OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued September 30, 2024

Bristol County District Attorney's Office

For the period July 1, 2020 through June 30, 2022

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

September 30, 2024

District Attorney Thomas M. Quinn III
Bristol County District Attorney's Office
218 South Main Street, Suite 101
Fall River, MA 02721

Dear District Attorney Quinn:

I am pleased to provide to you the results of the enclosed performance audit of the Bristol 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, 2020 through June 30, 2022. 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 Bristol 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
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 Bristol County District Attorney's Office (BCDA) for the period July 1, 2020 through June 30, 2022.

The purpose of our audit was to determine the following:

- whether BCDA made forfeiture trust fund expenditures in accordance with Section 47(d) of Chapter 94C of the General Laws;
- whether BCDA 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 BCDA 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 finding, the effect of that finding, and our recommendations, with links to each page listed.

Finding 1 **Page 10**	BCDA did not provide cybersecurity awareness training to its employees.
Effect	If BCDA does not educate its employees on their responsibility to protect the security of information assets, then BCDA exposes itself to a higher-than-acceptable risk of cybersecurity attacks and financial and/or reputational losses.
Recommendations **Page 11**	1. BCDA should provide cybersecurity awareness training to its employees. 2. 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.

OVERVIEW OF AUDITED ENTITY

The Bristol 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 the Commonwealth in accordance with Chapter 258 of the General Laws.

BCDA 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. BCDA serves the 20 cities and towns within Bristol County.

According to its internal control plan, "The Bristol County District Attorney's Office main mission is mandated by law. We represent the Commonwealth of Massachusetts in the prosecution of criminal acts that occur within Bristol County."

BCDA's main administrative office is located at 218 South Main Street in Fall River. As of December 31, 2020, BCDA had 133 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 agencies 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 BCDA, which holds the seized assets in safety deposit boxes at a local bank until a judge determines whether these assets should be forfeited to the Commonwealth. If the seized assets are ultimately deemed forfeited by a court order, then these assets are divided equally between BCDA and the police department that performed the seizure. They are then moved to and held in a forfeiture trust fund. 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, BCDA 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.*

BCDA's forfeited asset revenue was $1,125,345 during the audit period. Forfeited asset revenue remains in BCDA'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. BCDA's forfeiture trust fund expenditures totaled $874,151 during the audit period. BCDA groups forfeiture trust fund expenditures into one of the following two classifications: community grant expenditures, which BCDA disburses to not-for-profit community organizations to further law enforcement purposes, and law enforcement expenditures, which BCDA incurs itself.

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, EOTSS's policies require that all employees in state executive agencies complete a cybersecurity awareness course every year. All newly hired employees must complete an initial security awareness training course within 30 days of 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 Bristol County District Attorney's Office (BCDA) for the period July 1, 2020 through June 30, 2022.

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 make forfeiture trust fund expenditures in accordance with Section 47(d) of Chapter 94C of the General Laws?	**Yes**
2. Did BCDA 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?	**Yes**
3. Did BCDA 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 (EOTSS's) Information Security Risk Management Standard IS.010?	**No; see Finding 1**

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 and procedures and by interviewing BCDA officials. We evaluated the design and tested the operating effectiveness of internal controls related to the approval of forfeited fund expenditures, the review of supporting documents for forfeited fund expenditures, the verification of amounts of seized assets received from law enforcement agencies, and the approval of forfeited asset distribution calculations.

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

Forfeiture Trust Fund Expenditures

To determine whether BCDA made forfeiture trust fund expenditures in accordance with Section 47(d) of Chapter 94C of the General Laws, we took the actions described below.

