt collection policies to provide written guidance on prioritizing accounts for potential wage garnishments.</p>		

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

Finding 5

CCU did not have adequate controls over the abatement of accounts, which totaled approximately \$39.1 million during our audit period.

We recommend that DBM

- a. establish adequate controls over the abatement process by having an independent employee use system-generated reports to verify that all changes in account status to any type abatement status have been properly authorized;**
- b. investigate and resolve the aforementioned account for which there was no approval from the abatement committee, as well as the three accounts for which there was no approval for a change in abatement status; and**
- c. perform a review of all account changes to abatement status that were made since July 2016 to determine if there are additional unapproved changes in status and take appropriate action.**

Agency Response			
Analysis			
Recommendation 5a	Agree	Estimated Completion Date:	October 2019
Corrective Action:	<p>In the new debt manager system, there are no longer any abatement status codes. Accounts are tagged as eligible for abatement and placed into a queue to be reviewed for abatement by the committee. Appropriate segregation of duties will be implemented to ensure individuals who select accounts to be submitted to the abatement committee (i.e., apply the eligible for abatement tag) are separate from the individuals who forward approved accounts for processing. Once approved by the committee, an independent individual will update (apply the approved for abatement tag) the status of accounts in the system.</p> <p>An audit report will be developed for review that shows all changes in abatement status since the prior abatement committee meeting. This report will be reviewed by an individual that doesn't have access to make changes regarding abatement status (i.e., eligible, approved, etc.). Any changes that appear improper will be investigated and appropriate action will be taken. This review will be documented and maintained.</p>		
Recommendation 5b	Agree	Estimated Completion Date:	Completed
Corrective Action:	<p>The noted items were investigated and corrected to the appropriate status codes. This was done in the legacy debt collection system prior to the implementation of the new debt manager system.</p>		

Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019

Recommendation 5c	Agree	Estimated Completion Date:	December 2019
Corrective Action:	DBM Audit will perform a review of all account changes to abatement status that were made since July 2016 to determine if there are additional unapproved changes in status. Appropriate action will be taken for any inappropriate abatements or incorrect status changes. This review will be documented and maintained.		

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

Finding 6

CCU did not perform a periodic review of existing deviations from State regulations previously granted to State agencies regarding the submission of delinquent accounts to CCU.

We recommend that DBM establish a formal process for periodically monitoring deviations granted to State agencies to ensure that they remain necessary and effective. For example, DBM could require each agency to periodically renew its deviation and, at that time, provide documentation supporting the need for and the effectiveness of the deviation.

Agency Response			
Analysis			
Recommendation 6	Agree	Estimated Completion Date:	December 2019
Corrective Action:	<p>CCU will perform a review of approved deviations to determine if the deviations are still valid and to assess the impact of the deviation on debt collectability. Where appropriate, CCU will request supporting documentation from the applicable agency. This review will be documented and maintained.</p> <p>Based on the results of this review, CCU will determine how often future deviation reviews should be performed and establish a process to periodically perform such reviews. We will also analyze the existing deviations to determine whether expiration dates are needed based on the likely impact on debt collectability. Expiration dates may be established on a case by case basis. However, it is reasonable to establish indefinite deviations for some agencies (e.g. a higher educational institution). Specifically, indefinite deviations would be practical where the circumstances requiring the deviation (i.e. semester schedules) will remain unchanged.</p>		

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

State Tax Refund Intercept Program (TRIP)

Finding 7

Certain significant debt amounts were excluded from TRIP because of CCU system omissions and errors.

We recommend that DBM correct the aforementioned deficiencies in the processes used for submission of delinquent accounts to the Comptroller of Maryland for TRIP. Specifically, we recommend that DBM take the necessary steps to ensure that the total balance of each debtor account and all eligible debtor accounts are submitted for inclusion in TRIP.

Agency Response			
Analysis			
Recommendation 7	Agree	Estimated Completion Date:	Completed
Corrective Action:	<p>The account maximum of \$99,999.99 was a limitation of the legacy debt collection system which has been resolved with the implementation of the new debt manager system. With the implementation of the new system, there are no limitations on the amounts that may be submitted for TRIP. Thus, CCU will make certain that the total balance of accounts eligible for TRIP are included in the certified TRIP file.</p> <p>DBM CCU believes the process error identified in CCU's TRIP submissions for tax year 2017 was an isolated incident. This one-time mistake was made as part of the conversion process from the legacy debt collection system to the new debt manager system that removed debtors rather than individual accounts from TRIP certification. CCU is not aware of any significant, unexplained differences in TRIP submissions in previous years.</p> <p>Beginning with the 2018 tax year submission, CCU implemented additional controls to ensure that all eligible accounts are included for TRIP. The controls will consist of weekly meetings to manually review the TRIP data for reasonableness (e.g. dollar value compared to previous years, number of accounts compared to previous years). These reviews will be documented and maintained.</p> <p>CCU has verified that the programing issues, identified in the finding, have been corrected.</p>		

Auditor's Comment: DBM's response implies that the deficiency associated with its submission for TRIP of only the first \$99,999 in each debt was a limitation of its legacy debt collection system. As noted in the finding analysis, however, this limitation could

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

have been corrected in its system in 2004 when the limitation was corrected in the Comptroller's system.

