OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued May 4, 2023

Worcester County District Attorney's Office

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

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

May 4, 2023

District Attorney Joseph D. Early, Jr.
Worcester County District Attorney's Office
225 Main Street
Worcester, MA 01608

Dear District Attorney Early:

I am pleased to provide to you the results of the enclosed performance audit of the Worcester 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 Worcester 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.

Sincerely,

Diana DiZoglio

Diana DiZoglio
Auditor of the Commonwealth

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CFO	chief financial officer
COVID-19	2019 coronavirus
CTR	Office of the Comptroller of the Commonwealth
DAMION	District Attorney Management Information Office Network
EOTSS	Executive Office of Technology Services and Security
ICP	internal control plan
MMARS	Massachusetts Management Accounting and Reporting System
PD	police department
WCDA	Worcester County District Attorney's Office

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 Worcester County District Attorney's Office (WCDA) for the period July 1, 2019 through June 30, 2021. When reviewing updates to its internal control plan (ICP), we examined WCDA's most recent ICP as of the time of our fieldwork, which was dated March 2022.

The purpose of our audit was to determine the following:

- whether forfeited fund expenditures were made in compliance with Section 47(d) of Chapter 94C of the General Laws,
- whether confiscated and forfeited funds[1] were tracked and processed in accordance with WCDA's "Fiscal Policy and Procedures,"
- whether WCDA complied with the Office of the Comptroller of the Commonwealth's guidance by updating its ICP to address risks related to the 2019 coronavirus pandemic, and
- whether WCDA 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.

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

Finding 1 **Page 12**	WCDA did not ensure that its employees completed cybersecurity awareness training.
Recommendations **Page 12**	1. WCDA should ensure that employees complete cybersecurity awareness training within 30 days of their orientation and annually thereafter. 2. WCDA should ensure that its employees are aware of EOTSS requirements.

1. Funds initially seized by law enforcement agencies are considered confiscated until they are ultimately declared forfeited by a court order.

OVERVIEW OF AUDITED ENTITY

The Worcester County District Attorney's Office (WCDA) 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.

WCDA is one of 11 district attorneys' offices throughout the Commonwealth. WCDA serves four cities and 56 towns in central Massachusetts, representing approximately 862,000 residents of the Commonwealth. WCDA represents the Commonwealth at bail hearings, commitment proceedings related to criminal matters, rendition proceedings, and presentations of evidence as part of investigations into whether an individual's death was the result of a crime. WCDA also assists in the investigation of a variety of criminal activities.

WCDA's main administrative office is at 225 Main Street in Worcester. As of June 30, 2021, WCDA had 171 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 any profits of drug distribution or any property that is used, or was intended to be used, for illegal drug activity. Either WCDA or the local or state police department (PD) that performed the seizure holds the funds seized from a defendant until a judge determines whether the funds should be forfeited to the Commonwealth. If funds are ultimately deemed forfeited by a court order, the funds are divided equally between WCDA and the PD that performed the seizure. According to Section 47(d) of Chapter 94C of the General Laws, forfeited funds may then be expended by WCDA as follows:

> *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.*

Every year WCDA uses a portion (up to 10%) of forfeited funds to award grants to neighborhood nonprofit groups that offer programs (e.g., sports or arts and crafts initiatives) geared toward children and teenagers. According to WCDA's internal control plan, these grants "assist in funding programs which engage youth in positive and healthy activities at times when they could otherwise be at risk."

Community programs apply for grant funding by submitting a Funds Request Form to WCDA, describing the program's mission and reason for the request. Upon receipt of a Funds Request Form, a WCDA assistant district attorney summarizes the information on the form in a memorandum. A committee of three WCDA employees reviews each completed Funds Request Form and memorandum and makes recommendations to the District Attorney, who gives final approval. Once a grant is awarded, the community program is required to submit expense reports showing how the granted funds were spent.