BCDA provided us with a list of all 555 forfeiture trust fund expenditures (totaling $874,151) that BCDA made during the audit period. We organized these expenditures into two separate groups, according to BCDA's two classifications. The first group comprised community grant expenditures (47 expenditures, totaling $324,136) and the second group comprised law enforcement expenditures (508 expenditures, totaling $550,015). We then divided these 508 law enforcement expenditures (totaling $550,015), as follows:

Law Enforcement Expenditure Description	Number of Expenses	Total
Individual expenditures with values of $10,000 or more	8	$114,557
Individual expenditures with values of less than $10,000	500	$435,458

For the community grant expenditures, we selected a random, nonstatistical sample of 10 community grant expenditures (totaling $92,775) from the population of 47. For the law enforcement expenditures, we first selected all 8 law enforcement expenditures with values of $10,000 or more (totaling $114,557). We then selected a random, nonstatistical sample of 30 law enforcement expenditures with values of less than $10,000 (totaling $33,480) from the remaining population of 500. Finally, we selected an additional, judgmental[2] sample of 42 law enforcement expenditures with values of less than $10,000 (totaling $85,542) from the remaining population of 470. Combined, our total sample comprised 90 expenditures (or 16% of all 555 forfeiture trust fund expenditures), totaling $326,354 (or 37% of the total amount of $874,151).

For each of the expenditures in our sample of 90, we reviewed supporting documentation (i.e., invoices, purchase orders, requests for expense reimbursement, check requests, applications, email correspondence, canceled checks, and bank statements) to determine whether each expenditure was supported by adequate documentation and was allowable under Section 47(d) of Chapter 94C of the

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.

General Laws. Whenever the law enforcement purpose of an expenditure was not self-evident, we asked BCDA management how the expenditure related to a law enforcement purpose. According to Section 47(d) of Chapter 94C of the General Laws:

> *All such monies and proceeds received by any prosecuting district attorney or attorney general shall be deposited in such a trust fund and shall then 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.*

Therefore, District Attorneys have broad discretion, as they deem appropriate, to define expenditures as valid "other law enforcement purposes." BCDA was able to provide sufficient documentation that the District Attorney had done so for the expenditures in our sample.

We noted no exceptions in our testing sample. That being, all expenditures were supported by adequate documentation, and fit within an allowable category by statute, including those for "other law enforcement purposes" deemed appropriate by the District Attorney. Therefore, we concluded that, during the audit period, the forfeiture trust fund expenditures in our sample were made in accordance with Section 47(d) of Chapter 94C of the General Laws.

Forfeited Assets from Closed Cases

To determine whether BCDA 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, we took the actions described below.

BCDA provided us with a list of all 588 forfeited assets from closed cases (totaling $1,285,406) that it received during the audit period. We organized these forfeited assets into two separate groups. The first group comprised forfeited assets with values of $20,000 or more (9 forfeited assets, totaling $446,237). The second group comprised forfeited assets with values less than $20,000, (579 forfeited assets, totaling $839,169).

We selected all 9 of the forfeited assets with values of $20,000 or more (totaling $446,237). We then selected a random, nonstatistical sample of 30 forfeited assets with values less than $20,000 (totaling $60,778) from the remaining population of 579. Combined, our total sample comprised 39 forfeited assets

(or 6.6% of all 588 forfeited assets from closed cases), with a value of $507,015 (or 39.4% of the total amount $1,285,406).

For each of the forfeited assets in our sample of 39, we reviewed relevant case documentation (i.e., any corresponding Confiscated Monies Reports,[3] forfeiture orders from the courts, forfeited asset distribution calculations, police reports, checks, deposit slips, bank statements, or email correspondence) to determine whether BCDA accurately (1) collected and deposited forfeited assets and (2) distributed the forfeited assets to the police department(s) involved in the corresponding seizures.

We noted no exceptions in our testing. Therefore, we concluded that, during the audit period, BCDA 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.

Cybersecurity Awareness Training

To determine whether BCDA ensured that its employees completed cybersecurity awareness training in accordance with Sections 6.2.3 and 6.2.4 of EOTSS's Information Security Risk Management Standard IS.010, we interviewed BCDA's chief financial officer, information technology director, and human resources generalist.

