

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued December 19, 2025

Middlesex County District Attorney's Office

For the period July 1, 2022 through June 30, 2024

(When examining employee settlement agreements entered into by the auditee, we extended the audit period to July 1, 2019 through June 30, 2024)



OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

December 19, 2025

Marian Ryan, District Attorney
Middlesex County District Attorney's Office
15 Commonwealth Avenue
Woburn, MA 01801

Dear District Attorney Ryan:

I am pleased to provide to you the results of the enclosed performance audit of the Middlesex 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, 2022 through June 30, 2024. When examining employee settlement agreements entered into by MDAO, we extended the audit period to July 1, 2019 through June 30, 2024. 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 Middlesex 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 has any questions.

Best regards,



Diana DiZoglio
Auditor of the Commonwealth

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
OVERVIEW OF AUDITED ENTITY	3
AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY	7
DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE	12
1. The Middlesex County District Attorney's Office did not promptly revoke former employees' access rights within the statewide sexual assault evidence collection kit tracking system and did not complete certain data fields in the system.	12
2. The Middlesex County District Attorney's Office should have documented internal policies or procedures regarding state employee settlement agreements and supporting records, as would be best practice. ...	14
3. The Middlesex County District Attorney's Office should ensure that all employees complete cybersecurity awareness training upon hire and annually thereafter.	16
OTHER MATTERS	19

LIST OF ABBREVIATIONS

CMR	Code of Massachusetts Regulations
CTR	Office of the Comptroller of the Commonwealth
EOPSS	Executive Office of Public Safety and Security
EOTSS	Executive Office of Technology Services and Security
MDAO	Middlesex County District Attorney's Office
SAECK	sexual assault evidence collection kit

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 Middlesex County District Attorney's Office (MDAO) for the period July 1, 2022 through June 30, 2024. When examining employee settlement agreements entered into by MDAO, we extended the audit period to July 1, 2019 through June 30, 2024.

The purpose of our audit was to determine the following:

- To what extent did MDAO participate in the statewide sexual assault evidence collection kit (SAECK) tracking system as required by Section 18X(g) of Chapter 6A of the General Laws?
- Did MDAO adhere to Sections 6.2.3 and 6.2.4 of the Executive Office of Technology Services and Security's Information Security Risk Standard ISO.010 regarding cybersecurity awareness training?
- Did MDAO have internal policies and procedures in place for (a) the review and approval of employee settlement agreements, including the use of non-disclosure, non-disparagement, or similarly restrictive clauses, and (b) the reporting of monetary employee settlements to the Office of the Comptroller of the Commonwealth in accordance with Sections 5.06 and 5.09 of Title 815 of the Code of Massachusetts Regulations?

Below is a summary of our findings, the effects of those findings, and our recommendations, with hyperlinks to each page listed.

Finding 1 Page 12	MDAO did not promptly revoke former employees' access rights within the statewide SAECK tracking system and did not complete certain data fields in the system.
Effect	If MDAO does not promptly revoke former employees' access rights to the Track-Kit system, then there is a risk of unauthorized access to sensitive case and survivor information. Additionally, if MDAO does not assign its contact information to SAECKs, then the Track-Kit System is not being used as intended under statute. Having MDAO contact information assigned to SAECKs allows survivors to have an informed single point of contact and can streamline outreach and reduce confusion.
Recommendations Page 13	<ol style="list-style-type: none">1. MDAO should assign its contact information to each SAECK within its jurisdiction in the Track-Kit system and should train its employees on how to use this system.2. MDAO should develop, document, and implement policies and procedures for Track-Kit system access authorization for new users and the revocation of access upon termination of users. These policies and procedures should include periodic access reviews at least semiannually to ensure that users' access rights are limited to their job requirements.
Finding 2 Page 14	MDAO should have documented internal policies or procedures regarding state employee settlement agreements and supporting records, as would be best practice.

