OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued November 16, 2023

Plymouth County District Attorney's Office

For the period July 1, 2019 through June 30, 2021

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

November 16, 2023

District Attorney Timothy J. Cruz
Plymouth County District Attorney's Office
166 Main Street
Brockton, MA 02301

Dear District Attorney Cruz:

I am pleased to provide to you the results of the enclosed performance audit of the Plymouth 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, 2019 through June 30, 2021. 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 Plymouth 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 have any questions.

Best regards,

Diana DiZoglio

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 certain activities of the Plymouth County District Attorney's Office (PCDA) for the period July 1, 2019 through June 30, 2021.

The purpose of our audit was to determine the following:

- whether PCDA made forfeiture trust fund expenditures in accordance with Section 47(d) of Chapter 94C of the General Laws;
- whether PCDA ensured that forfeited assets from closed cases were collected, deposited, and distributed in accordance with Section 47(d) of Chapter 94C of the General Laws; and
- whether PCDA ensured that its employees completed cybersecurity awareness training in accordance with 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.

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

Finding 1 **Page 8**	PCDA underpaid the Brockton Police Department by $6,638.
Recommendation **Page 9**	PCDA should ensure that it accurately distributes forfeited assets to police departments.
Finding 2 **Page 9**	PCDA did not provide cybersecurity awareness training to its employees.
Recommendations **Page 10**	1. PCDA should provide cybersecurity awareness training to its employees. 2. PCDA should develop and implement policies and procedures that require employees to complete cybersecurity awareness training within 30 days of their orientation and annually thereafter.

OVERVIEW OF AUDITED ENTITY

The Plymouth County District Attorney's Office (PCDA) 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 the Commonwealth in accordance with Chapter 258 of the General Laws.

PCDA is one of 11 district attorneys' offices in the Commonwealth and represents the Commonwealth in the prosecution of criminal offenses that occur within its jurisdiction. PCDA serves the 27 cities and towns within Plymouth County.

According to its internal control plan,

> *The mission of [PCDA] is to protect the citizens of our community with the efficient and fair prosecution of criminal acts that occur in the cities and towns of Plymouth County. Along with the prosecution of crime, we strive to provide critical services to the victims of those crimes, and work to reduce criminal activity through intervention and prevention programs.*

PCDA's main administrative office is at 166 Main Street in Brockton. As of December 31, 2020, PCDA had 117 employees, including the District Attorney.

Asset Forfeiture

To prevent individuals from profiting from illegal drug activity, Section 47 of Chapter 94C of the General Laws authorizes law enforcement to seize assets, such as any profits of drug distribution or any property that is used, or was intended to be used, for illegal drug activity. Some examples of assets that may be subject to forfeiture are money, cell phones, computers, motor vehicles, and real property.[1]

The local or state police department that performed the seizure brings the seized assets to PCDA, where they are held in a safety deposit box at a local bank until a judge determines whether these assets should be forfeited to the Commonwealth. If the assets are ultimately deemed forfeited by a court order, then these assets are divided equally between PCDA and the police department that performed the seizure and then moved to and held in forfeiture trust fund accounts. If more than one police department was involved in the seizure, then the police departments split a 50% share equitably.

1. Real property (as opposed to personal property) includes land and additional structures/items in or on that land, such as buildings, sheds, or crops.

According to Section 47(d) of Chapter 94C of the General Laws, PCDA may expend money from the forfeiture trust fund for the following purposes:

> *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 . . . deems appropriate. The district attorney . . . may expend up to ten percent of the monies and proceeds for drug rehabilitation, drug education and other anti-drug or neighborhood crime watch programs which further law enforcement purposes.*

PCDA's forfeited asset revenue was $569,911 during the audit period. PCDA's forfeiture trust fund expenditures totaled $287,763 during the audit period. Forfeited asset revenue remains in PCDA's forfeiture trust fund account with the Office of the State Treasurer and Receiver General until expended, as required by Section 47(d) of Chapter 94C of the General Laws.