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

Finding 8

CCU collected TRIP revenues totaling \$11.6 million for a private entity after the law authorizing these collections was repealed in 2005.

We recommend that DBM

- a. ensure that future TRIP submissions exclude debts from this private entity; and
- b. in conjunction with legal counsel, determine the appropriate course of action regarding the \$11.6 million that was improperly collected on behalf of this private entity, as well as the appropriate disposition for the \$190,000 being retained and any related subsequent collections.

Agency Response			
Analysis			
Recommendation 8a	Agree	Estimated Completion Date:	Completed
Corrective Action:	As part of our annual TRIP process, we will ensure that all TRIP services provided are authorized by law or regulation. Immediately, CCU has ceased any TRIP activity related to the private entity noted by the auditors. We are currently not aware of any other unauthorized TRIP activity.		
Recommendation 8b	Agree	Estimated Completion Date:	December 2019
Corrective Action:	CCU is evaluating the appropriate course of action to be taken with funds previously collected.		

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

Financial Management Information System

Finding 9

Vendor PII was not adequately restricted in FMIS and was visible to 5,204 employees Statewide.

We recommend that DBM, in conjunction with the Comptroller and DoIT, take the necessary steps to adequately restrict and safeguard PII in FMIS.

Agency Response	
Analysis	
General Comment:	<p>DBM agrees that PII should be protected from any improper access or usage, including in DBM’s use of FMIS for its own fiscal, accounting and procurement activities. However, we disagree that DBM is the “owner” of FMIS and has the authority or responsibility to make the recommended changes as they pertain to the FMIS system in general. DBM’s AAG has discussed this issue with the General Assembly’s Counsel. Both AAG’s have advised DBM that the law (Chapter 9 of the laws of 2008) which established the Department of Information Technology (DoIT) essentially transferred everything that was the responsibility, right or duty of DBM’s Office of Information Technology prior to the effective date of July 1, 2008, to DoIT. This includes property and contracts. The transfer of responsibility for FMIS to DoIT is further evidenced by the fact that the entire budget and all staff associated with FMIS was transferred to DoIT. Additionally, DoIT is a signed party on the contract with the third party vendor that provides operation and maintenance services related to FMIS. DBM is not a party to this contract.</p> <p>The Comptroller’s General Accounting Division (GAD) is primarily responsible (ownership) for accounting R*STARS operations. DoIT continues to be responsible for daily FMIS administration, including maintenance, operation, security, and back-up of related database records and the computer programs. This is consistent with how the control agency responsibilities have been understood and presented in the last three audit reports issued by OLA on FMIS Centralized Operations since the split of DoIT from DBM in 2008. DBM has not even been contacted or involved in any way in these FMIS audits. DBM’s current role in using FMIS is limited to DBM’s own agency fiscal, accounting and procurement activities. DBM does not have the authority to make the system-wide FMIS changes recommended by OLA. DBM only has the authority to implement the PII recommendations as they pertain to DBM’s use of FMIS for DBM’s own fiscal, accounting, and procurement activities.</p> <p>We do agree that there is apparent conflicting language with the law in DBM’s MOU with DoIT, as well as the RSTARS Operating Agreement. We agree that these agreements should be modified to reflect current responsibilities with regard to FMIS.</p>

Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019

	DBM fully supports the Comptroller’s Office and DoIT and will provide any support necessary to ensure the necessary steps are taken to restrict access to and safeguard PII in FMIS.
--	--

Auditor’s Comment: DBM asserts that, as a result of the establishment of DoIT in July 2008 and the transfer of DBM’s Office of Information Technology to DoIT, it no longer has the authority or responsibility to make the recommended changes to FMIS. However, as noted in the Finding Analysis and as acknowledged by DBM in its response, this position is inconsistent with the subsequent MOU and Operating Agreement. Nevertheless, DBM does agree that PII should be restricted and safeguarded, and agrees to work with the Comptroller and DoIT to that end.