Effect	A documented, written process to handle employee settlement agreements, especially for those containing non-disclosure, non-disparagement, or similarly restrictive clauses, can help ensure that employee settlements are handled in an ethical, legal, and appropriate manner.
Recommendation Page <u>16</u>	MDAO should develop, document, and implement a written policy related to employee settlement agreements, including prohibiting the use of non-disclosure, non-disparagement, or similarly restrictive clauses in its agreements, as recommended in the Governor's "Executive Department Settlement Policy," issued January 27, 2025.
Finding 3 Page <u>16</u>	MDAO should ensure that all employees complete cybersecurity awareness training upon hire and annually thereafter.
Effect	If MDAO does not educate its employees on their responsibility to protect the security of information assets, then MDAO may expose itself to a higher-than-acceptable risk of cybersecurity attacks and financial and/or reputational losses.
Recommendation Page <u>17</u>	MDAO should ensure that all employees complete annual refresher cybersecurity awareness training and that all newly hired employees complete the initial training within the first 30 days of their new hire orientation.

Post-Audit Action

During the course of our audit, we were informed that, and subsequently provided evidence regarding how, MDAO revoked all former employees' access rights to the Track-Kit system. This corrective action addresses part of our audit finding related to the statewide SAECK tracking system.

OVERVIEW OF AUDITED ENTITY

The Middlesex County District Attorney's Office (MDAO) 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.

MDAO is one of 11 district attorneys' offices in the Commonwealth and represents the Commonwealth in criminal cases in two superior courts, 12 district courts, four juvenile courts, the Massachusetts Appeals Court, and the Massachusetts Supreme Judicial Court. It operates offices in Woburn, Framingham, and Lowell, and serves 54 cities and towns across Middlesex County. According to the 2020 US Census Bureau, the population of Middlesex County was 1,632,002 full-time residents at the time the census was taken.

MDAO's current District Attorney was sworn into office on January 2, 2019, and originally assumed office in April 2013.

According to MDAO's internal control plan,

The agency's goals are to ensure the peace and safety of the community by speedy prosecution of major offenders as well as by expediting the handling of minor criminal matters. In pursuing the reduction of criminal activity, the MDAO is assisted by Massachusetts State Police detectives who are assigned to the office. The office also works with the local police departments, and the sworn officers of the College and University Police Departments within the County and the Transit Police. The MDAO encourages cooperative relations among law enforcement agencies at all levels. In pursuing our mission objectives, we continue to emphasize the investigation and prosecution of crime at all levels. In addition to its law enforcement mandate, the District Attorney has established programs that address the needs of our community extending beyond the normal prosecution function that focuses on intervention and prevention efforts.

During fiscal years 2023 and 2024, MDAO received state appropriations of \$21,568,164 and \$24,074,078, respectively. MDAO had 222 employees as of June 30, 2024.

Statewide Sexual Assault Evidence Collection Kit Tracking System

Section 18X of Chapter 6A of the General Laws requires the Executive Office of Public Safety and Security (EOPSS) to establish and maintain a statewide sexual assault evidence collection kit (SAECK) tracking system. EOPSS implemented the web-based Track-Kit system to allow all users to trace a SAECK's location from distribution to collection to processing to storage. Track-Kit system users include medical facilities

that perform the examinations, law enforcement agencies that transport the kits and conduct investigations, and crime laboratories that perform testing and reporting on the kits. In addition, survivors of sexual assault can access the system to track the location and test status of their kits through a special Track-Kit system web portal. The EOPSS Policy Center administers the Track-Kit system and monitors user activities and statutory compliance.

Section 18X(g) of Chapter 6A of the General Laws states, "District attorney offices shall participate in the statewide sexual assault evidence kit tracking system established in this section for the purpose of tracking the status of all sexual assault evidence kits."

According to EOPSS's website,

Each department [including district attorneys' offices] is responsible for determining which personnel shall have access to the department portal and ensure those with access are properly trained in the operation of the tracking system. Each department should have a specific policy in place to address when an authorized user shall no longer access the tracking system and identify when revocation of privileges should occur.

