OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued April 11, 2025

Berkshire County District Attorney's Office

For the period July 1, 2021 through June 30, 2023

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

April 11, 2025

Timothy J. Shugrue, District Attorney
Berkshire County District Attorney's Office
7 North Street
Pittsfield, MA 01201

Dear District Attorney Shugrue:

I am pleased to provide to you the results of the enclosed performance audit of the Berkshire County District Attorney's Office. As is typically the case, this report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2021 through June 30, 2023. As you know, my audit team discussed the contents of this report with agency managers. This report reflects those comments.

I appreciate you and all your efforts at the Berkshire County District Attorney's Office. The cooperation and assistance provided to my staff during the audit went a long way toward a smooth process. Thank you for encouraging and making available your team. I am available to discuss this audit if you or your team has any questions.

Best regards,

Diana DiZoglio
Auditor of the Commonwealth

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of the Berkshire County District Attorney's Office (BCDA) for the period of July 1, 2021 through June 30, 2023.

The purpose of our audit was to determine the following:

- whether BCDA ensured that forfeited assets were collected, deposited, and distributed in accordance with Section 47(d) of Chapter 94C of the General Laws and BCDA's internal "Forfeited Property Procedures";
- whether all BCDA employees received cybersecurity awareness training in accordance with cybersecurity awareness training requirements included in Sections 6.2.3 and 6.2.4 of the Executive Office of Technology Services and Security's Information Security Risk Management Standard IS.010; and
- whether BCDA updated its internal control plan to include all the critical components of enterprise risk management as well as monitoring controls, as recommended in our prior audit.

Below is a summary of our findings, the effects of those findings, and our recommendations, with links to each page listed.

Finding 1 **Page 9**	BCDA did not ensure that all forfeited assets from cases were documented or deposited properly.
Effect	By not signing receipts or deposit slips for the received forfeited funds or documenting any associated police department funds BCDA held, BCDA may not be able to ensure the accuracy and transparency of accounting of the received funds. This could result in discrepancies and disputes about the total amount of funds that are being deposited and distributed to the associated police departments. By not depositing forfeited funds in a timely manner, BCDA made it so that it and local police departments did not have access to this funding—for an extended time–to which they were entitled, which could have been used to defray the costs of investigations, equipment, federal grant matching applications, drug rehabilitation and education, or for other purposes deemed appropriate by the District Attorney or local police department.

Recommendations Page 10	1. BCDA should establish controls to ensure that it promptly receives and distributes forfeited funds. 2. BCDA should ensure that it prepares and signs receipts for received forfeited funds. These receipts should document any funds owed to the police department associated with the case as evidence of verifying and certifying the received forfeited funds. 3. BCDA should ensure that, for all forfeiture cases, deposit slips are signed by the chief of appeals as proof that the funds were received and deposited.
Finding 2 Page 11	BCDA did not provide its employees with cybersecurity awareness training.
Effect	Without educating its employees on their responsibility to protect the security of information assets, BCDA exposes itself to a higher risk of cybersecurity attacks and financial and/or reputational losses.
Recommendations Page 12	1. BCDA should develop, document, and implement policies and procedures that require employees to complete cybersecurity awareness training within 30 days of their orientation and annually thereafter. 2. BCDA should ensure that it provides and documents cybersecurity awareness training for its employees.
Finding 3 Page 12	BCDA did not update its internal control plan to include all the critical components of enterprise risk management, as recommended in our prior audit.
Effect	Without updating its internal control plan, BCDA may not identify and/or mitigate all risks that could prevent it from accomplishing its objectives.
Recommendation Page 13	BCDA should establish policies and procedures to ensure that its internal control plan is updated annually and when significant changes occur.

OVERVIEW OF AUDITED ENTITY

The Berkshire County District Attorney's Office (BCDA) was established under Sections 12 and 13 of Chapter 12 of the Massachusetts General Laws, which provide for the administration of criminal law and the defense of civil actions brought against a public employer or employee of the Commonwealth in accordance with Chapter 258 of the General Laws.

BCDA is one of 11 district attorneys' offices in the Commonwealth and serves the 32 cities and towns in Berkshire County. BCDA represents the Commonwealth in criminal cases in the Berkshire Superior Court, three district courts, three juvenile courts, an Appeals Court, and a Supreme Judicial Court. BCDA has two offices, one in Pittsfield and one in North Adams.

