

# OFFICE OF THE STATE AUDITOR

---

# DIANA DIZOGLIO

Official Audit Report – Issued November 25, 2025

---

## Essex County District Attorney's Office

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

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



OFFICE OF THE STATE AUDITOR

---

**DIANA DIZOGLIO**

November 25, 2025

District Attorney Paul F. Tucker  
Essex County District Attorney's Office  
10 Federal Street  
Salem, MA 01970

Dear District Attorney Tucker:

I am pleased to provide to you the results of the enclosed performance audit of the Essex 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 the Essex County District Attorney's Office, 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 Essex 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

<b>EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>OVERVIEW OF AUDITED ENTITY .....</b>	<b>3</b>
<b>AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY .....</b>	<b>7</b>
<b>DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE .....</b>	<b>13</b>
1. The Essex 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.....	13
2. The Essex County District Attorney's Office should ensure that all of its employees complete cybersecurity awareness training. ....	15
3. The Essex County District Attorney's Office should have documented internal policies and procedures regarding state employee settlement agreements, as would be best practice. ....	17
<b>OTHER MATTERS.....</b>	<b>19</b>

---

## LIST OF ABBREVIATIONS

CMR	Code of Massachusetts Regulations
CTR	Office of the Comptroller of the Commonwealth
EDAO	Essex County District Attorney's Office
EOPSS	Executive Office of Public Safety and Security
EOTSS	Executive Office of Technology Services and Security
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 Essex County District Attorney's Office (EDAO) for the period July 1, 2022 through June 30, 2024. When examining employee settlement agreements, we extended the audit period to July 1, 2019 through June 30, 2024.

The purpose of our audit was to determine the following:

- the extent to which EDAO participated in the statewide sexual assault evidence kit (SAECK) tracking system in accordance with Section 18X(g) of Chapter 6A of the General Laws;
- whether EDAO ensured that its employees completed cybersecurity awareness training, in accordance with its "Security Training and Awareness" policy and Section 6.2.3 of the Executive Office of Technology Services and Security's Information Security Risk Management Standard IS.010; and
- whether EDAO 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 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.

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

<b>Finding 1</b> <b>Page <a href="#">13</a></b>	EDAO did not promptly revoke former employees' access rights within the statewide SAECK tracking system and did not complete certain data fields in the system.
<b>Effect</b>	If EDAO does not promptly revoke former employees' access rights to the Track-Kit system, then there is a higher-than-acceptable risk of unauthorized access to sensitive case and survivor information. Additionally, if EDAO does not assign its contact information to SAECKs, then the Track-Kit system is not being fully used as intended. Having EDAO contact information assigned to SAECKs allows survivors to have an informed single point of contact and can streamline outreach and reduce confusion.
<b>Recommendations</b> <b>Page <a href="#">14</a></b>	<ol style="list-style-type: none"><li>1. EDAO should develop, document, and implement policies and procedures for adding access authorization for new users and revoking user access to the Track-Kit system upon termination of a user's employment. These policies and procedures should incorporate periodic access reviews (at least semiannually) to ensure that users' access rights are limited to their individual job requirements.</li><li>2. EDAO 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.</li></ol>
<b>Finding 2</b> <b>Page <a href="#">15</a></b>	EDAO should ensure that all of its employees complete cybersecurity awareness training.

<b>Effect</b>	If EDAO does not ensure that all of its employees complete cybersecurity awareness training, then EDAO exposes itself to an increased risk of cybersecurity attacks and financial and/or reputational losses.
<b>Recommendation Page <u>16</u></b>	EDAO should implement effective monitoring controls to ensure that all employees complete agency-required bimonthly cybersecurity awareness training and that newly hired employees complete initial training within the first 30 days of their new hire orientation.
<b>Finding 3 Page <u>17</u></b>	EDAO should have documented internal policies and procedures regarding state employee settlement agreements, as would be best practice.
<b>Effect</b>	If EDAO does not have a documented process by which it handles employee settlement agreements, especially those containing non-disclosure, non-disparagement, or similarly restrictive clauses, then it cannot ensure that employee settlements are handled in an equitable, ethical, legal, and consistent manner.
<b>Recommendations Page <u>18</u></b>	<ol style="list-style-type: none"><li>1. EDAO should update its "Policies, Procedures, and Guidelines—Settlements and Judgments," effective July 2024, to include review and approval of agreement terms by the District Attorney and chief legal counsel.</li><li>2. EDAO should ensure that its "Policies, Procedures, and Guidelines—Settlements and Judgments," effective July 2024, is formally communicated to all relevant employees and fully integrated into its operations.</li></ol>

---

## OVERVIEW OF AUDITED ENTITY

The Essex County District Attorney's Office (EDAO) 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.