The Track-Kit system allows district attorneys' offices, including MDAO, to take the following actions:

- review SAECK information related to cases referred to their offices by law enforcement authorities;
- assign a prosecutor's or victim witness advocate's direct contact information to a SAECK; and
- search for SAECKs that were collected in their jurisdictions and assigned to their offices.

During the audit period, 583 SAECKs were collected in MDAO's jurisdiction and entered into the Track-Kit system.

EOPSS's website provides the following guidance to agencies that use the Track-Kit system:

Users who are terminated, resigned their employment, or are placed on suspension should have their privileges revoked immediately. Likewise, the policy should also address new user access privileges and training. It is each department's responsibility to ensure only authorized users have access to the tracking system and are properly trained in the operation of the tracking system.

Cybersecurity Awareness Training

The Executive Office of Technology Services and Security (EOTSS) has established policies and procedures that apply to all Commonwealth departments and agencies within the executive branch. EOTSS

recommends, but does not require, non-executive branch state agencies to follow these policies and procedures. Section 6.2 of EOTSS's Information Security Risk Management Standard IS.010¹ stated:

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 Agencies and Offices must ensure that all personnel are trained on all relevant rules and regulations for cybersecurity.

All employees in executive branch state agencies with access to a Commonwealth-provided email address are required to complete a cybersecurity awareness training course every year. All new employees must complete an initial cybersecurity awareness training course within 30 days of their orientation.

Employee Settlement Agreements

The Office of the Comptroller of the Commonwealth (CTR) has established policies and procedures for state agencies processing settlements and judgments. CTR's "Settlements and Judgments" Policy states,

A settlement or judgment results from a formal claim (grievance, complaint or lawsuit) against the Commonwealth that results in either a Settlement Agreement, or a court or administrative award, order or Judgment. . . .

A "claim" is considered any demand by any person for damages to compensate a wrong allegedly suffered, including but not limited to violation of civil rights, breach of contract, failure to comply with contract bidding laws, incorrect or improper personnel determinations regarding pay, promotion or discipline, failure to comply with statutory or constitutional provisions applicable to employment, an eminent domain taking, and attorney's fees, interest and litigation costs associated with these claims.

For the purposes of our audit, we focused on settlement agreements resulting from claims brought by current or former employees against MDAO for the period July 1, 2019 through June 30, 2024.

Section 5.00 of Title 815 of the Code of Massachusetts Regulations outlines the procedures by which state agencies may preserve the availability of funds and may obtain access to funds for the payment of settlements and judgments.

This regulation also requires state agencies to prepare and submit a report to CTR's general counsel before making the payment to ensure proper tax reporting. When reporting employee settlements to CTR, state

1. EOTSS has since changed the titles and numbers of at least some of its policies and standards between the end of the audit period and the publication of this report. In this report, we reference the titles and numbers of EOTSS's policies and/or standards as they were during the audit period (unless stated otherwise).

agencies use a Non-Tort Settlement/Judgment Payment Authorization Form (referred to in this report as the SJ Authorization Form) to document whether the claim will be paid by the agency or through the Settlement and Judgment Reserve Fund. The SJ Authorization form also identifies the type of claim, the agency's information, the employee's information, the type and amount of damages detailed in the settlement, the amount of any attorney fees awarded, and the amount of any interest awarded or accrued. Additionally, state agencies must include a copy of the employee settlement agreement signed by authorized representatives of both parties when they submit the SJ Authorization Form to CTR.

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 Middlesex County District Attorney's Office (MDAO) for the period July 1, 2022 through June 30, 2024. When examining employee settlement agreements entered into by MDAO, we extended the audit period to July 1, 2019 through June 30, 2024.

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.