WCDA's forfeited fund revenue was $645,169 for fiscal year 2020 and $430,018 for fiscal year 2021. WCDA's forfeited fund expenditures were $408,476 for fiscal year 2020 and $351,584 for fiscal year 2021. Unexpended forfeited revenue remains in WCDA's forfeiture trust fund account with the Office of the State Treasurer and Receiver General, as required by Section 47(d) of Chapter 94C of the General Laws.

When PDs Hold Confiscated Funds

When the PD investigating drug offenses initially seizes funds and/or property, the PD may elect to retain possession of the funds and/or property (pending the outcome of the forfeiture process) or may transfer possession of funds to WCDA.

When PDs hold confiscated funds, the PD completes and emails a Request for Asset Forfeiture Form to the assistant district attorney in charge of the Forfeiture Drug Unit (the chief of asset forfeiture) within 10 days of seizing funds. The Request for Asset Forfeiture Form documents the following information: the PD that performed the seizure, the defendant's name, the date of seizure, and the amount of funds seized. The chief of asset forfeiture emails a copy of this form to WCDA's Fiscal Unit. The fiscal administrator prints a copy of the Request for Asset Forfeiture Form and enters the information on the form into a Microsoft Excel spreadsheet. WCDA uses the spreadsheet to track all confiscated funds and/or property held by PDs until the forfeiture process is complete. The fiscal administrator maintains a binder where the PDs' hardcopy Request for Asset Forfeiture Forms are filed.

When the forfeiture proceeding is complete, the prosecutor emails the court order in favor of asset forfeiture to the chief of asset forfeiture. The chief of asset forfeiture emails the court order to the fiscal administrator, who enters the court order information into an Excel spreadsheet. WCDA uses the spreadsheet to track the disposition of forfeited funds and/or property held by PDs until WCDA receives the funds. The fiscal administrator maintains a binder where the hardcopy court orders are filed by city or town name and deletes the associated information in the spreadsheet.

The chief of asset forfeiture also sends a copy of the court order and a request for WCDA's share of the funds to the PD holding the forfeited funds. The PD sends a check to WCDA through the United States Postal Service. Upon receipt, WCDA's director of operations date stamps this mail and brings it to the fiscal administrator, who makes a copy of the check and retrieves the hardcopy court order from the city's or town's file. The fiscal administrator records the disposition of the forfeited funds in WCDA's Microsoft Access forfeiture database, which WCDA uses to track all confiscated and/or forfeited fund cases.

The fiscal administrator enters the forfeited fund information from the court order into QuickBooks, WCDA's electronic accounting system, using an intake sheet. The fiscal administrator prints the completed intake sheet for WCDA's hardcopy files.

The fiscal administrator uses the QuickBooks banking function to record the deposit of forfeited funds into WCDA's Bank of America forfeited fund sweep account[2] and the funds are then automatically transferred from this account to WCDA's forfeiture trust fund account within the Massachusetts Management Accounting and Reporting System (MMARS). The fiscal administrator prepares a deposit ticket, takes the funds to the bank, and deposits the funds into the Bank of America forfeited fund sweep account. Additionally, the fiscal administrator enters relevant court information (e.g., the defendant's name, case number, and date the funds were forfeited) and the receipt and deposit dates for the forfeited funds into the Microsoft Access forfeiture database.

The fiscal administrator staples the bank receipt, intake sheet, court order, and a copy of the check together and files the documents in a locked filing cabinet in the chief financial officer's (CFO's) office.

When WCDA Holds Confiscated Funds

Following the initial seizure, PDs in Worcester County may bring confiscated funds to WCDA's office, at the PDs' discretion. In this situation, the PD contacts the District Attorney to schedule a time to bring in the confiscated funds. Once the PD brings the funds to WCDA, WCDA's fiscal administrator and CFO and the PD representative count the funds together. The WCDA fiscal administrator or CFO records the dollar amount of the confiscated funds on the Request for Asset Forfeiture Form and signs and dates the form. The fiscal administrator retains copies of the Request for Asset Forfeiture Form for the fiscal department

2. WCDA's sweep account is a bank account that automatically transfers all funds, at the close of each day, to a designated account.

and the chief of asset forfeiture. The fiscal administrator provides the signed original Request for Asset Forfeiture Form to the PD representative.