EDAO is one of 11 district attorneys' offices in the Commonwealth and represents the Commonwealth in the prosecution of criminal offenses occurring within its jurisdiction. EDAO serves the 34 cities and towns that make up Essex County. EDAO's principal administrative and accounting office is located in Salem. In addition, EDAO maintains site offices at eight district courts throughout the county. As of June 30, 2024, EDAO employed 197 individuals, including 70 district attorneys and assistant district attorneys. The current District Attorney was sworn into office on January 2, 2023.

According to EDAO's 2024 Annual Report,

*With a primary mission of keeping Essex County residents safe, the District Attorney's office prosecutes criminal offenses in our communities in both Essex County Superior Court and in District Court locations throughout the county. The Office of the Essex County District Attorney is staffed with exceptional professional attorneys who specialize in handling cases ranging from homicide to child physical and/or sexual abuse to domestic violence and motor vehicle crimes, among many others.*

During fiscal years 2023 and 2024, EDAO received state appropriations of \$12,560,466 and \$14,216,949, respectively.

### 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 tracking system for sexual assault evidence collection kits (SAECKs).<sup>1</sup> EOPSS implemented the Track-Kit system, a web-based platform designed to trace SAECKs from distribution through collection, processing, and storage. Key users of the system include the following:

- medical facilities that perform sexual assault forensic examinations;

---

1. A SAECK is a sealed box containing a detailed protocol and all the medical equipment to conduct a thorough forensic medical exam of sexual assault survivors at the time of the assault. Police or prosecutors can use evidence collected in criminal investigation or prosecution.

- law enforcement agencies that transport the kits and conduct investigations; and
- crime laboratories that perform testing and reporting.

Survivors of sexual assault can access a specialized web portal to track the location and testing status of their own kits, enhancing transparency and empowerment throughout the process.

Section 18X(g) of Chapter 6A of the General Laws requires district attorneys' offices to participate in the statewide sexual assault evidence kit tracking system for the purpose of tracking the status of all sexual assault evidence kits.

The Track-Kit system provides district attorneys' offices, including EDAO, with several key functions to support their role in handling sexual assault cases. The system allows district attorneys' offices to assign the direct contact information of a prosecutor or victim witness advocate to a specific SAECK, helping to facilitate communication and support for survivors. District attorneys' offices can also search for SAECKs that were collected within their jurisdiction and have been assigned to their office, enhancing their ability to monitor and manage case-related evidence throughout the investigative and prosecutorial process.

According to data we obtained from the Track-Kit system, a total of 272 SAECKs within EDAO's jurisdiction were collected and entered into the system by a medical facility during the audit period.

According to the EOPSS 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. . . . 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**

EDAO's "Security Training and Awareness" policy requires all employees to complete bimonthly cybersecurity awareness training, for a total of six unique trainings per year, and requires new employees to complete training when first hired.



Additionally, the Executive Office of Technology Services and Security (EOTSS) has established policies and procedures that apply to all Commonwealth agencies within the executive branch. EOTSS recommends, but does not require, non-executive branch agencies to follow these policies and procedures. Section 6.2.3 of EOTSS's Information Security Risk Management Standard IS.010<sup>2</sup> required that all newly hired employees complete an initial cybersecurity awareness training course within 30 days of their orientation. Since EDAO's policy does not specify a timeframe for this initial training, we used EOTSS's standard as a best practice to measure EDAO's performance during the audit period in this area.

EDAO used a third-party, web-based training program to provide and track EDAO's cybersecurity awareness training during the audit period.

## State Employee Settlement Agreements

The Office of the Comptroller of the Commonwealth (CTR) has established policies and procedures for Commonwealth agencies processing settlements and judgments.

CTR's "Settlements and Judgments Policy," dated January 10, 2022 and in effect during the audit period stated,

*A settlement or judgment results from a formal claim (grievance, complaint or law suit) 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 EDAO for the period of July 1, 2019 through June 30, 2024.

Section 5.00 of Title 815 of the Code of Massachusetts Regulations describes the procedures for agencies to determine the availability of funds for the payment of settlements and judgments against the Commonwealth, as well as reporting requirements. The regulation requires agencies to prepare and

---

2. The Executive Office of Technology Services and Security updated 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).

submit a report to CTR's general counsel before making the payment to ensure proper tax reporting. When reporting employee settlements to CTR, state 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, agency information, employee's information, the type and amount of damages detailed in the settlement, amount of any attorney's fees awarded, and the amount of any interest awarded or accrued. Additionally, agencies must include a copy of the employee settlement agreement signed by authorized representatives of both parties when they submit the Authorization Form.