Objectives	Conclusion
1. To what extent did MDAO participate in the statewide sexual assault evidence collection kit (SAECK) tracking system as required by Section 18X(g) of Chapter 6A of the General Laws?	To an insufficient extent; see Finding <u>1</u> and <u>Other Matters</u>
2. Did MDAO adhere to Sections 6.2.3 and 6.2.4 of the Executive Office of Technology Services and Security's (EOTSS's) Information Security Risk Standard ISO.010 regarding cybersecurity awareness training?	No; see Finding <u>3</u>
3. Did MDAO have internal policies and procedures in place for (a) the review and approval of employee settlement agreements, including the use of non-disclosure, non-disparagement, or similarly restrictive clauses, and (b) the reporting of monetary employee settlements to the Office of the Comptroller of the Commonwealth (CTR) in accordance with Sections 5.06 and 5.09 of Title 815 of the Code of Massachusetts Regulations (CMR)?	No; see Finding <u>2</u>

To accomplish our audit objectives, we gained an understanding of the MDAO internal control environment relevant to our objectives by reviewing applicable policies and procedures and MDAO's internal control plan, as well as by interviewing MDAO officials. We also reviewed Track-Kit system user manuals, which included user roles for prosecuting attorneys. In addition, to obtain sufficient, appropriate evidence to address our audit objectives, we performed the procedures described below.

Statewide SAECK Tracking System

To determine to what extent MDAO participated in the statewide SAECK tracking system as required by Section 18X(g) of Chapter 6A of the General Laws, we took the following actions:

- We requested policies and procedures regarding the use of the Track-Kit system. MDAO informed us that it did not have any documented internal policies or procedures for how it should use the Track-Kit system during the audit period.
- We interviewed the chief of the Child Protection Unit about MDAO's use of the Track-Kit system. We were informed that MDAO rarely uses the Track-Kit system.
- We conducted a system walkthrough of MDAO's access to the data and observed that there were 583 SAECKs collected within MDAO's jurisdiction during the audit period in the Track-Kit system.
- We observed a virtual walkthrough of a sandbox² version of the prosecuting attorney and survivor portals within the Track-Kit system.
- We reviewed Track-Kit system access logs and determined that there were 21 active user accounts. We determined that 7 of the 21 users were former employees. Further, out of the 14 active users, only 1 user accessed the Track-Kit system during the audit period.

For this objective, we found certain issues during our testing regarding the extent to which MDAO participated in the statewide SAECK tracking system. See [Finding 1](#) and [Other Matters](#) for more information.

Cybersecurity Awareness Training

To determine whether MDAO adhered to Sections 6.2.3 and 6.2.4 of EOTSS's Information Security Risk Standard ISO.010 regarding cybersecurity awareness training, we took the following actions. First, we selected a random, nonstatistical³ sample of 40 employees from the population of 327 employees who were active during the audit period. We reviewed the MDAO cybersecurity awareness training platform's training certificates of completion to determine whether the sampled employees completed the required annual refresher cybersecurity awareness training. For sampled employees hired during the audit period, we determined whether the date on their certificate of completion was within 30 days of their hire date, as required by the EOTSS standard.

2. A sandbox is a staged, controlled environment that can be used for testing or demonstrating software without impacting live systems or sensitive data.

3. Auditors use nonstatistical 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.

We also determined the following:

- For calendar year 2022, 25 out of 40 sampled employees should have received annual refresher cybersecurity awareness training and 4 should have received initial cybersecurity training within 30 days of their hire date. None (0%) of the 25 employees received annual refresher training and none (0%) of the 4 new employees received the initial training.
- For calendar year 2023, 28 out of 40 sampled employees should have received annual refresher cybersecurity awareness training, and 8 should have received initial cybersecurity training within 30 days of their hire date. Of the 28 who should have received annual refresher training, 27 (96%) received training. MDAO could not provide evidence that 1 employee completed that training. Of the 8 new employees, 7 (88%) received initial cybersecurity training within 30 days, and 1 did not.
- For calendar year 2024, 32 employees out of 40 sampled employees should have received annual refresher cybersecurity awareness training, and 1 should have received initial cybersecurity training within 30 days of their hire date. Of the 32 employees who should have received annual training, all 32 (100%) received training. The 1 (100%) new employee received the initial cybersecurity training. Therefore, we noted no findings for 2024.

For this objective, we found certain issues during our testing regarding whether MDAO adhered to Sections 6.2.3 and 6.2.4 of EOTSS's Information Security Risk Standard ISO.010 regarding cybersecurity awareness training. See [Finding 3](#) for more information.