See Finding 1 for an issue we identified regarding BCDA's cybersecurity awareness training.

We used nonstatistical sampling methods for testing and therefore did not project the results of our testing to the corresponding population(s).

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 records, duplicate records, and dates outside of the audit period. To test for accuracy, we randomly selected a sample of 20 expenditures from this list and compared information from this list (i.e., expenditure dates and expenditure amounts) to information on corresponding copies of checks,

3. Confiscated Monies Reports are standardized forms that police departments prepare when processing seized assets. These reports accompany the corresponding police reports and are used to account for and administer seized assets. The BCDA chief financial officer reviews and approves Confiscated Monies Reports upon receipt of the seized assets from the arresting police department. The district attorney's office maintains a copy, which remains with the seized assets.

invoices, and payment requests. To test for completeness, we selected a judgmental sample of 20 invoices and/or payment requests from BCDA's files and compared information on each invoice and/or payment request (i.e., dates of expenditures, expense classifications, and expenditure amounts) to information recorded for the corresponding expenditures on the list.

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 BCDA to determine the completeness and accuracy of the list of forfeited assets from closed cases.

To determine the reliability of the list of seizures, we checked the list for invalid records, duplicate records, and dates outside of the audit period. To test for accuracy, we randomly selected a sample of 20 seizures from the list and compared information from this list (i.e., the date and amount of the seizure, the record number,[4] and the police department involved in the seizure) to information on corresponding copies of seized asset receipts and police reports. To test for completeness, we selected a judgmental sample of 20 seized asset records from BCDA's files and compared information on the receipts (i.e., dates, monetary amounts of seizures, and police department(s) involved in the seizures) to information recorded for the corresponding seizures on the list.

To determine the reliability of the list of forfeited assets, we checked the list for invalid records, duplicate records, and dates outside of the audit period. To test for accuracy, we randomly selected a sample of 20 forfeited assets from the list and compared information from this list (i.e., dates and monetary values of the forfeited assets) to information recorded for the corresponding forfeited assets in the court orders. To test for completeness, we selected a judgmental sample of 20 court orders from BCDA's files and compared information in the court orders (i.e., dates and monetary values of forfeited assets, the police department(s) involved in the cases, and the monetary amounts distributed to the police department(s) involved) to the information recorded for the corresponding forfeited assets on the list.

4. The record number is an internal tracking number that BCDA's forfeited asset database automatically assigns to each case entered by a BCDA employee.

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

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

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

The Bristol County District Attorney's Office (BCDA) did not provide cybersecurity awareness training to its employees during the audit period.

If BCDA does not educate its employees on their responsibility to protect the security of information assets, then BCDA exposes itself to a higher-than-acceptable risk of cybersecurity attacks and financial and/or reputational losses.

Authoritative Guidance

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 BCDA is not required to follow this standard, since it is not an executive branch agency, EOTSS still recommends that non-executive branch agencies follow these standards. We also consider it a best practice. 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." BCDA's internal control plans in effect during our audit period did not contain comparable cyber and data security standards.

Reasons for Noncompliance

BCDA did not have policies and procedures that require newly hired employees to complete cybersecurity awareness training within 30 days of their orientation or that require existing employees to receive annual refresher cybersecurity awareness training.

Recommendations

1. BCDA should provide cybersecurity awareness training to its employees.

2. 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.

Auditee's Response

The [BCDA] agrees that although EOTSS has established policies and procedures for cybersecurity awareness training, non-executive agencies (including the [BCDA]) are not required to follow or implement said policies and procedures.

The [BCDA], nonetheless, has implemented an online cybersecurity awareness training program for all staff beginning in June of 2023. The [BCDA] staff receive quarterly online cybersecurity awareness training, which exceeds the recommendation of EOTSS. All new [BCDA] hires receive an initial security awareness training within 30 days of hire.

Auditor's Reply

Based on its response, BCDA has taken 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.