We found that EDAO had not entered into any employee settlement agreements during the audit period.

## 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 Essex County District Attorney's Office (EDAO) for the period July 1, 2022 through June 30, 2024. When examining employee settlement agreements, 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.

Objective	Conclusion
1. To what extent did EDAO 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?	<b>To an insufficient extent; see Finding <u>1</u> and <u>Other Matters</u></b>
2. Did EDAO ensure that all of its employees completed cybersecurity awareness training in accordance with its "Security Training and Awareness" policy and Section 6.2.3 of the Executive Office of Technology Services and Security's (EOTSS's) Information Security Risk Standard IS.010?	<b>No; see Finding <u>2</u></b>
3. Did EDAO 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)?	<b>No; see Finding <u>3</u></b>

To accomplish our audit objectives, we gained an understanding of the EDAO internal control environment relevant to our objectives by reviewing applicable policies, procedures, and its internal control plan, as well as by interviewing EDAO management and employees. We also reviewed Track-Kit system user manuals, which included user roles for prosecuting attorneys. We evaluated the design and

implementation of the internal controls related to our audit objectives. We tested the operating effectiveness of internal controls related to the monitoring of employee cybersecurity awareness training.

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 EDAO participated in the statewide SAECK tracking system as required by Section 18X(g) of Chapter 6A of the General Laws, we performed the following procedures:

- We requested policies and procedures regarding the use of the Track-Kit system. EDAO informed us that it did not have any documented internal policies or procedures for how it should use the Track-Kit system.
- We interviewed EDAO officials about EDAO's use of the Track-Kit system. We were informed that EDAO does not and has not used it.
- We conducted a walkthrough of the Track-Kit system with EDAO, observing the current status and test results of kits, as well as system reports for the 272 SAECKs collected within EDAO's jurisdiction during the audit period. We also observed a sandbox<sup>3</sup> version of the prosecuting attorney and survivor portals within the Track-Kit system with the Executive Office of Public Safety and Security (EOPSS).
- We reviewed Track-Kit system access logs for EDAO and compared the listed user accounts to EDAO's current employee list.

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

## **Cybersecurity Awareness Training**

To determine whether EDAO ensured that all of its employees completed cybersecurity awareness training, in accordance with its "Security Training and Awareness" policy and Section 6.2.3 of EOTSS's Information Security Risk Management Standard IS.010, we took the actions described below.

We obtained a list of 197 employees who were employed by EDAO during the audit period. We grouped these 197 EDAO employees into the following two categories: 63 EDAO employees with hire dates during

---

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

the audit period (i.e., newly hired employees)—who were required to complete initial cybersecurity awareness training—and 134 EDAO employees with hire dates before the audit period (i.e., existing employees)—who were required to complete bimonthly cybersecurity awareness training.

We selected a random, nonstatistical sample<sup>4</sup> of 35 existing employees from the population of 134 and another random nonstatistical sample of 20 newly hired employees from the population of 63.

To determine whether EDAO ensured that its employees within our two samples completed cybersecurity awareness training—the bimonthly training for our sample of 35 existing employees and the initial training for our sample of 20 newly hired employees—we took the actions described below for each sample.

We obtained a report of all the 1,599 cybersecurity awareness trainings completed during the audit period from EDAO's training system. We inspected this report to determine whether there were cybersecurity awareness training completion dates recorded for each of the 35 existing employees.

To assess the timeliness of cybersecurity awareness trainings, we compared the training completion date to the training due date for all 1,599 training records to determine whether trainings were completed within five weeks of enrollment in accordance with EDAO's internal training policy.

Additionally, for the newly hired employees in our sample, we compared their hire dates from the EDAO employee list to the dates on which they completed their initial cybersecurity awareness training, based on the training activity report for the audit period. We calculated the number of days it took each of the newly hired employees to complete the initial cybersecurity awareness training to determine whether the number of days for each newly hired employee was within 30 days of their hire date.

For this objective, we found certain issues during our testing; namely, that EDAO did not ensure that all of its employees completed cybersecurity awareness training. See [Finding 2](#) for more information.