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

Employee Settlement Agreements

To determine whether MDAO had internal policies and procedures in place for (a) the review and approval of employee settlement agreements, including the use of non-disclosure, non-disparagement, or similarly restrictive clauses, and (b) the reporting of monetary employee settlements to CTR in accordance with 815 CMR 5.06 and 5.09, we took the following actions:

- We interviewed the District Attorney and the director of human resources. They stated that MDAO did not have any employee settlement agreements during the extended audit period.
- We inquired about internal policies and procedures regarding employee settlement agreements. We were informed that MDAO did not have any such documented policies.
- We inquired about internal policies and procedures regarding the use of non-disclosure, non-disparagement, and similarly restrictive language in employee settlement agreements. We were informed that MDAO did not have any such documented policies.

For this objective, we found certain issues during our testing; namely, that, while MDAO did not enter into any employee settlements during the extended audit period, it did not have a documented, transparent, or accountable process related to employee settlements agreements. See [Finding 2](#) for more information.

Data Reliability Assessment

Cybersecurity Awareness Training

To determine the reliability of MDAO's cybersecurity awareness training platform data, we interviewed MDAO management who were knowledgeable about the data. We reviewed System and Organization Control 2 reports⁴ covering the audit period. We ensured that certain information system control tests (i.e., access controls, security management, configuration management, contingency planning, and segregation of duties) had been performed without exception.

Employee Lists

We obtained from MDAO management a list of 327 employees who were active during the audit period. To ensure the reliability of the employee data, we tested the list to ensure that it did not contain certain dataset issues (i.e., duplicate records and employment start dates and end dates outside the audit period). To ensure the accuracy of the list, we compared the list of MDAO employees to a list of MDAO employee records obtained from the CTHRU statewide payroll website⁵ for calendar years 2022 through 2024. To ensure completeness of the active employee list, we traced the employee names listed from the CTHRU data back to the active employee list.

Employee Settlement Agreements

We requested a list of settlements executed during the extended audit period, July 1, 2019 through June 30, 2024. We were informed that MDAO did not enter into any settlement agreements with employees during the extended audit period.

To corroborate MDAO's statements, we contacted CTR to determine whether any employee settlement agreements were reported for MDAO in the CTR settlements and judgments Microsoft

-
4. A System and Organization Control report is a report, issued by an independent contractor, on controls about a service organization's systems relevant to security, availability, processing integrity, confidentiality, or privacy.
 5. According to the Office of the Comptroller of the Commonwealth's website, "CTHRU is an innovative open records platform, built and maintained by the Office of the Comptroller, that offers transparency into the finances and payroll of the Commonwealth of Massachusetts. CTHRU provides users with an intuitive experience for exploring how and where public money is utilized."

Access database during the extended audit period. CTR confirmed that there were no records of employee settlement agreements executed by MDAO in the database. We examined MDAO's personnel folders for a random, nonstatistical sample of 35 employees out of the population of 229 employees who separated from MDAO during the extended audit period for evidence of complaints, grievances, or settlement agreements and found none. We then ran a query from the Commonwealth Information Warehouse⁶ of all legal expenses paid by MDAO for the extended audit period. Using this data, we selected vendors that MDAO paid \$3,000 or more during the extended audit period and requested supporting invoices for all their legal expenses. We examined the invoices and confirmed that they did not contain settlement language in their descriptions.

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

6. The Commonwealth Information Warehouse contains budget, human resources, and payroll information as well as financial transaction data from the Massachusetts Management Accounting and Reporting System.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Middlesex County District Attorney's Office did not promptly revoke former employees' access rights within the statewide sexual assault evidence collection kit tracking system and did not complete certain data fields in the system.

During the audit period, the Middlesex County District Attorney's Office (MDAO) did not promptly revoke former employees' access rights to the Track-Kit system. Specifically, of the 21 active user accounts for the Track-Kit system, 7 of these users were former employees. Additionally, MDAO did not complete certain data fields (i.e., the assignment of MDAO's contact information in the system), despite this being part of the office's role within the Track-Kit system, as defined by the system's user manuals.