According to BCDA's website,

> *The Berkshire District Attorney's Office is unequivocally committed to:*
>
> - *Delivering equal justice for all residents of Berkshire County regardless of national origin, race, color, religion, disability, sex, gender identify, sexual orientation and familial status.*
> - *Involving the community through proactive programs that educate citizens and help individuals avoid criminal involvement including statutory diversion programs like drugs, mental health, and veterans programs.*
> - *Prosecuting those that harm our community including career criminals, gang members, individuals possessing illegal firearms, drug traffickers, and perpetrators of domestic violence.*
> - *Fighting for justice on behalf of those victimized by sex crimes, domestic violence, exploitation, and child abuse.*
> - *Partnering with law enforcement [in this case, police departments], social services, and the public to promote aggressive crime-prevention strategies.*
> - *Advocating for local businesses that have been victims of theft and larceny.*

During fiscal years 2022 and 2023, BCDA had 62 and 81 employees, respectively, and received state appropriations of $5,379,412 and $5,486,974, respectively.

Asset Forfeiture

Section 47 of Chapter 94C of the General Laws authorizes the Commonwealth to seize property including, but not limited to, monetary proceeds traceable to the exchange of a controlled substance or the equipment or vehicles associated with the manufacturing or distribution of controlled substances.

Per BCDA's "Forfeited Property Procedures," funds and/or property which are seized as possible asset forfeitures are to be kept secure by the police department responsible for the seizure. For funds and/or property seized by the Massachusetts State Police or the Berkshire Narcotic Unit, the funds may be held in evidence lockers or in an account set up by the State Police or by BCDA's director of fiscal affairs.

The assistant district attorneys are required to review all drug-related cases to determine whether any assets were seized that are subject to forfeiture and to contact the evidence officer at the police department to verify the amount seized. When BCDA receives a forfeiture order, the assistant district attorney is required to provide copies of the order to both the director of fiscal affairs and the chief of appeals.[1] When BCDA receives the funds from the police departments, a receipt of the funds received is required to be prepared and signed before the funds can be deposited. The chief of appeals is required to verify that BCDA has received and deposited all forfeited funds by signing off on all deposit slips.

Per Section 47 of Chapter 94C of the General Laws, all funds seized are to be divided equally between the prosecuting district attorney and the police department that performed the seizure. If more than one police department was involved in the seizure, then the police departments split their 50% share equitably. Per BCDA policy, the funds can be split between BCDA and the police department at the time BCDA receives the funds or distributed at a later date. If the funds are to be distributed at a later date, all of the funds received are to be deposited by BCDA and documented on the receipt, per BCDA's "Forfeited Property Procedures." Additionally, when the funds are later distributed, a letter detailing the distribution of funds is to be attached to the order and receipt.

During the audit period, BCDA processed $300,672 in forfeited funds and retained $218,677 in forfeited asset revenue; these funds are to remain in BCDA's forfeiture trust fund account with the Office of the State Treasurer and Receiver General until expended. According to Section 47(d) of Chapter 94C of the General Laws,

> *[Forfeiture funds are allowed to] be expended without further appropriation to defray the costs of protracted investigations, to provide additional technical equipment or expertise, to provide matching funds to obtain federal grants, or such other law enforcement purposes as the district attorney or attorney general deems appropriate.*

1. The responsibilities of the chief of appeals include overseeing matters related to post-conviction litigation. The chief of appeals also has oversight over appeals filed by either defendants or the Commonwealth.

This law also allows BCDA to use up to 10% of the forfeiture funds for drug rehabilitation, drug education, and neighborhood crime-watch programs.

Cybersecurity Awareness Training

The National Institute of Standards and Technology recommends that organizations provide system users with literacy training that should include an understanding of the need for security and privacy, how to respond to suspected security incidents, and how to handle personally identifiable information.