## **State Employee Settlement Agreements**

We requested a list of all employee settlements and complaints from a five-year period (July 1, 2019 through June 30, 2024). We were advised that EDAO had not entered into any settlement agreements

---

4. 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.

with employees since the current administration began in January 2023, and EDAO management was not aware of any such settlements under the prior administration.

To corroborate EDAO's statements, we performed the following procedures:

- We contacted CTR to determine whether any EDAO employee settlements were reported in the CTR Settlement and Judgment Access database during the audit period. CTR confirmed that there were no records of employee settlements in the database.
- We examined all eight EDAO employee complaints for the five-year audit period. We reviewed the complaint dates, descriptions of the complaints, actions administered or recommended, and the results of the complaints and determined that none of these complaints resulted in an employee settlement.
- We selected a random, nonstatistical sample of five terminated employees from a population of 44 during the period and inspected their personnel files to determine whether any of them had employee settlements related to their termination. We determined that none of these terminations resulted in an employee settlement.
- We then ran a data extract from the Commonwealth Information Warehouse<sup>5</sup> of all external legal expenses paid by EDAO for the period July 1, 2019 through June 30, 2024. For a random, nonstatistical sample of 30 legal expense records from a population of 549 attorneys and legal support service expenses during the period, we requested supporting invoices. We reviewed the vendor names, invoice dates, amounts, invoice numbers, and descriptions of work performed for any mention of employee settlement agreements. No employee settlements were identified as a result of this review.

To determine whether EDAO had internal policies and procedures in place for (a) the review and approval of employee settlement agreements, including the language used, and (b) the reporting of employee settlement agreements to CTR, we performed the following procedures:

- We conducted interviews with EDAO's chief financial officer, chief legal counsel, and director of human resources because they were knowledgeable about the employee settlement process. They told us that EDAO follows CTR's "Settlements and Judgments Policy" for monetary employee settlement agreements.
- We inquired about internal policies and procedures regarding entering into, approving, and processing employee settlement agreements. We obtained from EDAO its "Policies, Procedures, and Guidelines—Settlements and Judgments," an internal policy that requires the chief legal counsel, chief fiscal officer, and director of human resources to ensure that claims against the agency are negotiated and processed in compliance with 815 CMR 5.00. However, we noted that this policy became effective in July 2024 and, therefore, was not applicable to the audit period.

---

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

- We inquired about internal policies and procedures regarding the use of non-disclosure, non-disparagement, non-publication, and similarly restrictive language in settlement agreements. EDAO management explained that the District Attorney and chief legal counsel would review and approve the terms and language of any settlement agreement before execution. We also found that EDAO's "Policies, Procedures, and Guidelines—Settlements and Judgments," which went into effect in July 2024, did not describe this practice.

We did not perform testing on the reporting to CTR because we did not identify any employee settlement agreements executed during the extended audit period. See [Finding 3](#) for more information.

We used a nonstatistical sampling method for testing and, therefore, did not project the results of our testing to the corresponding populations.

## Data Reliability Assessment

### Cybersecurity Awareness Training

We obtained from EDAO a list of the 197 employees who were employed during the audit period. To determine the reliability of the list, we checked it for duplicate records and checked that employment start dates and termination dates were within the audit period. We traced employee names, identification numbers, and job titles from the employee list provided by EDAO to payroll summary data that we extracted from CTHRU, the Commonwealth's statewide payroll open records system.

Further, we verified employee names, employment statuses, employee titles, hire dates, and termination dates (if applicable) for a random sample of 10 employees from the list to physical personnel files maintained by EDAO. Additionally, we vouched employee names, employment statuses, employee titles, hire dates, and termination dates (if applicable) from a random sample of 10 personnel files to the employee list provided by EDAO.

To determine the reliability of the cybersecurity awareness training data obtained from EDAO's cybersecurity awareness training system, we reviewed System and Organization Control 2 Reports<sup>6</sup> covering the entire audit period. We ensured that certain information system control tests (access controls, security management, configuration management, contingency planning, and segregation of duties) had been performed without exception. We reviewed enrollment dates to ensure that the bimonthly trainings offered fell within the audit period. Additionally, we inspected the data for any

---

6. 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.

hidden rows and columns. According to EDAO management, this is the only record of enrollment and completion of cybersecurity awareness training for EDAO employees.

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.



## DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

### **1. The Essex 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 Essex County District Attorney's Office (EDAO) did not promptly revoke former employees' access rights to the Track-Kit system. Specifically, of the 7 active user accounts for the Track-Kit system, 2 of these users were former employees. Additionally, EDAO did not complete certain data fields (i.e., the assignment of EDAO's contact information in the system), despite this being part of the office's role within the Track-Kit system and having the capability to do so.