If MDAO does not promptly revoke former employees' access rights to the Track-Kit system, then there is a risk of unauthorized access to sensitive case and survivor information. Additionally, if MDAO does not assign its contact information to SAECKs, then the Track-Kit System is not being used as intended under statute. Having MDAO contact information assigned to SAECKs allows survivors to have an informed single point of contact and can streamline outreach and reduce confusion.

Authoritative Guidance

Section 18X(g) of Chapter 6A of the General Laws states, "District attorney offices shall participate in the statewide sexual assault evidence kit tracking system established in this section for the purpose of tracking the status of all sexual assault evidence kits."

The Track-Kit User Manual states that the role of the prosecuting attorney includes the following:

- *Review cases referred by law enforcement, if enabled.*
- *Assign [MDAO contact information] to a kit.*
- *Performing searches for kits available in the prosecuting attorney's jurisdiction.*

The Executive Office of Public Safety and Security's (EOPSS's) "Policies and Procedures for Sexual Assault Evidence Collection Kit Tracking," dated January 2020, requires district attorneys' offices to develop the following:

A policy to authorize access for new users of the system and to remove authorization from users who no longer require access, including users who have ended their employment, have been suspended, or terminated.

Further, Section 6.1.6. of the Executive Office of Technology Services and Security's (EOTSS's) Access Management Standard IS.003, dated July 15, 2020, states that access privileges should be removed "upon a transfer, termination or other significant change to a user's employment status or role."

Reason for Issue

MDAO did not have documented policies and procedures regarding the use of the Track-Kit system or the revocation of user access to the Track-Kit system upon termination of a user's employment.

Recommendations

1. MDAO should assign its contact information to each SAECK within its jurisdiction in the Track-Kit system and should train its employees on how to use this system.
2. MDAO should develop, document, and implement policies and procedures for Track-Kit system access authorization for new users and the revocation of access upon termination of users. These policies and procedures should include periodic access reviews at least semiannually to ensure that users' access rights are limited to their job requirements.

Auditee's Response

As of February 3, 2025, all access has been revoked for users who have either ended employment or no longer require access. That information was communicated to the Audit team at that time.

It is important to note that Track-Kit does not contain survivor-identifying information. User logs were provided to the Auditor's Office, which demonstrated that none of the former employees whose access was not previously revoked, accessed the system after separation. Thus, there was no improper access of case information.

The Middlesex District Attorney's Office has implemented a policy informing employees with access to the Track-Kit system of the requirement to enter contact information.¹ The policy includes a semiannual review, to be conducted by the Director of Information Technology, to ensure that only users who require access for their job requirements have authorized access to the Track-Kit system.

We have been informed that EOPSS is developing a technical training and we remain open to accepting any further guidance.

[Footnote:]

1. *All requested data has already been input into the Track-Kit System. On September 3, 2025, the Track-Kit system help desk advised [MDAO] that there was an error in the system that cut off some data from older kits which made it not possible to enter [assistant district attorney]*

and [victim witness advocate] information. This issue has been reported to the system administrator. Thus, we are presently in full compliance.

Auditor's Reply

Based on its response, MDAO 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.

2. The Middlesex County District Attorney's Office should have documented internal policies or procedures regarding state employee settlement agreements and supporting records, as would be best practice.

Even though MDAO did not enter into any settlement agreements during the extended audit period, July 1, 2019 through June 30, 2024, we found it should have had documented internal policies or procedures regarding employee settlement agreements during the extended audit period. We consider written policies to be best practice. We believe such policies and procedures should apply to the review, approval, processing, and reporting of employee settlement agreements, including the use of any non-disclosure or related clauses.

A documented, written process to handle employee settlement agreements, especially for those containing non-disclosure, non-disparagement, or similarly restrictive clauses, can help ensure that employee settlements are handled in an ethical, legal, and appropriate manner.