Cybersecurity Awareness Training

The Executive Office of Technology Services and Security (EOTSS) has established policies and procedures that apply to all Commonwealth agencies within the executive branch. EOTSS recommends, but does not require, non-executive branch agencies to follow these policies and procedures. Section 6.2 of EOTSS'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 Offices and Agencies must ensure that all personnel are trained on all relevant rules and regulations for cybersecurity.*

To ensure that employees are clear on their responsibilities, all employees in executive branch agencies with access to a Commonwealth-provided email address are required to complete a cybersecurity awareness course every year. All newly hired employees must complete an initial cybersecurity awareness training course within 30 days after their orientation.

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 Plymouth County District Attorney's Office (PCDA) for the period July 1, 2019 through June 30, 2021.

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 PCDA make forfeiture trust fund expenditures in accordance with Section 47(d) of Chapter 94C of the General Laws?	**Yes**
2. Did PCDA ensure that forfeited assets from closed cases were collected, deposited, and distributed in accordance with Section 47(d) of Chapter 94C of the General Laws?	**No; see Finding 1**
3. Did PCDA ensure that its employees completed cybersecurity awareness training in accordance with 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?	**No; see Finding 2**

To achieve our audit objectives, we gained an understanding of PCDA's internal control environment related to the objectives by reviewing applicable policies and procedures and interviewing PCDA officials. We evaluated the design and tested the operating effectiveness of internal controls related to the approval of forfeiture trust fund expenditures, the verification of amounts of seized assets received from police departments, and the approval of forfeited asset distribution calculations.

To obtain sufficient, appropriate audit evidence to address our audit objectives, we performed the following procedures.

Forfeiture Trust Fund Expenditures

To determine whether PCDA made forfeiture trust fund expenditures in compliance with Section 47(d) of Chapter 94C of the General Laws, we performed the following procedures.

PCDA provided us with a list of 277 forfeiture trust fund expenditures (totaling $287,763) that were made during the audit period. We then separated these expenditures into two groups. The first group comprised expenditures that were greater than or equal to $10,000, and the second group comprised expenditures that were less than $10,000. We selected all 4 expenditures (totaling $104,135) with amounts greater than $10,000. We then selected a random, nonstatistical sample of 35 expenditures (totaling $26,613) from the remaining population of expenditures that were less than $10,000 (totaling $183,628). This gave us a total sample size of 39 expenditures.

We reviewed supporting documentation (invoices, purchase orders, requests for expense reimbursement, check requests, emails, canceled checks, and bank statements) for our sample of 39 expenditures to determine whether each expenditure was supported by documentation and was allowable under Section 47(d) of Chapter 94C of the General Laws.

We used nonstatistical sampling methods for testing and therefore did not project the results of our testing to any population.

We noted no exceptions in our testing; therefore, we conclude that PCDA made the forfeiture trust fund expenditures that we sampled in accordance with Section 47(d) of Chapter 94C of the General Laws.

Forfeited Assets from Closed Cases

To determine whether PCDA ensured that forfeited assets from closed cases were collected, deposited, and distributed in compliance with Section 47(d) of Chapter 94C of the General Laws, we performed the following procedures.

PCDA provided us with a list of all 236 forfeited assets (totaling $569,911) that it received during the audit period. We then separated these forfeited assets into two groups. The first group comprised forfeited assets that were greater than or equal to $20,000, and the second group comprised forfeited assets that were less than $20,000. We selected all 5 forfeited assets (totaling $230,106) that were greater than $20,000 for testing. We then selected a random, nonstatistical sample of 20 forfeited assets

(totaling $22,716) from the remaining population of forfeited assets that were less than $20,000 for testing. This gave us a total sample size of 25 forfeited assets.

We reviewed relevant case documentation for each forfeited asset tested (such as any seized fund receipts, forfeiture orders from court, forfeiture split calculations, police reports, checks, deposit slips, bank statements, or emails) to determine whether PCDA (1) collected and deposited the correct amount of forfeited assets and (2) distributed the correct amount of forfeited assets to the police department(s) involved in the seizure.