Additionally, Section 6.2 of the Executive Office of Technology Services and Security's Information Security Risk Management Standard IS.010 states,

> *The objective of the Commonwealth information security training is to educate users on their responsibility to help protect the confidentiality, availability, and integrity of the Commonwealth's information assets. Commonwealth Agencies and Offices must ensure that all personnel are trained on all relevant rules and regulations for cybersecurity.*

Internal Control Plan

The Office of the Comptroller of the Commonwealth has developed the *Internal Control Guide*, which is based on the Committee of Sponsoring Organizations' Enterprise Risk Management Framework and the Standards for Internal Control. The role of the guide is to assist governmental entities with the design, documentation, and implementation of internal controls. The guide includes an internal control plan checklist that government entities, including BCDA, should follow to ensure compliance.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of certain activities of the Berkshire County District Attorney's Office (BCDA) for the period July 1, 2021 through June 30, 2023.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Below is a list of our audit objectives, indicating each question we intended our audit to answer; the conclusion we reached regarding each objective; and, if applicable, where each objective is discussed in the audit findings.

Objective	Conclusion
1. Did BCDA ensure that forfeited assets were collected, deposited, and distributed in accordance with Section 47(d) of Chapter 94C of the General Laws and BCDA's internal "Forfeited Property Procedures"?	**No; see Finding 1**
2. Did all BCDA employees receive training in accordance with cybersecurity awareness training requirements included in Sections 6.2.3 and 6.2.4 of the Executive Office of Technology Services and Security's Information Security Risk Standard IS0.010?	**No; see Finding 2**
3. Did BCDA update its internal control plan to include all the critical components of enterprise risk management as well as monitoring controls, in response to our previous recommendation from Audit No. 2018-1261-11J?	**No; see Finding 3**

To accomplish our audit objectives, we gained an understanding of the aspects of BCDA's internal control environment relevant to our objectives by reviewing applicable policies, procedures, and the internal control plan and by interviewing BCDA officials. We evaluated the design and implementation and tested the operating effectiveness of internal controls related to the verification of the forfeited amount, approvals of receipt of funds and deposit slips related asset forfeitures. In addition, to obtain sufficient, appropriate evidence to address our audit objectives, we performed the procedures described below.

Asset Forfeiture

To determine whether BCDA ensured that forfeited assets were collected, deposited, and distributed in accordance with Section 47(d) of Chapter 94C of the General Laws and BCDA's "Forfeited Property Procedures," we took the following actions. We obtained a list of 17 asset forfeitures processed by BCDA during the audit period. For each listed forfeiture, we reviewed relevant case documentation (including court forfeiture orders, seized fund receipts, forfeiture split calculation memorandums, checks, deposit slips, bank statements, and email communications) to determine the following:

- whether each forfeiture case contained a forfeiture order;
- whether each case had a receipt of funds received on file that was prepared and signed by a BCDA official;
- whether the deposit slips were signed by the chief of appeals as proof that the funds were received and deposited;
- whether BCDA documented whether it retained any portion of the forfeited funds owed to the police department;
- whether a distribution letter was created that documented the distributions between BCDA and any associated police departments;
- whether any of the funds BCDA retained may be owed to the associated police department;
- whether the distributed amounts followed Section 47(d) of Chapter 94C of the General Laws (50% to BCDA, with the remaining 50% going to any associated police departments; and
- whether all forfeiture case funds were deposited within 30 business days (which we reviewed by calculating the number of business days between the court order and the date of the receipt of funds).

See Finding 1 for more information regarding the results of our testing related to whether BCDA ensured that forfeited assets were collected, deposited, and distributed properly.

Cybersecurity Awareness Training

To determine whether BCDA employees received cybersecurity awareness training in accordance with Sections 6.2.3 and 6.2.4 the Executive Office of Technology Services and Security's Information Security Risk Management Standard IS.010, we interviewed a BCDA official to discuss whether BCDA had established a cybersecurity awareness training program for its employees.

See Finding 2 for more information regarding the results of our testing related to cybersecurity awareness training.

Internal Control Plan

To determine whether BCDA updated its internal control plan to include all the critical components of enterprise risk management as recommended in our previous audit, we interviewed a BCDA official and reviewed the internal control plan in effect during the audit period, which was dated April 1, 2016.

See Finding 3 for more information regarding the results of our testing related to BCDA's updating its internal control plan as recommended in our previous audit.

