Audit Report

Office of the Public Defender

August 2021

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

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

August 10, 2021

Senator Clarence K. Lam, M.D., Senate Chair, Joint Audit and Evaluation Committee
Delegate Carol L. Krimm, 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 Office of the Public Defender (OPD) for the period beginning September 23, 2016 and ending June 30, 2020. We also reviewed and substantiated two allegations received on our fraud, waste and abuse hotline related to the procurement of information technology services from one vendor and questionable charges by a panel attorney providing legal services. OPD is primarily responsible for providing legal services to eligible indigent individuals charged with violating State, county, or municipal laws involving possible incarceration.

Our audit disclosed various issues related to the procurement and monitoring of information technology (IT) contracts. Specifically, OPD did not comply with State procurement laws and regulations when awarding two sole source IT contracts with expenditures totaling $960,000 during fiscal years 2018 through 2020. For example, OPD awarded a one-year sole-source contract totaling $288,000 to a vendor for IT advisory services without a sole-source justification. We were advised that this vendor was selected based on a cursory internet search, several telephone interviews, and a meeting with the vendor awarded the contract. In addition, this vendor's initial contract as well as 19 contract modifications, totaling $850,000 from May 2018 to December 2020, were not approved by the Department of General Services or the Board of Public Works, as required.

Furthermore, OPD advised that it ultimately concluded no deliverables were met for the IT vendor who was paid $1.8 million during our audit period and was

responsible for the day-to-day operations of the OPD's IT department. These deliverables included ensuring that IT systems were secure and maintained. We were unable to determine if the lack of these deliverables was related to IT security problems at OPD; however, we noted that between January 2017 and March 2020, OPD experienced three significant information technology hardware failures that resulted in OPD permanently losing access to critical data and a ransomware attack. In addition, OPD had not yet fully implemented 3 of 10 recommendations to improve IT security issued by the Department of Information Technology on May 15, 2020. DoIT's recommendations were based upon its investigation of an information technology security incident which resulted in the ransomware attack that was experienced by OPD during March 2020.

We also noted that OPD lacked comprehensive procedures to ensure the propriety of panel attorney (PA) invoices, and when questionable billings were identified, OPD did not expand its review and initiate collection actions. OPD's review of PA invoices did not include a process to determine the reasonableness of hours charged per day by PA; therefore, OPD was unable to readily determine instances when it was billed for excessive or duplicate hours. OPD retains PAs to handle cases when a conflict of interest arises, such as when OPD is already representing a codefendant.

In fiscal year 2019, OPD management identified certain questionable charges on invoices from one PA and hired a forensic accountant to perform a review of that individual PA's billings. OPD did not seek reimbursement for any questionable payments identified by the forensic accountant and did not expand its review to other payments to this PA. Our expanded review disclosed additional questionable charges valued at approximately $47,000.

Finally, our audit included a review to determine the status of two of the three findings contained in our preceding audit report. We determined that OPD satisfactorily addressed these findings.

OPD's response to this audit is included as an appendix to this report. In accordance with State law, we have reviewed the response and noted that although OPD disagrees with certain information in this report, the corrective actions identified are sufficient to address all audit issues. In accordance with generally accepted government auditing standards, we have included an "auditor comment" within OPD's response to explain our position.

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

Respectfully submitted,

Gregory A. Hook, CPA
Legislative Auditor

Table of Contents

Background Information

Agency Responsibilities

The Office of the Public Defender (OPD) is primarily responsible for providing legal services to eligible indigent individuals charged with violating State, county, or municipal laws involving possible incarceration. Legal representation is provided in criminal and juvenile proceedings, post-conviction proceedings, probation and parole revocations, involuntary commitments to public or private institutions, and termination of parental rights proceedings. OPD provides these services through a central headquarters and 44 offices located in 12 districts throughout the State.

According to the State's records, during fiscal year 2020, OPD had 888.5 authorized positions and operating expenditures totaled approximately $117.8 million, primarily for salaries, wages, and fringe benefits. According to its annual report for fiscal year 2020, OPD opened approximately 151,000 and 185,000 new cases during calendar years 2019 and 2018, respectively.

