OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued November 28, 2023

Hampden County District Attorney's Office

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

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Novemeber 28, 2023

District Attorney Anthony D. Gulluni
Hampden County District Attorney's Office
50 State Street
Springfield, MA 01103

Dear District Attorney Gulluni:

I am pleased to provide to you the results of the enclosed performance audit of the Hampden 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 Hampden 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 performed an audit of the Hampden County District Attorney's Office (HCDA) for the period July 1, 2019 through June 30, 2021.

In this performance audit, we examined the following:

- whether HCDA made forfeiture trust fund expenditures in accordance with Section 47(d) of Chapter 94C of the General Laws;
- whether HCDA ensured that forfeited assets from closed cases were collected and deposited in accordance with Section 47(d) of Chapter 94C of the General Laws; and
- whether HCDA 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 and recommendations, with links to each page listed.

Finding 1 **Page 7**	HCDA did not provide cybersecurity awareness training to its employees.
Recommendations **Page 7**	1. HCDA should create a policy and procedure to train new and existing employees on cybersecurity awareness. 2. HCDA should provide cybersecurity awareness training to its employees within 30 days of orientation and annually thereafter.

OVERVIEW OF AUDITED ENTITY

The Hampden County District Attorney's Office (HCDA) 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.

HCDA 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. HCDA serves 23 cities and towns across southwestern Massachusetts and serves a population of about 460,000 citizens. HCDA had a budget of $12,429,625 in fiscal year 2020 and $13,951,535 in fiscal year 2021. HCDA's main office is in Springfield, with satellite locations in Chicopee, Holyoke, Palmer, and Westfield.

According to its website, HCDA "is proud to serve the people of Hampden County by faithfully pursuing criminal justice and ensuring public safety with ethics, integrity, and fairness as [its] guiding values."

HCDA's forfeited asset revenue was $327,446 during the audit period. HCDA's forfeiture trust fund expenditures totaled $497,913 during the audit period. Forfeited asset revenue remains in HCDA'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. The unexpended balance at the end of a fiscal year in the forfeiture trust fund account is rolled forward for the next fiscal year.

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 was 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 maintains possession of the seized assets until a judge determines whether these assets should be forfeited to the Commonwealth. If assets are ultimately deemed forfeited by a court order, then these assets are divided equally between HCDA and the police department that performed the seizure and are moved to and held in a forfeiture trust fund

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.

account. If more than one police department was involved in the seizure, then the police departments split a 50% share equitably.

According to Section 47(d) of Chapter 94C of the General Laws, HCDA 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.*

Cybersecurity Awareness Training

The Executive Office of Technology Services and Security 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 state executive 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 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 Hampden County District Attorney's Office (HCDA) 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. Were expenditures from HCDA's forfeiture trust fund appropriate and in compliance with Section 47(d) of Chapter 94C of the General Laws?	**Yes**
2. Did HCDA ensure that all forfeited assets were collected and deposited in accordance with Section 47(d) of Chapter 94C of the General Laws?	**Yes**
3. Did HCDA 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 1**

To achieve our audit objectives, we gained an understanding of HCDA's internal control environment related to the objectives by reviewing HCDA's policies and procedures and interviewing HCDA staff members and management. We evaluated the design and tested the operating effectiveness of the internal control (specifically, supervisory approval) for forfeited trust fund expenditures.

Forfeiture Trust Fund Expenditures

To determine whether expenditures from HCDA's forfeited trust fund were appropriate and in compliance with Section 47(d) of Chapter 94C of the General Laws, we obtained a list from HCDA of all forfeiture trust

fund expenditures that were made during the audit period. Using TeamMate Analytics,[2] we selected a nonstatistical, random sample of 5 forfeited trust fund expenditures (totaling $7,504) out of a total population of 49 forfeited trust fund expenditures (totaling $497,913) made during the audit period.

We examined supporting documentation (including invoices, bills, and purchase orders) to determine whether each expenditure was supported by documentation and was allowable under Section 47(d) of Chapter 94C of the General Laws.

We noted no exceptions in our testing; therefore, we conclude that HCDA's expenditures from its forfeiture trust fund account were allowable and in compliance with Section 47(d) of Chapter 94C of the General Laws.

Forfeited Assets

To determine whether HCDA ensured that all forfeited assets were accurately collected and deposited in accordance with Section 47(d) of Chapter 94C of the General Laws, we obtained a list of all forfeited assets that HCDA received during the audit period. Using TeamMate Analytics, we selected a nonstatistical, random sample of 33 forfeited assets HCDA received (totaling $16,863) from a population of 499 (totaling $327,446) from the audit period. We examined supporting documentation (including forfeiture orders, checks to and from police departments, deposit slips, bank statements, and forfeiture trust fund account activity) to determine whether forfeited assets were accurately collected and deposited.

We noted no exceptions in our testing; therefore, we conclude that HCDA ensured that all forfeited assets were accurately collected and deposited in accordance with Section 47(d) of Chapter 94C of the General Laws.

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

Cybersecurity Awareness Training

To determine whether HCDA 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, we obtained a list of all employees who worked

2. This is a Microsoft Excel-based data analytics tool that allows auditors to execute advanced data analysis.

for part or all of the audit period. The list contained 190 employees. We interviewed HCDA staff members about cybersecurity awareness training at the agency during the audit period. See Finding 1 for an issue we identified with HCDA's cybersecurity awareness training.

Data Reliability Assessment

In 2018 and 2022, the Office of the State Auditor performed data reliability assessments of the Massachusetts Management Accounting and Reporting System (MMARS). These assessments focused on testing selected system controls, including access, cybersecurity awareness, audit and accountability, configuration management, identification and authentication, and personnel security. In addition, as part of our current audit, we tested the controls in place over HCDA's personnel security.

For the list of forfeited trust fund expenditures, we selected a random sample of five invoices from HCDA's hardcopy files and determined whether the information on the invoices matched the data in MMARS. We also selected a random sample of five forfeited trust fund expenditures from MMARS and traced the information to the invoices. For the list of employees, we selected a random sample of 10 employees from HCDA's personnel files and determined whether the information in the personnel files matched the data in MMARS. We also selected a judgmental sample of 10 employees from MMARS and traced the information to personnel files.

To determine the reliability of the data from the list of all forfeited assets HCDA received for the period July 1, 2019 through June 30, 2021, we traced a sample of 20 forfeited assets from the list to the source documents and selected 20 hardcopy documents to trace back to the list. In addition, we conducted tests to identify any duplicates to determine the integrity of the information in the list.

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

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

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

The Hampden County District Attorney's Office (HCDA) 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, HCDA is exposed to a higher risk of cybersecurity attacks and financial and/or reputational losses.

Authoritative Guidance

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

Reasons for Issue

HCDA 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. HCDA should create a policy and procedure to train new and existing employees on cybersecurity awareness.
2. HCDA should provide cybersecurity awareness training to its employees within 30 days of orientation and annually thereafter.

Auditee's Response

During the audit period, the Hampden District Attorney's Office did not have a specific cybersecurity training program in place. However, all employees were instructed regarding security measures

and how to report breaches of security should they occur. Knowing the importance of having a specific training regimen, this office was in the process of securing cybersecurity awareness training during the audit period.

When the audit was begun in July of 2022, the Hampden District Attorney's Office had a policy and procedure in place for all employees regarding cybersecurity awareness training. This consists of periodic training sessions throughout the year as well as security awareness testing. Therefore, the recommendations resulting from the finding have been implemented.

Auditor's Reply

Based on its response, HCDA has taken measures to address our concerns on this matter.