If EDAO does not promptly revoke former employees' access rights to the Track-Kit system, then there is a higher-than-acceptable risk of unauthorized access to sensitive case and survivor information. Additionally, if EDAO does not assign its contact information to SAECKs, then the Track-Kit system is not being fully used as intended. Having EDAO 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 [EDAO contact information] to a kit.*
- *Performing searches for kits available in the prosecuting attorney's jurisdiction.*

EOPSS's "Policies and Procedures for Sexual Assault Evidence Collection Kit Tracking," dated January 2020, requires district attorneys' offices to develop "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."

## Reasons for Issue

EOPSS offered voluntary trainings on the use of the Track-Kit system to district attorneys' offices in 2019, but we did not find any evidence that EDAO staff members attended this training. EDAO management told us that they generally opt to use the Massachusetts State Police Crime Lab's Legal Access Web-Based System, a laboratory information system, to obtain testing results for SAECKs associated with EDAO's active cases. 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 (see Other Matters). According to EDAO management, staff members at EDAO have the discretion to use the system as they see fit.

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

## Recommendations

1. EDAO should develop, document, and implement policies and procedures for adding access authorization for new users and revoking user access to the Track-Kit system upon termination of a user's employment. These policies and procedures should incorporate periodic access reviews (at least semiannually) to ensure that users' access rights are limited to their individual job requirements.
2. EDAO 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.

## Auditee's Response

*We acknowledge our statutory obligation to actively participate in the statewide sexual assault evidence collection kit (SAECK) tracking system, known as Track-Kit. We will take immediate steps to ensure EDAO becomes fully compliant with this requirement.*

*We will work with the Executive Office of Public Safety and Security (EOPSS) to clearly define and standardize our role in the Track-Kit system. This will include seeking clarification about best practices and standardization for the system's use. EDAO will also develop, document, and implement policies and procedures for adding new users and for revoking user access upon termination of employment. These procedures will incorporate periodic access reviews at least semiannually to ensure that user access rights are limited to their individual job requirements.*

*It is important to note, however, that the office has not experienced any discernible adverse impact on cases as a result of using the Massachusetts State Police Crime Lab's Legal Access Web-Based System (LIMS) in place of the Track-Kit system. While this is not an excuse for non-compliance, it serves as an explanation of our past practice. We are fully committed to fulfilling our statutory obligations moving forward.*

## **Auditor's Reply**

EDAO states in its response that it “has not experienced any discernible adverse impact on cases” from using the Massachusetts State Police Crime Lab’s Legal Access Web-Based System instead of the Track-Kit system. The Track-Kit system, like the law that implemented it, was designed to serve survivors of sexual assault, not only to serve as a case management system for district attorneys’ offices. Full participation in the Track-Kit system is necessary to meet the law’s intent and ensure consistent, survivor-centered practices across the Commonwealth.

Based on its response, EDAO is taking 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 Essex County District Attorney's Office should ensure that all of its employees complete cybersecurity awareness training.**

EDAO should ensure that all of its employees complete cybersecurity awareness training.

We found that 10 out of 35 (29%) EDAO employees in our sample did not complete all of the required bimonthly cybersecurity awareness training.

Additionally, we found that of the 1,599 training records we reviewed, 235 (15%) of trainings were completed after the five-week deadline. As a result, we determined that EDAO was not in compliance with its internal cybersecurity awareness training policy.

We also found that 10 out of 20 (50%) EDAO employees in our sample who were hired during the audit period did not complete cybersecurity training within 30 days of new hire orientation. Seven of these 10 newly hired employees completed the training after the 30-day deadline, and the remaining 3 newly hired employees did not complete training at all.

If EDAO does not ensure that all of its employees complete cybersecurity awareness training, then EDAO exposes itself to an increased risk of cybersecurity attacks and financial and/or reputational losses.

## **Authoritative Guidance**

According to the training schedule outlined in EDAO’s “Security Awareness Training” policy, “Six trainings are scheduled throughout each calendar year. . . . generated in February, **April**, June, August, October,

**December.** [In this policy, April and December are bolded to indicate that those sessions are longer than the others.] Trainings must be completed within 5 weeks of enrollment.”

According to Section 6.2.3 of the Executive Office of Technology Services and Security's Information Security Risk Standard IS.010, “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.”

## Reasons for Issue

EDAO did not have effective monitoring controls in place to ensure that all of its employees completed the required initial and bimonthly cybersecurity awareness trainings.