Data Reliability Assessment

To determine the reliability of the list of forfeited funds that BCDA received, which was provided to us by BCDA, we tested the list to ensure that there were no duplicates or missing data and that all of the data corresponded to dates from within the audit period. We selected a random sample of five forfeiture cases from the list and matched the docket numbers, deposit date, police department involved, and amount forfeited to the corresponding data on the forfeiture orders and fund receipts. We judgmentally[2] selected a sample of five forfeiture cases from BCDA's physical files and matched the docket number, deposit date, and forfeited amount on the forfeiture orders and fund receipts to the information recorded in the list of forfeited funds. Further, we reviewed the monthly bank statements for BCDA's forfeiture account and reviewed each deposit to determine whether the deposits were for forfeited funds. For all deposits determined to be related to a forfeiture, we ensured that they were on the list of forfeited funds provided by BCDA.

Based on the results of the data reliability assessment procedures described above, we determined that the information we obtained was sufficiently reliable for the purposes of our audit.

2. Auditors use judgmental sampling to select items for audit testing when a population is very small, the population items are not similar enough, or there are specific items in the population that the auditors want to review. Auditors use their knowledge and judgment to select the most appropriate sample. For example, an auditor might select items from areas of high risk. The results of testing using judgmental sampling cannot be used to make conclusions or projections about entire populations; however, they can be used to identify specific issues, risks, or weaknesses.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Berkshire County District Attorney's Office did not ensure that all forfeited assets from cases were documented or deposited properly.

During the audit period, the Berkshire County District Attorney's Office (BCDA) did not prepare receipts to be signed by BCDA officials for 7 out of the 17 forfeiture cases (41%) processed. Further, it did not ensure that deposit slips were signed by the chief of appeals as proof that the funds were received and deposited for all 16 forfeiture cases[3] for which BCDA physically received forfeited funds. Additionally, there were 3 cases for which BCDA did not document the portion of the forfeited funds owed to the police department that BCDA retained.

During our prior audit of BCDA (Audit No. 2018-1261-11J), we found that some forfeited funds were not deposited by BCDA until up to 780 days after cases were disposed of. In our current audit, we reviewed the entire population of 17 forfeitures, totaling $300,672, and found that 15 forfeitures (88%), totaling $198,592, had been ordered by court motions but were not deposited by BCDA as required until 55 to 377 days after they were ordered by a court.

By not signing receipts or deposit slips for the received forfeited funds or documenting any associated police department funds BCDA held, BCDA may not be able to ensure the accuracy and transparency of accounting of the received funds. This could result in discrepancies and disputes about the total amount of funds that are being deposited and distributed to the associated police departments. By not depositing forfeited funds in a timely manner, BCDA made it so that it and local police departments did not have access to this funding—for an extended time–to which they were entitled, which could have been used to defray the costs of investigations, equipment, federal grant matching applications, drug rehabilitation and education, or for other purposes deemed appropriate by the District Attorney or local police department.

Authoritative Guidance

BCDA's "Forfeited Property Procedures" states,

> *When the funds are received from the police, a receipt must be signed before the funds are deposited and attached to the copy of the forfeiture order. . . . If the police share of funds is to be*

3. For one forfeiture case, the local police department deposited the funds directly into BCDA's account within the Massachusetts Management Accounting and Reporting System, the official accounting system for Commonwealth business.

distributed at a later date, all funds received will be deposited and that information will be noted on receipt.

The Chief of Appeals will verify all funds have been received and deposited by regularly signing off on all deposit slips.

BCDA's internal control plan states that "it is the responsibility of the Chief of Appeals to determine why funds are not deposited in a timely manner."

Reasons for Issue

During a meeting with the District Attorney, it was stated that the audit period occurred before his administration and that, when he took over, there were no proper policies and procedures over the forfeiture process other than the policies that had been put in place in 2016.

Recommendations

1. BCDA should establish controls to ensure that it promptly receives and distributes forfeited funds.
2. BCDA should ensure that it prepares and signs receipts for received forfeited funds. These receipts should document any funds owed to the police department associated with the case as evidence of verifying and certifying the received forfeited funds.
3. BCDA should ensure that, for all forfeiture cases, deposit slips are signed by the chief of appeals as proof that the funds were received and deposited.

Auditee's Response

In its response to this audit report, BCDA provided background information regarding the audit period. See the Appendix for this background information.

