OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued October 24, 2023

Norfolk District Attorney's Office

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

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

October 24, 2023

District Attorney Michael Morrissey
Norfolk District Attorney's Office
45 Shawmut Road
Canton, MA 02021

Dear District Attorney Morrissey:

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

LIST OF ABBREVIATIONS

EOTSS	Executive Office of Technology Services and Security
MMARS	Massachusetts Management Accounting and Reporting System
NDAO	Norfolk District Attorney's Office
PD	police department

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 Norfolk District Attorney's Office (NDAO) for the period July 1, 2019 through June 30, 2021.

The purpose of our audit was to determine the following:

- whether NDAO made forfeiture trust fund expenditures in accordance with Section 47(d) of Chapter 94C of the General Laws;
- whether NDAO 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 NDAO ensured that its employees completed cybersecurity awareness training in accordance with Sections 6.2.1, 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 findings and recommendations, with links to each page listed.

Finding 1 **Page 10**	NDAO disbursed to two police departments $28,086 in forfeited assets that it should have retained.
Recommendations **Page 10**	1. NDAO should collect all of the forfeited assets to which it is entitled. 2. NDAO should include language in its policies that references (1) the part of Section 47(d) of Chapter 94C of the General Laws about forfeited asset splits involving multiple police departments and (2) its process for forfeited asset distribution calculation review to ensure that all forfeitures are processed in compliance with Section 47(d) of Chapter 94C of the General Laws.
Finding 2 **Page 11**	NDAO did not ensure that its employees completed cybersecurity awareness training.
Recommendations **Page 12**	1. NDAO should ensure that its employees complete cybersecurity awareness training within 30 days of their orientation and annually thereafter. The cybersecurity awareness training should include a test of each individual's understanding of all policies and their role in maintaining the security of NDAO's information technology systems. 2. NDAO should implement monitoring controls to ensure that its employees complete their cybersecurity awareness training on time. 3. NDAO should ensure that its employees are informed on all requirements outlined in EOTSS's Information Security Risk Management Standard IS.010. 4. NDAO should maintain a record of completion of cybersecurity awareness training for each employee.

OVERVIEW OF AUDITED ENTITY

The Norfolk District Attorney's Office (NDAO) 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.

NDAO is one of 11 district attorneys' offices in the Commonwealth. NDAO serves 27 cities and towns in eastern Massachusetts. NDAO's main administrative office is at 45 Shawmut Road in Canton, and NDAO operates from five district courts in Norfolk County, as well as the superior and juvenile courts.

According to its website,

> *[NDAO] works with court personnel and the law enforcement community every day to prosecute approximately 20,000 cases a year. These cases involve homicide, sexual assault, domestic violence, robbery, drug sales and possession, fraud, theft, driving under the influence of alcohol and drugs, and many other offenses.*

According to NDAO's most recent internal control plan, dated June 2021, as of the time of our audit,

> *[NDAO's mission] is to seek justice through the fair and ethical prosecution of criminal cases, to work with victims and their families to ensure that those who otherwise might not be heard have a voice in the criminal justice system, and to create a safer community through positive partnerships with law enforcement agencies and the citizens of Norfolk County.*

NDAO received appropriations of $11,027,852 and $12,139,064 from the Commonwealth for fiscal years 2020 and 2021, respectively. As of June 30, 2021, NDAO had approximately 149 employees.

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 (PD) that performed the seizure holds the assets seized from a defendant until a judge determines whether these seized assets should be forfeited to the

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.

Commonwealth. Each forfeiture case is heard as part of its related criminal court case, regardless of how many or what kind of assets were seized. However, if the seized assets involve (1) more than $2,500, (2) a motor vehicle, or (3) real property, then there will be an additional, separate civil court case. If assets are ultimately deemed forfeited by a court order, then these assets are (1) divided equally between NDAO and the PD that performed the seizure and (2) moved to and held in a forfeiture trust fund. If more than one PD was involved in the seizure, then the PDs split a 50% share equally.

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

NDAO's forfeited asset revenue was $434,174 during the audit period. NDAO's forfeiture trust fund expenditures were $528,695 during the audit period. According to NDAO officials, forfeited asset revenue, which accrues over multiple years, remains in NDAO'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. NDAO officials also told us that the unexpended balance of the forfeiture trust fund at the end of a fiscal year is rolled forward for the next fiscal year.