Recommendation 9	Agree	Estimated Completion Date:	TBD
Corrective Action:	<p>DBM understands that DoIT is working on a plans to address this finding including any changes required to adequately restrict or possibly delete PII from FMIS. This includes the possibility of masking PII on FMIS reports and FMIS screens. DoIT has indicated that any changes that results from these plans will require GAD approval which may be difficult to obtain since GAD has stated how access and the ability to view certain PII information is necessary and required for their job duties.</p> <p>We understand the following specific actions are being taken by DoIT:</p> <ul style="list-style-type: none"> • Agency security officers will be requested to review FMIS user’s security level for each online screen. They will determine if access to the screen is necessary and revoke as required. Essentially, only users of FMIS that require access to the specific system components are granted access. • The replacement of the State’s online procurement application was recently implemented. This new system (eMMA) is required to adhere to the State’s Cybersecurity policy including items related to protecting PII. • It is impractical to remove PII in FMIS in its entirety given our tax reporting mandate. However, DoIT will work to minimize PII exposure where ever possible. FMIS reports will be reviewed determining if masking the vendor number is an option. Masking will take into consideration report type (control, request-able), GAD concerns and that actions taken should not inhibit the ability of State employees to perform their job function. • Online screens within FMIS will be reviewed to determine the screen type –data entry or inquiry - and if masking the vendor number is practical. Masking will take into consideration screen type, document status, user access, GAD concerns and that actions taken should not inhibit the ability of State employees to perform their job function. Any masking discussion will require a lengthy detailed walk through of all processes to gain a complete understanding of how all of the tables interact. Any 		

Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019

	<p>programming changes made could introduce significant operational risk to daily State-wide payment functions.</p> <p>While we understand the risk associated with PII in FMIS, the data elements are necessary for tax reporting and liability offset capture. Vendors and their associated PII are only added into FMIS when payment is required. Hence, the vendor associated PII is necessary. Yearly processes are executed in FMIS that disable vendors after five years of inactivity and are removed from the application after 10 years of inactivity. The purge function minimizes the amount of PII captured and retained within FMIS.</p>
--	--

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

Information Systems Security and Control

Finding 10

Sensitive PII maintained by CCU was stored without adequate safeguards.

We recommend that DBM use approved encryption methods or other substantial mitigating controls to properly protect all sensitive PII (repeat).

Agency Response			
Analysis			
Recommendation 10	Agree	Estimated Completion Date:	Completed
Corrective Action:	The legacy debt collection system has been replaced and will remain as a read-only library for approximately one year. DBM CCU utilizes software tools that allow secure and automatic transfer of files as well as file encryption software to ensure encryption of critical, nonpublic personal payment information. In addition, the new debt manager system, which was implemented in July 2018 to replace the legacy system, provides for encryption of sensitive PII data using appropriate encryption which are consistent with current industry standards.		

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

Finding 11

DBM did not have a complete information technology disaster recovery plan (DRP) for recovering computer operations.

We recommend that DBM

- a. develop and implement a comprehensive DRP that is in accordance with the aforementioned *Information Technology Disaster Recovery Guidelines*; and**
- b. periodically test the DRP, document the testing, and retain the documentation for future reference.**

Agency Response			
Analysis			
Recommendation 11a	Agree	Estimated Completion Date:	TBD
Corrective Action:	DoIT is in the process of hiring a full time dedicated resource to develop and maintain DRPs for each of our enterprise services customers. These DRPs will include DBM and its unique information technology operations and will be consistent with the State of Maryland <i>Information Technology (IT) Disaster Recovery Guidelines</i> .		
Recommendation 11b	Agree	Estimated Completion Date:	TBD
Corrective Action:	Once established, DoIT will periodically test the DRP. Testing will be documented and retained for future reference.		

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

Finding 12

Network security risks existed from IT contractors having unnecessary network-level access to the DBM network and the unnecessary assignment of administrative rights on numerous workstations.

We recommend that DBM

- a. restrict IT contractors' network-level access to only those network devices and ports required for them to perform their duties; and
- b. limit the assignment of administrative rights on workstations to only system/network administrators and those users specifically allowed such rights, with any such assignments to non-IT administrators being justified, approved, documented, and regularly reviewed to determine whether they are still needed.

Agency Response			
Analysis			
Recommendation 12a	Agree	Estimated Completion Date:	December 2019
Corrective Action:	DoIT and DBM will need to collaborate to determine the most appropriate design to resolve the issue. Addressing this issue will require that we functionally change the way the DBM network works, possibly enabling and using user-id, or one of many other potential options. This project could scale to be large, depending on the use cases defined. We may find it easier to provide guest wireless and have contractors with limited need-to-know VPN in to the required resources or try to implement user-id. Because there are several potential options, we are creating a new project with the purpose of developing the most appropriate solution for this finding. We expect a solution will be developed and implemented by December 2019.		
Recommendation 12b	Agree	Estimated Completion Date:	December 2019
Corrective Action:	DoIT will document policies for maintaining and controlling access rights. DoIT plans to leverage various tools to assess all current environments by the end of the fiscal year. Unnecessary local administrative accounts will be removed through group policies applied to the DBM domain. Once in place, these group policies will remove any non-approved local administrative access each time the computer checks in. With this in place, DoIT will reassess every six months to ensure policies are being properly applied. Documentation of any necessary exceptions will be kept in spreadsheet form and provided to the Security team to review and maintain.		