## Recommendation

EDAO should implement effective monitoring controls to ensure that all employees complete agency-required bimonthly cybersecurity awareness training and that newly hired employees complete initial training within the first 30 days of their new hire orientation.

## Auditee's Response

*The EDAO is committed to ensuring all employees receive proper cybersecurity training. The EDAO's "Security Training and Awareness" policy requires all employees to complete bimonthly cybersecurity awareness training. We acknowledge that some employees in your sample did not complete the required training within the 30-day new hire period or the bimonthly schedule. The Executive Office of Technology Services and Security (EOTSS) Information Security Risk Management Standard IS.010 recommends new employees complete this training within 30 days of their orientation. The EDAO's policy does not specify a timeframe for initial training. All new personnel are required to complete an initial Security Awareness Training, and while a number of employees completed it outside the 30-day period, all required trainings were eventually completed.*

*We recognize that our monitoring controls were not as effective as they should have been. To address this, we will implement more rigorous monitoring to ensure all new employees complete their initial training within the first 30 days of their new hire orientation, and that all existing employees complete the required bimonthly trainings in a timely manner. We are dedicated to mitigating the risk of cybersecurity attacks and protecting sensitive information.*

## Auditor's Reply

Based on its response, EDAO is taking 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 Essex County District Attorney's Office should have documented internal policies and procedures regarding state employee settlement agreements, as would be best practice.**

EDAO should have documented policies and procedures to manage employee separation or settlement agreements, including the use of non-disclosure, non-disparagement, or similarly restrictive clauses. We found that EDAO's internal settlement policy provided to us was dated July 2024 and, therefore, was not in effect during the period under review. During interviews, EDAO management told us that the agency would not be inclined to use non-disclosure language within the context of employee settlement agreements. The District Attorney and agency counsel would review and approve the terms and language of any employee settlement agreements before execution. However, we found that the internal policy document provided to us did not describe this practice.

If EDAO does not have a documented process by which it handles employee settlement agreements, especially those containing non-disclosure, non-disparagement, or similarly restrictive clauses, then it cannot ensure that employee settlements are handled in an equitable, ethical, legal, and consistent manner.

#### **Authoritative Guidance**

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 in the following way:

*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 EDAO is not required to follow this policy, since it is not a federal entity, we consider it to be a best practice.

#### **Reasons for Issue**

EDAO officials could not explain why they did not have documented policies and procedures regarding employee settlement agreements in place during the audit period.

## Recommendations

1. EDAO should update its "Policies, Procedures, and Guidelines—Settlements and Judgments," effective July 2024, to include review and approval of agreement terms by the District Attorney and chief legal counsel.
2. EDAO should ensure that its "Policies, Procedures, and Guidelines—Settlements and Judgments," effective July 2024, is formally communicated to all relevant employees and fully integrated into its operations.

## Auditee's Response

*During the audit period, the EDAO did not have a documented, internal policy for employee settlement agreements. We relied on the Office of the Comptroller's (CTR) "Settlements and Judgments Policy," which was in effect from January 10, 2022, to handle monetary settlements. Your audit found that the EDAO did not enter into any employee settlement agreements during the entire five-year review period from July 1, 2019, through June 30, 2024. Furthermore, no non-disclosure, non-disparagement, or similarly restrictive clauses were used in any settlement agreements during this time.*

*Just outside the audit period, in July 2024, the EDAO created its own "Policies, Procedures, and Guidelines-Settlements and Judgments". We have revised this policy to formalize a documented and transparent process for handling any future employee settlements. . . . This will ensure that such matters are handled in a legal, ethical, and consistent manner, with terms and language reviewed and approved by the District Attorney and chief legal counsel.*

## Auditor's Reply

Based on its response, EDAO is taking 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 district attorneys in the statewide sexual assault evidence collection kit tracking system.**

During our audit of the Essex County District Attorney's Office (EDAO), we found that the law does not define the role of 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 kits. 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 Help Center in the Track-Kit system, 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 [EDAO contact information] to a kit.*
- *Perform searches for kits available in the prosecuting attorney's jurisdiction.*

We inquired with 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 voluntary training on the use of the Track-Kit system to district attorneys' offices in 2019, but we did not find any evidence that EDAO staff members attended these trainings.

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 kits. Due to this, there has been inconsistent use of the Track-Kit system across the Commonwealth's district attorneys' offices. EDAO management told us in interviews that the agency did not use the Track-Kit system during the audit period and does not currently use it. They 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.

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