Cybersecurity Awareness Training

The Executive Office of Technology Services and Security has established policies and procedures that apply to all Commonwealth agencies. Its 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 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 Norfolk District Attorney's Office (NDAO) 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 NDAO make forfeiture trust fund expenditures in accordance with Section 47(d) of Chapter 94C of the General Laws?	**Yes**
2. Did NDAO 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 NDAO ensure that its employees completed cybersecurity awareness training in accordance with Sections 6.2.1, 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 NDAO's internal control environment related to the objectives by reviewing NDAO's internal control plan and applicable policies and procedures, as well as by interviewing NDAO officials. We evaluated the design and tested the operating effectiveness of internal controls related to the verification of amounts of forfeited assets received from law enforcement agencies, the monthly reconciliation of forfeiture trust fund deposits, and the approval of forfeiture trust fund expenditures.

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

Forfeiture Trust Fund Expenditures

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

NDAO provided us with a list—maintained by NDAO's Financial Department using Microsoft Excel spreadsheets—of 211 forfeiture trust fund expenditures that were made during the audit period. We selected a random, nonstatistical sample of 35 (totaling $186,312) out of the 211 forfeiture trust fund expenditures (totaling $528,695). We reviewed supporting documentation (e.g., invoices, receipts, grant applications, email correspondence between NDAO staff members, written explanations of charges and travel, and training request memos) to determine whether each expenditure 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 NDAO made forfeiture trust fund expenditures in compliance with Section 47(d) of Chapter 94C of the General Laws.

Forfeited Assets from Closed Cases

To determine whether NDAO 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.

NDAO provided us with a list—maintained by NDAO's asset forfeiture unit using Microsoft Excel spreadsheets—of all closed and open forfeiture cases. From that list, we identified 121 forfeiture cases that were closed during the audit period, totaling $502,794[2] in seized assets.

We selected a random, nonstatistical sample of 35 closed forfeiture cases for testing, totaling $354,670.65 in seized assets. We reviewed relevant case documentation (e.g., forfeiture split letters, forfeiture orders from courts, police reports, checks, and deposit slips) to calculate the forfeited asset split for each case, with NDAO's portion being half of the forfeiture amount ordered by the court plus half of the forfeited asset revenue of any property sold at auction. We compared our calculation to the amounts listed in the

2. This amount includes forfeited assets ultimately distributed to police departments.

forfeiture split letters (which NDAO prepares and disseminates) to determine whether NDAO distributed the correct amount of forfeited assets to the police department(s) involved in each case. We reviewed copies of checks and deposit slips to determine whether NDAO collected and deposited the correct amount of forfeited assets.

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 NDAO's distribution of forfeited assets.

Cybersecurity Awareness Training

To determine whether NDAO employees completed cybersecurity awareness training in accordance with standards issued by the Executive Office of Technology Services and Security, we performed the following procedures.

To ensure that NDAO's employees received cybersecurity awareness training, we interviewed NDAO's information technology director and first assistant district attorney to discuss whether NDAO had established a cybersecurity awareness training program (using a training system called KnowBe4). Beginning in calendar year 2020, NDAO implemented an annual cybersecurity awareness training program for its employees. In October 2020, NDAO used KnowBe4 to assign all its current employees cybersecurity awareness training, which they were to complete also using KnowBe4. The NDAO-established deadline for completion of this training was November 1, 2020.

NDAO's Human Resources Department provided us with a list of all 149 NDAO employees as of June 30, 2021. We filtered out employees on this list with (1) termination dates before October 1, 2020 or (2) start dates in 2021. The filtered list included a total of 114 employees who would have been required to take NDAO's annual cybersecurity awareness training during calendar year 2020. We obtained electronic cybersecurity awareness training records from KnowBe4 to determine whether these employees completed cybersecurity awareness training within the timeframe established by NDAO.

See Finding 2 for an issue we identified with NDAO's cybersecurity awareness training program.

Data Reliability Assessment

Massachusetts Management Accounting and Reporting System

In 2018 and 2022, the Office of the State Auditor performed a data reliability assessment of the Massachusetts Management Accounting and Reporting System (MMARS), the state's accounting system. The assessment focused on reviewing selected system controls, including access controls, security awareness, audit and accountability, configuration management, identification and authentication, and personnel security.