OPD has a 13-member Board of Trustees with 11 members appointed by the Governor with the advice and consent of the Senate, one member selected by the Senate President, and one member selected by the Speaker of the House. The Board reviews the administration of OPD, advises the Public Defender on its operations, coordinates the activities of district advisory boards, and consults on certain matters such as fees.

Law Change

As noted in our previous audit, Chapter 606, Laws of Maryland 2017, effective October 1, 2017, transferred the responsibility for determining eligibility for most OPD services to the Judiciary. As a result, individuals charged with a crime that carries a penalty of incarceration apply to a district court commissioner, rather than OPD to obtain the services of a public defender. OPD retained the responsibility for determining eligibility for juvenile proceedings, post-conviction proceedings, probation and parole revocations, involuntary commitments to public or private institutions, and termination of parental rights proceedings. The law leaves in place long-standing criteria for determining indigency for eligibility purposes.

The procedures and controls over eligibility determinations made after October 1, 2017 were audited during our audit of the Judiciary. Eligibility determinations

from the beginning of our audit period, September 23, 2016, through September 30, 2017 were subject to review during our current OPD audit.

Ransomware Security Incident

In March 2020, OPD experienced a broad security incident which resulted in a ransomware attack[1]. This incident affected the entire OPD computer network and disrupted IT operations for all OPD servers and end user computers. After the onset of this incident, OPD notified the Department of Information Technology's (DoIT) Office of Security Management, which initiated incident response measures for OPD.

The DoIT response and investigation included extensive incident analysis work, which concluded on May 5, 2020. DoIT made ten recommendations for improving OPD's overall IT security environment. For OPD, a multi-phase IT recovery effort occurred, which extended from early April to completion at the end of June 2020. OPD's business operations were substantially impacted by this security incident; however, its impact was significantly lessened by the fact that the IT recovery period coincided with a Courts pandemic shutdown period of March 16, 2020 to June 5, 2020. Based on our review, direct unplanned monetary expenses arising from this incident were nominal and no ransom was paid on this incident.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of two of the three findings contained in our preceding audit report dated January 11, 2018. As disclosed in Figure 1 below, we determined that OPD satisfactorily addressed these two findings and the status of the final finding was addressed during our audit of the Judiciary and a similar condition was included in the Judiciary audit report dated April 7, 2021.

[1] As defined by the Federal Department of Homeland Security Cybersecurity and Infrastructure Security Agency, ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

Figure 1
Status of Preceding Findings

Preceding Finding	Finding Description	Implementation Status
Finding 1	The Office of the Public Defender (OPD) did not ensure that applications for legal representation were always adequately supported and maintained on file, and that eligibility determinations were subject to supervisory review as required.	Not Repeated – Status assessed during Judiciary audit during which a similar condition was noted
Finding 2	OPD did not ensure that administrative fees were assessed to all applicable clients.	Not Repeated
Finding 3	OPD has not implemented a formal process to determine whether existing attorney caseload standards should be revised. Average attorney caseloads for Circuit and District Courts continue to exceed current standards.	Not Repeated

Findings and Recommendations

Information Systems Procurement and Monitoring

Background

The Office of the Public Defender (OPD) has a centralized Information Technology Division (ITD) that is responsible for office-wide technology planning, acquisition, policies, connectivity, and support for a broad portfolio of infrastructure and applications. A staff of 12 ITD employees supervised by the OPD Chief Information Officer, provide information technology (IT) asset management and help desk support to approximately 1,100 users (including OPD employees and others such as law students) in 45 locations throughout the State in their use of laptop, desktop, and mission-critical applications. In addition, OPD has contracted out IT application services and infrastructure support since June 2015, which is collectively referred to as enterprise support. OPD made payments totaling approximately $1.8 million to this Enterprise Support Services (ESS) vendor during the audit period.

In November 2017, OPD hired a consultant to perform an independent assessment of OPD's IT environment. Upon receipt of the consultant's report, OPD contracted with an IT advisory services vendor in February 2018 to address the deficiencies noted in the report and to provide IT application services and infrastructure support.