The [BCDA] has developed a Forfeited Property Policy included in both the Internal Control Plan and the Procedures and Forms Manual that is an addendum to the Employee Handbook (all dated April 1, 2024). These controls outline the procedures for identifying assets that could potentially be subject to forfeiture at the outset of proceedings and require notation in the office case management system. The procedures outline the process for the documentation required for the receipt and disbursement of forfeited funds. The audit findings recommend the Chief of Appeals sign all deposit slips as proof of receipt of hinds, but the [BCDA] has designed the First Assistant as the person who will receive a copy of all forfeiture orders and will verify funds have been received in a timely manner, deposited and distributed. The policy also requires regular review of reports developed from the case management system to identify potential forfeitures and ensure the policies have been followed in securing these assets.

Auditor's Reply

Based on its response, BCDA is taking measures to address our concerns regarding this matter. As part of our post-audit review process, we will follow up on this matter in approximately six months.

2. The Berkshire County District Attorney's Office did not provide its employees with cybersecurity awareness training.

BCDA did not provide cybersecurity awareness training to its employees during the audit period. Additionally, the agency did not have any policy to require that this training be administered to its staff members.

Without educating its employees on their responsibility to protect the security of information assets, BCDA exposes itself to a higher risk of cybersecurity attacks and financial and/or reputational losses.

Authoritative Guidance

The National Institute of Standards and Technology's "Special Publication 800-53r5, Security and Privacy Controls for Information Systems and Organizations," states,

> *AT-2 LITERACY TRAINING AND AWARENESS . . .*
>
> *a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):*
>
> *1. As part of initial training for new users and . . . [organization-defined frequency] thereafter.*

Section 6.2 of the Executive Office of Technology Services and Security's Information Security Risk Management Standard IS.010 states,

> *6.2.3 New Hire Security Awareness Training: All new personnel must complete an Initial Security Awareness Training course. This course will be conducted via web-based learning or in-class training and will be included in the new hire orientation checklist. The New Hire Security Awareness course must be completed within 30 days of new hire orientation.*
>
> *6.2.4 Annual Security Awareness Training: All personnel are required to complete Annual Security Awareness Training. Once implemented, automatic email reminders will be sent to personnel 12 months after course completion, alerting personnel to annual refresher training completion deadlines.*

Although BCDA is not required to follow these standards, we consider them best practices.

Reasons for Issue

The District Attorney stated that policies related to cybersecurity awareness training were not in place when he started his administration.

Recommendations

1. BCDA should develop, document, and implement policies and procedures that require employees to complete cybersecurity awareness training within 30 days of their orientation and annually thereafter.

2. BCDA should ensure that it provides and documents cybersecurity awareness training for its employees.

Auditee's Response

The [BCDA] current administration was unaware of any requirement from the previous administration administering cybersecurity awareness training. The [BCDA] under the current administration has contracted to use a cybersecurity training system known as "KnowB4". The [BCDA] now requires cybersecurity awareness training to be completed as part of the onboarding process and as an annual requirement for all staff. The training must be completed within 30 days of hire and then renewed annually for all staff. Additionally, the Chief of Information Technology also performs random screenings to ensure compliance. Compliance for initial and annual completion of the KnowB4 training is monitored by the Chief of Information Technology. In addition to the KnowB4 training, the Employee Handbook [newly implemented by the current BCDA administration] outlines procedures for Fraud Prevention, Computer Viruses, Network Security, and provides staff with the standards known as "WISP" (Written Information Security Program) for the protection of personal information.

Auditor's Reply

Based on its response, BCDA is taking measures to address our concerns regarding this matter. As part of our post-audit review process, we will follow up on this matter in approximately six months.

3. The Berkshire County District Attorney's Office did not update its internal control plan to include all the critical components of enterprise risk management, as recommended in our prior audit.

During our prior audit of BCDA (Audit No. 2018-1261-11J), we found that the agency's internal control plan had not been updated since 2016. Further, we found that BCDA's internal control plan did not comply with the Office of the Comptroller of the Commonwealth's *Internal Control Guide*. We recommended that BCDA should immediately update its internal control plan to include all the critical components of enterprise risk management. Further, we recommended that BCDA should establish policies and

procedures for annually updating its internal control plan, as well as monitoring controls to ensure that these policies and procedures are adhered to.