Forfeiture Trust Fund Expenditures

To determine the reliability of the list of forfeiture trust fund expenditures, we (1) checked the list for duplicate records, (2) inquired about any missing values in key fields, (3) ensured that payment records were only for services provided during the audit period, and (4) compared the total amount of the expenditures on the list to data recorded in MMARS. We also randomly selected a sample of 10 expenditures from this list and compared the expenditure information to source documentation (e.g., receipts, invoices, purchase orders, and bank statements) that NDAO's Financial Department maintained.

Forfeited Assets from Closed Cases

To determine the reliability of the lists of forfeited assets from closed cases, we (1) checked for duplicate records, (2) inquired about any missing values in key fields, (3) ensured that the dates cases were closed were within the audit period, (4) compared the total number of cases that were closed during the audit period against NDAO's deposit workbook, and (5) compared the total amount of forfeiture trust fund deposits made during the audit period to data recorded in MMARS. We selected a random sample of 20 closed cases from the list and compared them to source documents maintained within NDAO's hardcopy case files.

Cybersecurity Awareness Training

To determine the reliability of the cybersecurity awareness training records we obtained from KnowBe4, we reviewed System and Organization Control reports[3] for KnowBe4 that covered the audit

3. A System and Organization Control report is a report on controls about a service organization's systems relevant to security, availability, processing integrity, confidentiality, or privacy issued by an independent contractor.

period and ensured that an independent certified public accountant performed certain information system control tests on KnowBe4. We also interviewed NDAO's information technology director, who monitors training completion.

To determine the reliability of the list of all 149 NDAO employees that NDAO's Human Resources Department provided to us, we selected a random sample of 20 employees from the list and traced them to employee data reported in CTHRU.[4] We also selected a random sample of 20 employees from CTHRU and traced them back to NDAO's employee list. In addition, we checked the list for duplicate and blank fields, verified that employment dates were valid (i.e., no start dates after the end of the audit period or end dates before the start of the audit period), and compared the total number of unique employee records on the employee list to the total number of unique employee records reported in CTHRU.

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.

4. According to the Office of the Comptroller of the Commonwealth's website, "CTHRU is an innovative open records platform that offers transparency into the finances of the Commonwealth of Massachusetts. CTHRU provides users with an intuitive experience for exploring how and where our tax dollars are utilized."

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Norfolk District Attorney's Office disbursed to two police departments $28,086 in forfeited assets that it should have retained.

During the audit period, the Norfolk District Attorney's Office (NDAO) disbursed to two police departments (PDs) $28,086 in forfeited assets that it should have retained. In October 2019, NDAO auctioned off a house that the court deemed forfeited to the Commonwealth and generated $168,520 in forfeited assets. The investigation that led to the seizure of this house was conducted by the Randolph and Weymouth PDs. NDAO split the forfeited assets of this house equally three ways, between itself and the two PDs, with each party receiving $56,173. However, NDAO should have received $84,260, and the two PDs should have split the remaining $84,260 equally ($42,130 each). NDAO overpaid the PDs a total of $28,086.

If NDAO does not collect all of the forfeited assets to which it is entitled, it cannot use the associated revenue for other purposes, such as anti-drug or neighborhood crime watch programs.

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.*

Reasons for Noncompliance

NDAO officials told us that they decided to split the forfeited assets equally three ways because of the complexity of the case and the amount of work put in by each party involved. However, Section 47(d) of Chapter 94C of the General Laws does not authorize such a practice. Additionally, NDAO does not include language in its policies that references (1) the part of Section 47(d) of Chapter 94C of the General Laws about forfeited asset splits involving multiple PDs or (2) its process for forfeited asset distribution calculation review, in which NDAO officials approve distributions when forfeiture split letters are sent.

Recommendations

1. NDAO should collect all of the forfeited assets to which it is entitled.

2. NDAO should include language in its policies that references (1) the part of Section 47(d) of Chapter 94C of the General Laws about forfeited asset splits involving multiple PDs and (2) its process for forfeited asset distribution calculation review to ensure that all forfeitures are processed in compliance with Section 47(d) of Chapter 94C of the General Laws.

Auditee's Response

The [State Auditor's Office (SAO)] reviewed hundreds of asset forfeiture cases both open and closed during the audit period. The cited case was the only case during the audit period and in its forfeiture history in which the NDAO split the proceeds three ways instead of the 50/50 split. This case also represented the first time the NDAO seized a house under Section 47(d) of Chapter 94C. It required an inordinate amount of time, effort and work on the part of the NDAO as well as the two police departments involved.