As previously mentioned in the Background Information section of this report, OPD experienced a significant IT security incident in March 2020. Subsequently, in September 2020, the Department of Information Technology (DoIT) began to provide certain IT support services to OPD, which include:

- cybersecurity services (including firewall and intrusion detection prevention systems operations and maintenance)
- remote access service
- vulnerability scanning service

Various OPD offices and the headquarters site utilize a statewide network, maintained by DoIT, which provides OPD users' access to various IT services including a significant case management system, network and email services, and internet access.

We received a referral to our fraud, waste, and abuse hotline regarding concerns with OPD's procurement of IT application services and infrastructure support from one vendor. As a result, we reviewed the procurement of this vendor's

contract and a second vendor's contract for IT services. In addition, we reviewed OPD's procedures for monitoring its IT contracts. Based on our review, we were able to substantiate the concerns raised in the allegation. However, the results of our review of the allegation did not identify any issues that warranted a referral to the Office of the Attorney General – Criminal Division.

Finding 1
OPD did not comply with State procurement laws and regulations when awarding two sole source IT contracts with expenditures totaling $960,000.

Analysis
OPD did not comply with State procurement laws and regulations when awarding two sole source IT contracts with expenditures totaling approximately $960,000 during fiscal years 2018 through 2020. In November 2017, OPD hired a consultant via a sole source contract for $19,800 to perform an independent assessment of OPD's IT environment. The consultant identified numerous areas for OPD to address, such as outdated software and the lack of comprehensive IT program management, and recommended that OPD obtain an IT advisory services vendor to address these deficiencies. OPD subsequently awarded a one-year contract totaling $288,000 to a different vendor for these advisory services in February 2018, with later modifications of $850,000 bringing the total contract value to $1,138,000, and had paid $939,000 as of June 2020.

Our review disclosed that for both of these procurements, OPD did not justify the use of a sole source procurement and did not publish the solicitations or the award of the advisory services contract on *eMaryland Marketplace* (*eMM*)[2], as required by State regulations. We were advised that the selection of the vendor to assess IT needs was done based on the recommendation of an OPD executive management employee, and the selection of the vendor for advisory services was done based on a cursory internet search, several telephone interviews, and a meeting with the vendor awarded the contract.

In addition, for the advisory services contract, neither the initial contract nor any of the 19 contract modifications totaling $850,000 for the period from May 2018 to December 2020 were approved by the Department of General Services (DGS) or the Board of Public Works (BPW), as required. The purpose of these modifications was to extend the initial contract term and for additional work that was not included in the scope of the original contract. For example, one modification for $158,000 was to provide project management services for the implementation of OPD's new case management system.

[2] *eMM* is an internet-based, interactive procurement system managed by DGS. Effective July 2019, DGS replaced *eMM* with *eMaryland Marketplace Advantage (eMMA).*

State procurement regulations provide that sole source procurements should only be used when goods or services are available from only a single vendor, and require that written justifications be prepared and approved prior to the contract award. When competitive procurements are used, two responsive bids are required for procurements exceeding $5,000. State procurement regulations also provide that procurements of information technology contracts of less than $200,000 require DGS approval and contracts over $200,000 require BPW approval. In addition, State procurement regulations provide that contract modifications less than $50,000 require DGS approval and modifications for more than $50,000 require BPW approval.

Finally, State procurement regulations require the solicitation of contracts greater than $15,000 to be published on *eMM* and State procurement laws and regulations require awards for contracts greater than $50,000 (greater than $25,000 prior to October 1, 2017) to be published on *eMM*. Publishing awards on *eMM* provides transparency over State procurements, including information about winning bidders and the amounts of the related awards.

Recommendation 1
We recommend that OPD comply with State procurement regulations when contracting for information technology services. Specifically, we recommend that OPD

a. use the sole source procurement method only when a single vendor can meet the requirements, and adequately document this justification;
b. ensure that publication of solicitations and awards of contracts on *eMMA* is in accordance with State regulations; and
c. submit contracts and contract modifications, including as appropriate those noted above, to DGS and/or BPW for review and approval, as required.

Finding 2
OPD's procedures for monitoring two IT contracts did not ensure that certain deliverables were provided and tasks were performed.