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

Interagency Agreements

Finding 13
DBM did not require State agencies to report interagency agreements with local community colleges.

We recommend that, in its written instructions regarding the reporting of interagency agreements, DBM inform State agencies that agreements with community colleges are considered interagency agreements, and, accordingly, are subject to the aforementioned reporting requirements.

Agency Response			
Analysis			
General Comment:	DBM is fully aware that State agency agreements with public community colleges are interagency agreements. From the very start of reporting requirements, and based on discussions with and concurrence from DLS, State agency agreements with non-State of Maryland community colleges have not been included within required reporting. BCCC has been included because it is a State entity. The fact that the legislative language requires “all State agencies and public institutions of higher education to report” their agreements to DBM further underscores the understanding of this language to apply only to State of Maryland higher education institutions as this budget language does not impact and cannot compel non-State institutions to report to DBM. Furthermore, the initial concern of DLS in including this language was to identify the amount of State agency funds going to State institutions of higher education and the purposes for which those funds were going.		
Recommendation 13	Agree	Estimated Completion Date:	Completed
Corrective Action:	Beginning with the FY 19 Annual Report, DBM has included in its instructions to State Agencies that Agencies are required report agreements with Maryland community colleges that exceed \$100,000 and to submit such agreements that exceed \$500,000 to DBM for approval. Note, DBM has no authority to instruct those same community colleges to report to DBM, as we do with State of Maryland higher education institutions. For this reason, various data in the annual report may be missing for these agreements.		

Auditor’s Comment: In its response, DBM notes that budget language cannot compel non-State institutions (that is, public community colleges) to report interagency agreements to DBM. This is irrelevant to the finding which addresses the requirement for *State agencies* to report interagency agreements with local community colleges. State agency agreements with community colleges are exempt from State procurement laws and, accordingly, should be appropriately monitored.

**Department of Budget and Management
Office of the Secretary and Other Units
Response to Legislative Audits Findings and Recommendations
October 2019**

Motor Vehicle Fleet

Finding 14

DBM lacked documented justification for excluding certain vehicle types from its annual review of vehicle usage. In addition, DBM's cost assessments of the need for an agency to retain vehicles when they were not driven the minimum annual miles without adequate justification were not properly calculated.

We recommend that DBM

- a. document its justification for excluding certain vehicle types from its annual review of vehicle usage;
- b. based on the vehicle types to be reviewed, include all vehicles of that type in its review; and
- c. use appropriate cost data for each vehicle type when performing its breakeven assessments.

Agency Response			
Analysis			
General Comment:	<p>The current policy and procedures is written to allow flexibility so that all vehicle types are not required to be included in the 10,000 mile review. It is difficult to specify each type of vehicle for which this review is not applicable, especially since this could change over time. Thus, the current written procedures allow this flexibility while also allowing us the ability to internally make those decisions of which vehicles should not be subject to this review. For example, it has been DBM's practice to not include police vehicles in mileage requirements of the general fleet. DBM will consider including additional vehicle categories in the 10,000 mile review.</p> <p>DBM believes that it does not make sense to require certain vehicles, particularly larger and specific use vehicles, be justified by mileage. In many instances, these vehicles are required for job performance irrespective of number of official miles driven annually.</p>		
Recommendation 14a	Agree	Estimated Completion Date:	January 2020
Corrective Action:	DBM agrees to maintain written justification, to be updated annually, for why certain vehicle types are not included in the annual review of vehicle usage.		
Recommendation 14b	Agree	Estimated Completion Date:	November 2019
Corrective Action:	For 2019, DBM's review will include all vehicles of each vehicle type that is determined to be reviewed.		
Recommendation 14c	Agree	Estimated Completion Date:	Completed
Corrective Action:	For 2018, DBM calculated a breakeven for three vehicle types and re-evaluated processes to determine the best approach to conduct both the 10,000 mile review and breakeven analysis for 2018. For example, certain vehicle types were defined into categories for analysis purposes. We will consider adding additional categories, or groupings, in future years where such reviews are feasible and would provide benefit to the State.		

AUDIT TEAM

Michael J. Murdzak, CPA
Audit Manager

Richard L. Carter, CISA
R. Brendan Coffey, CPA, CISA
Information Systems Audit Managers

Catherine M. Clarke, CPA, CIA, CFE
Senior Auditor

Edward O. Kendall
Information Systems Senior Auditor

Matusala Y. Abishe
Patrick J. Cavanaugh
Stephanie A. Laciny
Staff Auditors

Roman J. Gouin
Information Systems Staff Auditor