The NDAO will follow the language of the forfeiture statute.

Auditor's Reply

We encourage NDAO to implement our recommendations fully, including using language in its policies that references the part of Section 47(d) of Chapter 94C of the General Laws about forfeited asset splits involving multiple PDs and its process for forfeited asset distribution calculation review.

2. The Norfolk District Attorney's Office did not ensure that its employees completed cybersecurity awareness training.

NDAO did not ensure that its employees completed cybersecurity awareness training. Specifically, NDAO provided its 32 new employees with a verbal overview of NDAO's information technology policies during orientation and had these new employees sign acknowledgement forms confirming that they received this training. However, NDAO did not test these new employees on their understanding of these policies or on their role in maintaining the security of NDAO's information technology systems.

Additionally, although all 114 employees in our sample who were assigned to take the 2020 annual refresher cybersecurity awareness training completed the training, we found that 4 employees completed the training late. One of these employees completed the training 318 days late; one completed the training 284 days late; one completed the training 5 days late; and one completed the training 1 day late.

A lack of cybersecurity awareness training for new employees and untimely annual refresher cybersecurity awareness training for existing employees exposes NDAO to a higher 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,

> *6.2.1 Implement an enterprise-wide information security awareness and training program. . . .*
>
> *6.2.1.3 The training shall: . . .*
>
> *6.2.1.3.4 Test each individual's understanding of all policies and of his or her role in maintaining the highest ethical standards. . . .*
>
> *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

When asked about the lack of training for new employees, NDAO officials told us that they were unaware of the requirements outlined in EOTSS's Information Security Risk Management Standard IS.010. Additionally, NDAO did not have monitoring controls to ensure that its employees completed their cybersecurity awareness training on time.

Recommendations

1. NDAO should ensure that its employees complete cybersecurity awareness training within 30 days of their orientation and annually thereafter. The cybersecurity awareness training should include a test of each individual's understanding of all policies and their role in maintaining the security of NDAO's information technology systems.
2. NDAO should implement monitoring controls to ensure that its employees complete their cybersecurity awareness training on time.
3. NDAO should ensure that its employees are informed on all requirements outlined in EOTSS's Information Security Risk Management Standard IS.010.
4. NDAO should maintain a record of completion of cybersecurity awareness training for each employee.

Auditee's Response

During the audit period, the NDAO repeatedly advised the SAO that its office did not fall within the Executive Branch and thus was not required to comply with any Executive Branch mandates

including the mandate that requires compliance with EOTSS Information Security Risk Management Standard IS.010.

Attached, please find a letter dated July 31, 2023 from . . . [EOTSS's] General Counsel/Chief Privacy Officer. In it, the letter confirms that "the Norfolk County District Attorney's office was not subject to the EOTSS required annual cybersecurity training during the scope of the audit currently in progress."

Notwithstanding the fact that the NDAO is not required to follow Executive Branch mandates, the NDAO takes cyber security and cyber training seriously. On its own initiative, the NDAO purchased KnowBe4 software to help train and educate staff on cyber security issues. It annually trains it staff, provides mock exercises to teach employees about cyber issues to ensure a safe network and provides a platform to easily track and monitor users' training and track training completion. The NDAO also sends out frequent emails, news stories and articles about cyber security, the risks involved with using technology and the important part each employee plays in keeping our network safe.

Auditor's Reply

NDAO is correct in stating that it does not fall within the state executive branch and therefore is not required to follow EOTSS's Information Security Risk Management Standard IS.010. However, this policy does represent what the Commonwealth considers a best practice for protecting information when conducting business on behalf of the state. 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."

We acknowledge that NDAO provides annual cybersecurity awareness training to its employees, which includes mock exercises and cybersecurity-related news articles. However, as noted above, during the audit period, we found that the cybersecurity awareness training NDAO provided to its new employees only contained a verbal overview of NDAO's information technology policies. NDAO did not test these employees on their understanding of NDAO's information technology policies or on their role in maintaining the security of NDAO's information technology systems. In addition, annual training for current employees was not always completed on time.

We urge NDAO to implement our recommendations fully and to improve its cybersecurity policies and practices.