Analysis
OPD's procedures for monitoring two IT contracts (including the advisory services vendor mentioned in Finding 1) with payments totaling $2.7 million during our audit period did not ensure that certain deliverables were provided and tasks were performed. From January 2017 through March 2020, OPD experienced three significant information technology hardware failures and, as previously mentioned, a ransomware attack.

OPD failed to adequately monitor its ESS contract

OPD did not adequately monitor its ESS contract to ensure the adequacy and comprehensiveness of service and that certain deliverables were provided and tasks were performed. Such deliverables included ensuring that IT systems were secure and maintained, developing network diagrams, performing long-term planning, and providing IT training. OPD acknowledged that no deliverables were met in relation to this contract[3] and did not initiate action to obtain these deliverables until the ESS contract employee acting as the system network engineer tendered his resignation in August 2019.

In addition, the contract did not include certain details as to the specific tasks to be provided, for example, the nature and frequency of IT training. The contract also did not specify a dollar amount to be charged for the aforementioned deliverables/tasks, but rather only specified an hourly rate for two IT specialists (Senior Network Support Resource and Senior Database Support Resource). The lack of sufficient details and specific dollar amounts to be charged precluded us from quantifying the value of deliverables/tasks that were not provided.

Despite OPD not implementing comprehensive performance monitoring and the lack of receipt of certain deliverables, OPD continued to renew the ESS vendor's contract through May 31, 2020. Specifically, OPD provided the ESS vendor with three continuous one-year renewals between 2017 and 2020 by describing the services provided as exemplary, before ultimately canceling the contract effective December 2019.

OPD could not adequately document that contracted IT advisory services were provided and monitored

OPD did not retain adequate documentation that IT advisory services were provided and monitored. Specifically, in response to the performance issues with the ESS vendor identified by the independent consultant, OPD contracted with an IT advisory services vendor to obtain IT leadership services and to develop an IT strategy. The contract included a number of tasks to be provided, and we were advised that these services were provided and that OPD's monitoring consisted of periodic meetings with the vendor to discuss the status of ongoing operations. Although OPD obtained timesheets for certain services, we noted that descriptions of the work performed did not match the aforementioned tasks, and accordingly OPD had no documentation that these services were provided in accordance with the contract, such as the IT strategy that was to be developed,

[3] The lack of deliverables being met was included in a justification prepared by OPD in October 2020 to the Department of General Services when seeking retroactive approval from the Board of Public Works for the sole source procurement of the IT ESS advisory services contract (as discussed in Finding 1). We noted that retroactive BPW approval was obtained.

and lacked adequate evidence of the periodic meetings, such as, meeting minutes, frequency, and attendees. OPD payments for this contract totaled approximately $939,000 from February 2018 to June 2020.

The lack of comprehensive monitoring of the vendors' performance could be significant because according to OPD management personnel, with the exception of asset management and help desk support, the vendors were responsible for IT operations management at OPD. Furthermore, although we were unable to determine if the lack of these deliverables was a direct or related cause, between January 2017 and March 2020, OPD experienced three significant IT hardware failures that resulted in OPD permanently losing access to critical data and a ransomware attack on March 25, 2020.

Recommendation 2
We recommend that OPD establish procedures to ensure that all IT contract deliverables/tasks are identified and received.

Finding 3
OPD had not fully implemented three of ten recommendations issued by DoIT based upon its investigation of the IT security incident experienced during March 2020.

Analysis
OPD had not fully implemented three of ten recommendations which were issued by DoIT on May 15, 2020 that were based upon its investigation of the IT security incident experienced during March 2020. As discussed under the Ransomware Attack Incident heading in the Background Information section of this report, DoIT made these recommendations based on extensive analysis work performed during its investigation of the security incident that resulted in the ransomware attack.

Our review disclosed approximately one year after the previously noted security incident (and ten months after DoIT's report) that OPD continued its efforts to finish implementation of the three remaining IT security-related recommendations issued by DoIT. Specifically, as of March 23, 2021, OPD had partially completed actions on these recommendations which involved creating and implementing policies for IT risk management and software updating, and also conducting a periodic IT security risk assessment. For developing and maintaining a secure IT environment, the State of Maryland *Information Technology Security Manual* defines mandated IT security practices and requirements for Maryland agencies. These requirements include management security controls, with risk management

included as the control process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

Recommendation 3
We recommend that OPD continue its efforts and ensure the timely and complete implementation of the three outstanding DoIT security recommendations arising from the 2020 IT security incident.