The fiscal administrator records the confiscated fund information from the Request for Asset Forfeiture Form in QuickBooks using an intake sheet. This entry records the deposit of the funds into WCDA's Bank of America confiscated funds trust account, pending determination by a judge's court order. The fiscal administrator also records relevant case details (e.g., defendant name, case number, date confiscated) from the Request for Asset Forfeiture Form in the Microsoft Access forfeiture database.

The fiscal administrator completes a deposit ticket for WCDA's Bank of America confiscated funds trust account and places it in a sealed deposit bag with the confiscated funds. The fiscal administrator or CFO makes the deposits on the same day. If the amount exceeds $3,000, the fiscal administrator and CFO bring the funds to the bank, and the PD representative accompanies them.

The fiscal administrator staples the Request for Asset Forfeiture Form, intake sheet, and bank receipt together and files the documents in a locked cabinet in the CFO's office.

When the case is adjudicated, the prosecutor forwards the court order in favor of asset forfeiture to the chief of asset forfeiture. The chief of asset forfeiture forwards the court order to the fiscal administrator. The fiscal administrator writes checks in QuickBooks from WCDA's Bank of America confiscated funds trust account to the PD that seized the funds and WCDA. The fiscal administrator mails the check with the PD's share of the funds to the corresponding PD with a letter addressed to the chief of police and a copy of the court order. The fiscal administrator updates the Microsoft Access forfeiture database with the relevant case information and changes the case status from open to closed.

The fiscal administrator or CFO deposits WCDA's check into WCDA's Bank of America forfeited fund sweep account. These funds are transferred daily into the state's General Fund and credited to WCDA's forfeiture trust fund account in MMARS through the Office of the State Treasurer and Receiver General and are available for expenditure.

Office of the Comptroller of the Commonwealth's Pandemic Response Guidance

On September 30, 2020, the Office of the Comptroller of the Commonwealth provided guidance in response to the 2019 coronavirus (COVID-19) pandemic for state agencies. The guidelines helped state

agencies experiencing significant changes to their business processes to identify their goals, objectives, and risks associated with COVID-19. Objectives could include telework; return-to-office plans; a risk assessment of the impact of COVID-19 on state agency operations; changes to the business process; safety protocols for employees and visitors; and tracking of COVID-19–related awards and expenditures, which are tracked separately from other federal, state, and local expenditures.

Cybersecurity Awareness Training

The Executive Office of Technology Services and Security has established policies and procedures that apply to all Commonwealth agencies. Information Security Risk Management Standard IS.010 requires that all Commonwealth personnel be trained annually for cybersecurity awareness. Section 6.2 of the document 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 new hires must complete an initial cybersecurity 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 Worcester County District Attorney's Office (WCDA) for the period July 1, 2019 through June 30, 2021. When reviewing updates to its internal control plan (ICP), we examined WCDA's most recent ICP as of the time of our audit work, which was dated March 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 WCDA make all forfeited fund expenditures in compliance with Section 47(d) of Chapter 94C of the General Laws?	**Yes**
2. Did WCDA process and track all confiscated funds in accordance with its "Fiscal Policy and Procedures" to ensure that all funds are properly accounted for?	**Yes**
3. Did WCDA process and track all forfeited funds in accordance with its "Fiscal Policy and Procedures" to ensure that all funds are properly accounted for?	**Yes**
4. Did WCDA update its ICP to address the 2019 coronavirus (COVID-19) pandemic, in accordance with the Office of the Comptroller of the Commonwealth's (CTR's) "COVID-19 Pandemic Response Internal Controls Guidance," dated September 30, 2020?	**Yes**
5. Did WCDA 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 achieve our audit objectives, we gained an understanding of WCDA's internal control environment related to the objectives by reviewing applicable policies and procedures and interviewing WCDA officials. We evaluated the design, and tested the operating effectiveness of, internal controls related to the

approval of forfeited fund expenditures, the verification of amounts of confiscated funds received from law enforcement agencies, and the monthly reconciliation of confiscated and forfeited funds.