Authoritative Guidance

According to Section 5.09 of Title 815 of the Code of Massachusetts Regulations (CMR),

(1) Responsibility of assigned attorney or staff person: Preparation of Reports. When litigation involving a monetary claim against the Commonwealth covered by these regulation terminates in a final Settlement or judgment with regard to such a claim, the agency attorney or staff person assigned to handle or monitor the claim shall do the following:

(a) Prepare a report indicating:

- 1. the principal amount of the settlement or judgment;*
- 2. the amount of any attorney's fee award;*
- 3. the amount of any interest award or accrued, and whether the interest continues to accrue post-judgment;*
- 4. a request for payment of the amount;*

-
5. *a description of the basis for the request, (e.g., Court order or settlement agreement); and*
 6. *whether the assigned attorney desires to award the payment check to the claimant;*
- (b) *Forward the report with a copy of the settlement or judgment just described to the General Counsel of the Comptroller within the time frames set forth in 815 CMR 5.09(2). . . .*
- (2) *Time for preparation of reports. The report . . . shall be sent by the agency attorney to the General Counsel of the Comptroller:*
- (a) *if based on a settlement agreement, within 15 days of signing of the final settlement papers; or*
 - (b) *if based on a judgment against the Commonwealth or any agency, within fifteen days of the Commonwealth's decision not to appeal; or*
 - (c) *if based on a judgment against the Commonwealth or an agency, where the Commonwealth decides to take an appeal from the judgment, within fifteen days of any final order on appeal or in remand proceedings, if such remand proceedings are ordered.*

The US Government Accountability Office's *Standards for Internal Control in the Federal Government*, known as the Green Book, sets internal control standards for federal entities. The Green Book defines internal controls and recommends that government entities design and implement them in the following excerpt:

Internal control comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the entity. Internal control serves as the first line of defense in safeguarding assets. In short, internal control helps managers achieve desired results through effective stewardship of public resources. . . . Management should design control activities to achieve objectives and respond to risks. . . . Management should implement control activities through policies.

While MDAO is not required to follow this policy, since it is not a federal entity, we consider it a best practice.

Reason for Issue

MDAO management informed us that policies and procedures related to employee settlements have not been established because they do not support the use of such agreements and do not anticipate engaging in them.

Recommendation

MDAO should develop, document, and implement a written policy related to employee settlement agreements, including prohibiting the use of non-disclosure, non-disparagement, or similarly restrictive clauses in its agreements, as recommended in the Governor's "Executive Department Settlement Policy," issued January 27, 2025.

Auditee's Response

As the Auditor's report indicates, the Middlesex District Attorney's Office is not subject to any of the requirements regarding settlements that have been established by state executive order. Nevertheless, as of September 1, 2025, the Middlesex District Attorney's Office has modified its Employee Handbook to include a policy governing employee settlement agreements, particularly those containing non-disclosure, non-disparagement or similar restrictive clauses. This Handbook is issued to all employees and is accessible on the Office intranet. A copy of the policy has been provided to the Office of the State Auditor.

Auditor's Reply

Based on its response, MDAO 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.

3. The Middlesex County District Attorney's Office should ensure that all employees complete cybersecurity awareness training upon hire and annually thereafter.

MDAO should ensure that all employees complete cybersecurity awareness training.

Regarding calendar year 2022, we found that none of the 25 required employees in our sample of 40 completed annual refresher cybersecurity awareness training, and none of the 4 new employees completed initial cybersecurity awareness training within 30 days of their hire date.

Regarding calendar year 2023, we found that 1 of the 28 required employees in our sample of 40 did not complete annual refresher cybersecurity awareness training, and 1 of the 8 new employees did not complete initial cybersecurity awareness training within 30 days of their hire date.

The following table breaks down annual refresher and initial training completion for sampled MDAO employees who were active during the audit period.

Calendar Year	Annual Refresher Training Required	Annual Refresher Training Not Completed	Initial Training Required	Initial Training Not Completed	Not Applicable*
2022	25	25	4	4	11
2023	28	1	8	1	4
2024	32	0	1	0	7

* The Not Applicable column regards individuals who were not employed at MDAO in a given year. This would include, for example, employees who left MDAO employment before the training was assigned.