Panel Attorney Payments

Background
OPD retains panel attorneys (PAs) to handle cases when a conflict of interest arises, such as when OPD is already representing a codefendant. While PAs frequently worked on multiple cases simultaneously, invoices were submitted for each individual case upon the conclusion of the case, which may last months or years. According to State records, expenditures related to PA billings totaled approximately $9.5 million in fiscal year 2020.

We received a referral to our fraud, waste, and abuse hotline related to questionable charges by one PA. Based on this allegation, we reviewed OPD's procedures for monitoring PA charges and performed an extended review of payments made to the PA referenced in the allegation. Based on our review, we were able to substantiate the concerns raised in the allegation.

Finding 4
OPD lacked comprehensive procedures to ensure the propriety of PA invoices. In addition, OPD lacked documentation that the payments for certain PA services that exceeded the maximum rate were properly authorized.

Analysis
OPD lacked comprehensive procedures to ensure the propriety of PA invoices and, when questionable billings were identified, OPD did not expand its review and initiate collection actions, when appropriate. In addition, OPD could not document that payments for services that exceeded the maximum rate allowed by State regulations were properly authorized, and OPD paid certain invoices that were not submitted timely.

<u>PA Invoice Review Process Deficiencies</u>
OPD's review of PA invoices did not include a comprehensive process to routinely determine the reasonableness of hours charged per day by PA and

therefore, OPD was unable to readily determine instances when it was billed for excessive or duplicate hours. Rather, OPD generally assessed the total number of hours billed by task on a case for reasonableness and made adjustments accordingly, but did not consider the daily hours worked and billed by a specific PA.

In fiscal year 2019, OPD management identified certain questionable charges on invoices from one PA and hired a forensic accountant to perform a review of that individual PA's billings for the period from May 29, 2015 to April 15, 2019. The resultant report determined that the PA billed OPD for more than 20 hours on 42 different days, including 21 days for which 24 hours or more were billed. The report did not estimate the value of the questionable payments; however, based on OPD's lowest reimbursable rate at the time, we estimated that the questionable charges for more than 20 hours billed in one day on the 42 different days, totaled at least $9,150.

While OPD subsequently referred this issue to the Office of the Attorney General – Criminal Division and the Attorney Grievance Commission, OPD did not seek reimbursement for any questionable payments made and did not expand its review to other payments to this PA or the PA's firm beyond the period of the forensic audit. A referral to the Criminal Division does not mean that a criminal act has actually occurred or that criminal charges will be filed.

We performed an extended review of 170 payments totaling approximately $245,000 made to this PA's law firm during the period from January 4, 2019 through July 24, 2019, including all payments made by OPD after the forensic audit report was received on May 31, 2019. Our test disclosed that this PA billed and was paid for more than 20 hours on 40 different days, including one day for which the attorney was paid for 49.5 hours. We also noted 25 cases that were billed and paid twice, and 2 cases that were billed and paid three times. In total, the additional questionable charges that we identified were valued at approximately $47,000.

Payments of Excessive or Untimely PA Invoices

OPD paid, through normal invoice processing, PAs for amounts in excess of the maximum amount allowed and paid invoices that were not submitted timely. Our test of nine payments totaling approximately $242,000 that included payments in excess of the amount allowed per case disclosed that OPD lacked documented justification from the Public Defender for seven of these payments totaling approximately $179,000. In addition, two payments totaling approximately $53,000 were not requested within 60 days as required, including one payment totaling approximately $32,000 submitted 47 months late.

State regulations establish maximum fees for panel attorneys based on the type of court case (such as $11,500 for a Circuit Court case in fiscal year 2020), and allow for additional fees to be paid when authorized by the Public Defender. State regulations also require panel attorneys to submit reimbursement requests within 60 days of the case disposition date.