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

Forfeited Fund Expenditures

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

- WCDA provided us with a list of all forfeited fund expenditures for the audit period from QuickBooks. Total forfeited fund expenditure activity for the audit period consisted of 861 transactions, totaling $969,138. We split the population of forfeited fund expenditures into two categories based on the type of expenditure: financial assistance awards given to community programs and all other expenditures.
- We selected a random, nonstatistical sample of 20 of the 106 financial assistance awards that WCDA gave to community programs. We examined each community program's completed Funds Request Form, spending report, and supporting documentation (invoices and receipts) to validate the nature and purpose of the expenditures.
- We also selected a random, nonstatistical sample of 35 of the 755 other forfeited fund expenditures. We reviewed supporting documentation (payment requests, invoices, and receipts) to determine whether each expenditure was supported by adequate documentation and was allowable under Section 47(d) of Chapter 94C of the General Laws.

Confiscated Funds

To determine whether WCDA processed and tracked all confiscated funds in accordance with its "Fiscal Policy and Procedures," WCDA provided us with a list of all 659 of WCDA's open confiscated fund cases during the audit period from the District Attorney Management Information Office Network (DAMION)[3] case management system. We selected a nonstatistical, random sample of 30 of the 659 cases for testing.

- For 14 of the 30 cases selected for testing, the confiscated funds were being held by either the local or state police department (PD) that seized the funds. For these 14 cases, we examined the Request for Asset Forfeiture Forms to determine whether case information was accurately recorded in the electronic spreadsheet WCDA's Fiscal Unit maintains.

3. WCDA uses DAMION to perform a variety of tasks, including maintaining case, victim, and witness information and tracking court events. DAMION was implemented by the Massachusetts District Attorneys Association for all 11 district attorneys' offices. Each office can customize the system to some extent to meet its own needs.

- WCDA held confiscated funds from the remaining 16 cases selected for testing. For these cases, we examined Request for Asset Forfeiture Forms and deposit slips to determine whether case information was accurately recorded in WCDA's Fiscal Unit open case database and that the funds were deposited into WCDA's confiscated funds trust account.

Forfeited Funds

To determine whether WCDA processed and tracked all forfeited funds in accordance with its "Fiscal Policy and Procedures," WCDA provided us with a list of all 383 of WCDA's forfeited fund cases that were closed during the audit period from DAMION. We selected a nonstatistical, random sample of 25 of the 383 cases.

- For 11 of the 25 cases selected for testing, the local or state PD that seized the funds held the forfeited funds. For these 11 cases, we examined forfeiture orders, checks, intake sheets, and deposit slips to determine whether (1) the amount of forfeited funds collected was accurate, (2) the forfeited funds were deposited into WCDA's Bank of America forfeited funds sweep account, and (3) the forfeited funds were transferred into WCDA's forfeiture trust fund account within the Massachusetts Management Accounting and Reporting System (MMARS). In addition, we verified that the amount of forfeited funds were listed in the Microsoft Access forfeiture database.

- WCDA held the forfeited funds from the remaining 14 cases selected for testing. For these cases, we examined forfeiture orders, checks, intake sheets, and deposit slips to determine whether (1) WCDA deposited its portion of the forfeited funds into its Bank of America forfeited funds sweep account, (2) the PD's portion was accurately disbursed to the appropriate PD, and (3) funds were accounted for on WCDA's Microsoft Access forfeiture database, maintained by its Fiscal Unit. If the PD's portion was not disbursed as of the time of our audit, we verified that the funds were accounted for within WCDA's Microsoft Access forfeiture database.

ICP Updates

To determine whether WCDA updated its ICP to address COVID-19 in accordance with CTR's "COVID-19 Pandemic Response Internal Controls Guidance," we inspected the 2020 and 2021 Internal Control Questionnaires that WCDA submitted to CTR. We reviewed the Internal Control Questionnaire questions that addressed COVID-19 preparedness, as well as CTR's guidance. We also inspected WCDA's most recent ICP, dated March 2022, to determine whether WCDA made updates to address COVID-19 in accordance with the guidance.