BCDA did not update its internal control plan as required by the Office of the Comptroller of the Commonwealth's *Internal Control Guide* during this report's audit period either. BCDA's last published internal control plan was created on April 1, 2016.

An internal control plan identifies objectives and risks and identifies control activities to mitigate risks that may prevent an agency from accomplishing its public mission. Without updating its internal control plan, BCDA may not identify and/or mitigate all risks that could prevent it from accomplishing its objectives.

Authoritative Guidance

The Office of the Comptroller of the Commonwealth's *Internal Control Guide* states,

> *Your department is obligated to review and update your Internal Control Plan on an annual basis, as well as whenever there is a new objective, risk, or management structure. . . .*
>
> *An internal control plan should have a statement of awareness and compliance with [the Massachusetts General Laws'] Chapter 647 guidelines in addition to the [Committee of Sponsoring Organizations' eight Enterprise Risk Management Framework] components.*

Reasons for Issue

Even though there was an appointed internal control officer during the audit period, in an email dated February 4, 2025, a BCDA official stated,

> *Prior to taking office . . . [District Attorney] Shugrue requested copies of all policies, but we have been unable to find any documentation or reference to an internal control plan and can only assume the previous administration used the old 2016 Plan for procedural guidance.*

Recommendation

BCDA should establish policies and procedures to ensure that its internal control plan is updated annually and when significant changes occur.

Auditee's Response

> *When I [Timothy J. Shugrue, District Attorney] assumed Office, I was made aware that there was no written Internal Control Plan in place other than the 2016 version. Completing an Internal Control Plan was a priority. I immediately initiated the process towards completing said plan. This was an extensive task and, upon further investigation, it was uncovered that there was not an*

active Employee Handbook or Policies and Procedures Manual. These had to be developed in conjunction with the Internal Control Plan as they set out the policies that met the requirements of internal controls and addressed issues unique to the management of the [BCDA]. My Office worked with the Quality Assurance Bureau of the Office of the Comptroller's Office to guarantee the Plan was following all applicable rules, regulations, and statutes. The final Plan was issued April 1, 2024, to all staff and contains a requirement that it be reviewed on a regular basis for any needed modifications. The Plan must contain the effective date of the Plan and any modifications and be distributed annually to all staff. The Internal Control Officer as well as an Internal Control Committee described in the Plan are responsible for this task.

Auditor's Reply

Based on its response, BCDA is taking measures to address our concerns regarding this matter. As part of our post-audit review process, we will follow up on this matter in approximately six months.

APPENDIX

District Attorney Timothy J. Shugrue's Response to This Audit Report

In its response to this audit report, the Berkshire County District Attorney's Office (BCDA) provided the following background information regarding the audit period.

I [Timothy J. Shugrue, District Attorney] first want to thank Auditor DiZoglio and her staff for responding to my request for an audit and for the thorough and timely review.

[BCDA] agrees with the findings and deficiencies that occurred in this audit period. As noted, the audit review examines the period between July 1, 2021 to June 30, 2023. My administration was responsible for only the last six months of the audit period, having taken over January 4, 2023.

At the start of my administration, January 4, 2023, I requested an audit. Upon entering Office, I immediately reviewed the policies and procedures and Internal Controls of the Office. Based on all material provided to me at the start of my administration, I discovered that the policies and procedures and Internal Controls had not been updated since 2016 despite the April 2019 audit findings. This means that none of the audit findings from the April 2019 audit had been remedied in during the prior administration's tenure.

It appears, based on the information provided to me, that no update had been made to the policies and procedures since 2016. The April 2019 audit noted deficiencies related to forfeiture procedures. The April 2019 audit noted that an annual update to the Internal Controls was required. Based on material and information I was provided with, neither of these findings were adjudicated.

Updating the policies and procedures and completing an annual Internal Control review was a massive undertaking that could not fully be completed within the first six-month period of my administration. However, I immediately took steps to begin updating the policies and procedures and completing an Internal Control review. The [BCDA]'s current personnel policies and procedures and updated Internal Control Procedures took effect April 1, 2024. These identify and correct the concerns and deficiencies noted in the current audit.