Recommendation 4
We recommend that OPD

a. **establish comprehensive procedures to verify the propriety of PA invoices including a mechanism to review daily hours billed by specific PAs over all cases, amounts paid are within the allowable amounts, and that invoices are only paid when they are submitted in accordance with the timeframe established in regulations; and**
b. **expand its review when questionable billings are identified, including those noted above, and take appropriate action, such as seeking reimbursement for inappropriate payments or referring the matter to the Office of the Attorney General.**

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the Office of the Public Defender (OPD) for the period beginning September 23, 2016 and ending June 30, 2020. 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 OPD'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 budgeting, procurements and disbursements, and payroll. Furthermore, we reviewed the procurement and monitoring of information technology services and the monitoring of charges by panel attorneys regarding referrals received on our fraud, waste, and abuse hotline. We also determined the status of the findings contained in our preceding audit report.

Our assessment of internal controls was based on agency procedures and controls in place at the time of our fieldwork. Our tests of transactions and other auditing procedures were generally focused on the transactions occurring during our audit period of September 23, 2016 to June 30, 2020, but may include transactions before or after this period as we considered necessary to achieve our audit objectives.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, tests of transactions and to the extent practicable, observations of OPD's operations. Generally, transactions were selected for testing based on auditor judgment, which primarily considers risk, the timing or dollar amount of the transaction, or the significance of the transaction to the area of operation reviewed. As a matter of course, we do not normally use sampling in our tests, so unless otherwise specifically indicated, neither statistical nor non-statistical audit sampling was used to select the transactions tested. Therefore, unless sampling is specifically indicated in a finding, the results from any tests conducted or disclosed by us 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 revenue and expenditure data) and the State's Central Payroll Bureau (payroll data). These 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. Finally, we performed other auditing procedures that we considered necessary to achieve our audit objectives. The reliability of data used in this report for background or informational purposes was not assessed.

OPD'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. As provided in *Government Auditing Standards*, there are five components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring. Each of the five components, when significant to the audit objectives, and as applicable to OPD, were considered by us during the course of this audit.

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 OPD'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 OPD that did not warrant inclusion in this report.

OPD'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 OPD regarding the results of our review of its response.

APPENDIX

MARYLAND OFFICE OF THE PUBLIC DEFENDER

PAUL DEWOLFE
PUBLIC DEFENDER

August 6, 2021

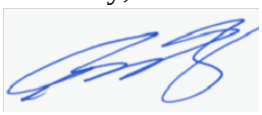
Via email: response@ola.state.md.us
Mr. Gregory A. Hook, CPA, Legislative Auditor
301 W. Preston Street #1202
Baltimore MD 21201

Dear Mr. Hook,

Enclosed please find our Agency Response form.

Should you have any questions, please do not hesitate to contact our office.

Sincerely,



Paul DeWolfe

Office of the Public Defender

Agency Response Form

Information Systems Procurement and Monitoring

Finding 1
OPD did not comply with State procurement laws and regulations when awarding two sole source IT contracts with expenditures totaling $960,000.

We recommend that OPD comply with State procurement regulations when contracting for information technology services. Specifically, we recommend that OPD

a. use the sole source procurement method only when a single vendor can meet the requirements, and adequately document this justification;

b. ensure that publication of solicitations and awards of contracts on *eMMA* is in accordance with State regulations**; and**

c. submit contracts and contract modifications, including as appropriate those noted above, to DGS and/or BPW for review and approval, as required.

Agency Response			
Analysis			
Please provide additional comments as deemed necessary.			
Recommendation 1a	Agree	**Estimated Completion Date:**	7/1/2021
Please provide details of corrective action or explain disagreement.	Management will use the sole source procurement method only when a single vendor can meet the requirements, and adequately document the justification for its use.		
Recommendation 1b	Agree	**Estimated Completion Date:**	7/1/2021
Please provide details of corrective action or explain disagreement.	Management will ensure that publication of solicitations and awards of contracts on *eMMA* is in accordance with State regulations		
Recommendation 1c	Agree	**Estimated Completion Date:**	7/1/2021
Please provide details of corrective action or explain disagreement.	Management will submit contracts and contract modifications to DGS and/or BPW for review and approval, as required. The subject contract was approved by BPW on 6/17/21.		