Cybersecurity Awareness Training

To determine whether WCDA was in compliance with Sections 6.2.3 and 6.2.4 of EOTSS's Information Security Risk Management Standard IS.010 regarding cybersecurity awareness training, we interviewed

WCDA's chief information officer and first assistant district attorney to discuss whether WCDA had established a program to ensure that employees received cybersecurity awareness training.

Whenever sampling was used, we applied a nonstatistical sampling approach, and, as a result, we could not project our results to the entire population.

Data Reliability

In 2018 and 2022, the Office of the State Auditor performed a data reliability assessment of MMARS. The assessment focused on reviewing selected system controls, including access controls, cybersecurity awareness, audit and accountability, configuration management, identification and authentication, and personnel security.

To determine the reliability of the list of financial assistance awards that WCDA gave to community programs from the forfeited funds expenditure list, we checked the list for invalid and duplicate records. To test for accuracy, we randomly selected a sample of 10 expenditures from this list and compared the expenditure amounts to copies of the checks and the assistant district attorney's original memoranda. To test for completeness, we selected a judgmental sample of 10 original memoranda and compared expenditure information on the memoranda to the corresponding expenditures recorded in QuickBooks. Additionally, we compared the aggregate amount of the expenditures on the list to data recorded in MMARS.

To determine the reliability of the list of all other WCDA forfeited fund expenditures, we checked the list for invalid and duplicate records. To test for accuracy, we randomly selected a sample of 20 expenditures from this list and compared the expenditure amounts to copies of the checks and the original memoranda. To test for completeness, we selected a judgmental sample of 20 original check stubs and corresponding invoices and compared expenditure information on the check stubs and invoices to the corresponding expenditures in QuickBooks. Additionally, we compared the aggregate amount of the expenditures on the list to data recorded in MMARS.

To determine the reliability of the list of WCDA's open confiscated fund cases, we checked the list for invalid and duplicate records. To test for accuracy, we selected a judgmental sample of 20 cases from this list and compared case information to the Request for Asset Forfeiture Forms. To test for completeness,

we selected a judgmental sample of 20 Request for Asset Forfeiture Forms from WCDA's open case files and compared case information to the information recorded in DAMION.

To determine the reliability of the list of forfeited fund cases that were closed during the audit period, we checked the list for invalid and duplicate records. To test for accuracy, we selected a judgmental sample of 20 cases from this list and compared case information to the information recorded in the court orders. To test for completeness, we selected a judgmental sample of 20 court orders from WCDA's closed case files and compared case information to the information recorded in DAMION.

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 work.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Worcester County District Attorney's Office did not ensure that its employees completed cybersecurity awareness training.

The Worcester County District Attorney's Office (WCDA) did not ensure that all new employees completed cybersecurity awareness training as part of their orientation when they began working or that all employees completed annual cybersecurity awareness training.

Without educating all employees on their responsibility to protect the security of information assets, WCDA is exposed to a higher risk of cybersecurity attacks and financial and/or reputation losses.

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.*

Reasons for Noncompliance

WCDA officials told us that they were unaware of the EOTSS requirement.

Recommendations

1. WCDA should ensure that employees complete cybersecurity awareness training within 30 days of their orientation and annually thereafter.
2. WCDA should ensure that its employees are aware of EOTSS requirements.

Auditee's Response

> *After reviewing the draft audit report on the Worcester County District Attorney's Office, our office is in agreement on the finding and recommendations. . . .*
>
> *The WCDA promptly implemented a mandatory annual cybersecurity program for all current and new employees using the KnowBE4 platform. The WCDA now requires newly hired employees receive initial cybersecurity awareness training within 30 days of their date of hire as part of the*

onboarding process. The WCDA engaged the cybersecurity vendor and implemented these policies and practices during the audit process.

The Information Technology Department of the WCDA will review the EOTSS policies and standards on a quarterly basis and continue interaction with professional [information technology] organizations to maintain current knowledge of policies and procedures. The WCDA will provide informational updates concerning policy and procedure updates to employees as needed.

Auditor's Reply

Based on its response, WCDA has taken measures to address our concerns in this area.