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

Authoritative Guidance

Section 6.2 of 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. This course will be conducted via web-based learning or in-class training and will be included in the new hire orientation checklist. 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 are required to complete Annual Security Awareness Training. Once implemented, automatic email reminders will be sent to personnel 12 months after course completion, alerting personnel to annual refresher training completion deadlines.

Although MDAO is not required to follow these standards, since it is not an executive branch state agency, we consider them best practices.

Reason for Issue

MDAO stated that it did not provide cybersecurity awareness training before 2023, though we note that it has been recommended by EOTSS since 2018.

Recommendation

MDAO should ensure that all employees complete annual refresher cybersecurity awareness training and that all newly hired employees complete the initial training within the first 30 days of their new hire orientation.

Auditee's Response

As the Auditor's report indicates, the Middlesex District Attorney's Office is not required to follow the guidance from EOTSS since it is not an Executive Branch state agency. However, in June 2022, the Office of the State Auditor recommended that the Massachusetts District Attorney's Association (MDAA) develop and implement policies and procedures requiring newly hired employees to receive cybersecurity awareness training. . . . Recognizing the value of such training, the Middlesex District Attorney's Office immediately adopted this guidance and purchased the . . . cybersecurity training platform. That training launched in January 2023, just six months after the Auditor's recommendation. As this audit shows, by 2024, the Office was in full compliance. As part of our ongoing commitment to information security, all new employees now complete the training immediately upon hire.

Auditor's Reply

Based on its response, MDAO 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.

OTHER MATTERS

Section 18X(g) of Chapter 6A of the Massachusetts General Laws does not clearly define the role of the district attorneys in the statewide sexual assault evidence collection kit tracking system.

During our audit of the Middlesex County District Attorney's Office (MDAO), we found that the law does not define the role of the district attorneys in the Track-Kit system; it just requires district attorneys to participate in the system for the purpose of tracking the status of all sexual assault evidence collection kits (SAECKs). Specifically, Section 18X(g) of Chapter 6A of the Massachusetts General Laws states, "District attorney offices shall participate in the statewide sexual assault evidence kit tracking system established in this section for the purpose of tracking the status of all sexual assault evidence kits."

We asked the Executive Office of Public Safety and Security (EOPSS) what the role of a district attorney's office is regarding the Track-Kit system. EOPSS told us that the primary role for a district attorney's office is to use the system, but what they do with it is up to them. Further, according to user manuals within the Track-Kit system's Help Center, the role of district attorneys in the system is as follows:

The prosecuting attorney's role in Track-Kit is to:

- *Review cases referred by law enforcement, if enabled.*
- *Assign [MDAO contact information] to a kit.*
- *Perform searches for kits available in the prosecuting attorney's jurisdiction.*

We inquired EOPSS about this and were informed that this was included in the system based on frequently asked questions from various district attorneys about their role within the system. EOPSS offered trainings in the use of the Track-Kit system to various district attorney offices in 2019, outside the audit period, but we were unable to determine the participation of MDAO staff members during the course of our audit.

Beyond these trainings, there has not been clarification or guidance—from either EOPSS or the law—on what district attorneys are required to do to participate in the system for the purpose of tracking the status of all SAECKs. Because of this, the Track-Kit system has been used inconsistently across the Commonwealth's district attorney offices. MDAO management told us during interviews that the agency rarely used the Track-Kit system; they provided user activity logs during the audit period that supported their statements. MDAO management also told us that they generally opt to use the Massachusetts State

Police Crime Lab's Laboratory Information Management System to obtain testing results for SAECKs within the office's jurisdiction.

The Track-Kit system was designed to increase transparency, accountability, and survivor-centered care in the handling of SAECKs. If the role of the district attorneys in the Track-Kit system is not clearly defined, then there could be inconsistent use of the system across district attorneys' offices, which may limit the effectiveness of the system.

MDAO should work with EOPSS to clearly define and standardize its role in the Track-Kit system.