Office of the Public Defender

Agency Response Form

Finding 2
OPD's procedures for monitoring two IT contracts did not ensure that certain deliverables were provided and tasks were performed.

We recommend that OPD establish procedures to ensure that all IT contract deliverables/tasks are identified and received.

Agency Response	
Analysis	
Please provide additional comments as deemed necessary.	The IT Advisory Services cited in the finding amounted to $288,000, not the amount stated.

Auditor's Comment: The OPD response purports that the effect of the cited lack of contract monitoring was limited to the $288,000 initial contract amount, but it incorrectly ignores the cost of the subsequent contract modifications, which had brought contract payment totals to $939,000 (at the time of the report). Nevertheless, in accordance with the audit report recommendation, OPD has agreed to establish procedures to ensure that all IT contract deliverables/tasks are identified and received.

Recommendation 2	Agree	**Estimated Completion Date:**	1/1/2020
Please provide details of corrective action or explain disagreement.	OPD established procedures to ensure that all IT contract deliverables/tasks are identified and received, effective with our new IT management that started at OPD in October 2019.		

Office of the Public Defender

Agency Response Form

Finding 3
OPD had not fully implemented three of ten recommendations issued by DoIT based upon its investigation of the IT security incident experienced during March 2020.

We recommend that OPD continue its efforts and ensure the timely and complete implementation of the three outstanding DoIT security recommendations arising from the 2020 IT security incident.

Agency Response			
Analysis			
Please provide additional comments as deemed necessary.			
Recommendation 3	Agree	**Estimated Completion Date:**	12/31/2021
Please provide details of corrective action or explain disagreement.	OPD is actively working to complete the last three recommendations. The patch management policy is being documented and the matrix for risk management is being finalized. Once the risk assessment is completed, the recommended policy will be developed.		

Office of the Public Defender

Agency Response Form

Panel Attorney Payments

Finding 4
OPD lacked comprehensive procedures to ensure the propriety of PA invoices. In addition, OPD lacked documentation that the payments for certain PA services that exceeded the maximum rate were properly authorized.

We recommend that OPD

a. establish comprehensive procedures to verify the propriety of PA invoices including a mechanism to review daily hours billed by specific PAs over all cases, amounts paid are within the allowable amounts, and that invoices are only paid when they are submitted in accordance with the timeframe established in regulations; and

b. expand its review when questionable billings are identified, including those noted above, and take appropriate action, such as seeking reimbursement for inappropriate payments or referring the matter to the Office of the Attorney General.

Agency Response			
Analysis			
Please provide additional comments as deemed necessary.			
Recommendation 4a	Agree	**Estimated Completion Date:**	7/1/2021
Please provide details of corrective action or explain disagreement.	OPD management has established procedures to verify the propriety of PA invoices including a mechanism to review daily hours billed by specific PAs over all cases, amounts paid are within the allowable amounts, and that invoices are only paid when they are submitted in accordance with the timeframe established in regulations, including: • Effective July 1, 2021, invoices must be submitted within 60 days of the final action, as required by Regulations. Exceptions will be documented. • OPD Fiscal will conduct quarterly reviews of PA activity to determine exceptions to daily hours across cases that warrant detailed review and follow up. • Reasons for payments that exceed allowable amounts will be documented.		
Recommendation 4b	Agree	**Estimated Completion Date:**	7/1/2021

Office of the Public Defender

Agency Response Form

Please provide details of corrective action or explain disagreement.	When questionable billings are identified, OPD will expand its review and take appropriate action, including seeking reimbursement for inappropriate payments or referring the matter to the Office of the Attorney General. In this case, the PA has threatened OPD with legal action, regarding our request for reimbursement of certain payments.

AUDIT TEAM

Heather A. Warriner, CPA
Audit Manager

R. Brendan Coffey, CPA, CISA
Information Systems Audit Manager

Julia M. King
Joseph E. McWilliams, CFE
Senior Auditors

Edward O. Kendall, CISA
Information Systems Senior Auditor

Thea A. Chimento, CFE
Ibijoke O. Owolabi, CPA
Gary B. Staples
Staff Auditors

Charles O. Price
Information Systems Staff Auditor