We used nonstatistical sampling methods for testing and therefore did not project the results of our testing to any population.

See Finding 1 for an issue we identified with PCDA's forfeited asset distribution.

Cybersecurity Awareness Training

To determine whether PCDA employees completed cybersecurity awareness training in accordance with Information Security Risk Management Standard IS.010 issued by the Executive Office of Technology Services and Security, we interviewed PCDA's chief financial officer, information technology director, and human resources generalist to discuss whether PCDA had established a cybersecurity awareness training program for its employees.

See Finding 2 for an issue we identified regarding PCDA's cybersecurity awareness training.

Data Reliability Assessment

Forfeiture Trust Fund Expenditures

To determine the reliability of the list of forfeiture trust fund expenditures, we checked the list for invalid and duplicate records. We also checked the list for dates outside of our audit period. To test for accuracy, we randomly selected a sample of 20 expenditures from this list and compared expenditure dates and amounts to copies of checks, invoices, and payment requests. To test for completeness, we selected a judgmental sample of 20 invoices / payment requests from PCDA's files and compared expenditure information on each invoice and/or payment request to the corresponding expenditures recorded on the list, including dates of expenditures, expense classifications, and expenditure amounts.

Forfeited Assets from Closed Cases

All forfeited assets from closed cases result from initial seizures of those assets. Given this, we reviewed a list of seizures provided by PCDA to determine the completeness and accuracy of the list of forfeited assets.

To determine the reliability of the list of seizures, we checked the list for invalid and duplicate records. We also checked the list for dates outside of our audit period. To test for accuracy, we randomly selected a sample of 20 seizures from the list. We compared the date and amount of the seizure, receipt number, and the police department involved in the seizure to copies of seized fund receipts and police reports. To test for completeness, we selected a judgmental sample of 20 seized fund receipts from PCDA's files. We compared seizure information on the receipts to the information recorded on the list of seizures, including dates, monetary amounts of seizures, and police department(s) involved in the seizures.

To determine the reliability of the list of forfeited assets, we checked the list for invalid and duplicate records. We also checked the list for dates outside of our audit period. To test for accuracy, we randomly selected a sample of 20 forfeitures from the list and compared the date and amount of the forfeitures to information recorded in the court orders. To test for completeness, we selected a judgmental sample of 20 court orders from PCDA's files. We compared information in the court orders to the information recorded on the list of forfeited assets, including dates and amounts of forfeited assets, the monetary amounts distributed to police departments, and the police departments involved in the cases.

Based on the data reliability procedures described above, we determined that the data obtained for our audit period were sufficiently reliable for the purposes of our audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Plymouth County District Attorney's Office underpaid the Brockton Police Department by $6,638.

During the audit period, the Plymouth County District Attorney's Office (PCDA) underpaid the Brockton Police Department by $6,638. When reviewing the forfeited asset splits for the 25 forfeiture cases that we examined, we found 4 cases where PCDA had received 80% of the forfeited assets, distributing only 20% to the police department involved in the seizure. The forfeited assets should have been split equally between PCDA and the police department. The Brockton Police Department, with assistance from the Massachusetts State Police Gang Unit,[2] was the agency involved in the seizures for these 4 cases.[3] We then reviewed the remaining 14 cases in our population that involved both the Massachusetts State Police Gang Unit and the Brockton Police Department and found that in all 14 of these cases, the forfeited assets were distributed using the same 80% and 20% split.

We identified 18 total cases, totaling $22,126, which should have been split equally between PCDA and the Brockton Police Department ($11,063 each). However, PCDA received $17,701 and the Brockton Police Department received $4,425; therefore, the Brockton Police Department was underpaid by $6,638.

If police departments do not receive all of the forfeited assets to which they are entitled, they cannot use the associated revenue for law enforcement needs such as training and equipment.

Authoritative Guidance

Section 47(d) of Chapter 94C of the Massachusetts General Laws states,

> *The final order of the court shall provide that [forfeited assets] and the proceeds of any such sale shall be distributed equally between the prosecuting district attorney . . . and the city, town or state police department involved in the seizure. If more than one department was substantially involved in the seizure, the court having jurisdiction over the forfeiture proceeding shall distribute the fifty percent equitably among these departments.*

2. The Massachusetts State Police Gang Unit investigates gang-related crimes and patrols in high-crime areas. The unit works with the Brockton Police Department to monitor and prevent gang-related activity in Brockton.
3. The Massachusetts State Police Gang Unit assisted the Brockton Police Department during all of these cases; however, the funds were distributed to just the Brockton Police Department.

Reasons for Noncompliance

PCDA management told us that they received 80% of forfeited assets and the Brockton Police Department received 20% because of an agreement the two agencies made several decades ago.[4] PCDA management told us that the district attorney, the police department, and the gang unit made the agreement because PCDA provides operational support (such as supplies, equipment, and training) to the Massachusetts State Police Gang Unit, which assisted the Brockton Police Department.

Recommendation

PCDA should ensure that it accurately distributes forfeited assets to police departments.

Auditee's Response

Historically, there has been an agreement in place between the Plymouth County District Attorney's Office, the Massachusetts State Police Gang Unit and the Brockton Police Department that when the latter two agencies work together on a case, the Plymouth County District Attorney's Office would retain the Gang Unit's entire share of funds. This agreement was put in place so that the Plymouth County District Attorney's Office could support the Gang Unit investigations as needed consistent with the statutory provisions, including that forfeiture funds may be used for "other law enforcement purposes."

Going forward the Plymouth County District Attorney's Office will request, in each Gang Unit case, a memorandum to establish the degree of involvement of each participating Department in order to have the equitable share appropriately ordered by the Court and distributed to the participating departments for Gang Unit seizures.

Auditor's Reply

Based on its response, PCDA is taking measures to address our concerns in this area.

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

PCDA did not provide cybersecurity awareness training to its employees during the audit period.

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

4. In our last audit (No. 2017-1265-3J) of PCDA, we examined PCDA's activities related to its Diversion Program and Victim Assistance Program. We were therefore not aware of this agreement until the audit outlined in this report.

Authoritative Guidance

Section 6.2 of the Executive Office of Technology Services and Security's (EOTSS'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. . . . 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 will be required to complete Annual Security Awareness Training.*

Although PCDA is not required to follow this standard, we consider it a best practice.

Reasons for Noncompliance

PCDA did not have policies and procedures that require new employees to complete cybersecurity awareness training within 30 days of their orientation or that require employees to receive annual cybersecurity awareness training.

Recommendations

1. PCDA should provide cybersecurity awareness training to its employees.
2. PCDA should develop and implement policies and procedures that require employees to complete cybersecurity awareness training within 30 days of their orientation and annually thereafter.

Auditee's Response

> *As stated above and confirmed by the EOTSS General Counsel/Chief Privacy Officer, . . . our agency was not required to follow the EOTSS policy for annual cybersecurity training during the audit period.*
>
> *During the audit period, we followed the [Performance and Career Enhancement (PACE) Learning Management System] training schedule established by the Commonwealth for employees to complete within 90 days of hire. Cyber Security training was not offered as part of the PACE trainings.*
>
> *Cyber Security training is currently offered via MassAchieve which we do not currently or have ever had access to. As of January 2022, we have required all employees to complete cybersecurity awareness training annually via KnowBe4, an Automated Security Awareness Program which we pay for.*
>
> *Giving all departments access to MassAchieve seems the most cost-effective way for every state employee to be trained.*

Auditor's Reply

PCDA is correct in stating that it is not required to follow EOTSS's Information Security Risk Management Standard IS.010. However, this policy represents what the Commonwealth considers a best practice for protecting information when conducting business on behalf of Massachusetts. According to the Office of the Comptroller of the Commonwealth's website, EOTSS's Enterprise Information Security Policies and Standards "are the default standard for non-Executive Departments who have not adopted comparable cyber and data security standards as part of their Internal Control Plan."

Based on its response, PCDA is taking steps to address this issue. We urge PCDA to fully implement our recommendations.