OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued November 25, 2025

Cape and Islands District Attorney's Office

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

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

OFFICE OF THE STATE AUDITOR
DIANA DIZOGLIO

November 25, 2025

Robert J. Galibois, District Attorney
Cape and Islands District Attorney's Office
3231 Main Street
Barnstable, MA 02630

Dear District Attorney Galibois:

I am pleased to provide to you the results of the enclosed performance audit of the Cape and Islands 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 executed by CIDAO, 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 Cape and Islands 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

LIST OF ABBREVIATIONS

CIDAO	Cape and Islands District Attorney's Office
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
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 Cape and Islands District Attorney's Office (CIDAO) for the period July 1, 2022 through June 30, 2024. When examining employee settlement agreements executed by CIDAO, we extended the audit period to July 1, 2019 through June 30, 2024.

The purpose of this audit was to determine the following:

- whether CIDAO had policies and procedures in place to participate in the statewide sexual assault evidence collection kit (SAECK) tracking system in accordance with Section 18X(g) of Chapter 6A of the General Laws;
- whether CIDAO ensured that its employees received cybersecurity awareness training in accordance with the requirements in Sections 6.2.3 and 6.2.4 of the Executive Office of Technology Services and Security's[1] Information Security Risk Management Standard IS.010;
- whether CIDAO 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 employee settlement agreements to the Office of the Comptroller of the Commonwealth (CTR); and
- whether CIDAO reported all monetary employee settlement agreements entered into from July 1, 2019 through June 30, 2024 to CTR in accordance with CTR's Settlements and Judgments Policy and 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 recommendations, with hyperlinks to each page listed.

Finding 1 **Page 13**	CIDAO 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 CIDAO 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 CIDAO does not assign its contact information to SAECKs, then the Track-Kit System is not being used as intended under statute. Having CIDAO contact information assigned to SAECKs allows survivors to have an informed single point of contact and can streamline outreach and reduce confusion.

1. The Executive Office of Technology Services and Security 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).

Recommendations Page 14	1. CIDAO 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 the system. 2. CIDAO 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 15	CIDAO 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. Additionally, if CIDAO does not maintain documentation regarding severance agreements, then it cannot determine whether the severance agreements included a release of future claims clause that would then require CIDAO to report the agreements to CTR.
Recommendations Page 18	1. CIDAO 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. 2. CIDAO should maintain all records related to all types of employee settlement and severance agreements, particularly those that include a written release of future claims against CIDAO, in accordance with Massachusetts public records laws and the Massachusetts Records Retention Schedule. 3. CIDAO should work with CTR to ensure that CIDAO understands the reporting requirements for all types of monetary employee settlement and severance agreements and ensure that CIDAO reports those agreements to CTR.
Finding 3 Page 20	CIDAO should ensure that all employees complete cybersecurity awareness training when hired and annually thereafter.
Effect	Without educating its employees on their responsibility to protect the security of information assets, CIDAO exposes itself to a higher risk of cybersecurity attacks and financial and/or reputational losses.
Recommendations Page 21	1. CIDAO should ensure that all employees complete annual cybersecurity awareness training and that all newly hired employees complete initial training within the first 30 days of their new hire orientation. 2. CIDAO should design and implement policies and procedures to ensure that its employees complete cybersecurity awareness training. Additionally, CIDAO should retain copies of cybersecurity awareness training certificates as evidence that its employees completed the training.

OVERVIEW OF AUDITED ENTITY

The Cape and Islands District Attorney's Office (CIDAO) 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.

CIDAO is one of 11 district attorneys' offices in the Commonwealth and represents the Commonwealth in criminal cases in three superior courts, five district courts, five juvenile courts, the Massachusetts Appeals Court, and the Massachusetts Supreme Judicial Court. It operates five offices in Barnstable, Falmouth, Orleans, Edgartown, and Nantucket and serves 23 towns across Barnstable, Dukes, and Nantucket Counties. According to US Census Bureau estimates as of July 1, 2024, the combined population of these three counties is 268,301 full-time residents. The total population is estimated to increase to over 500,000 people during the summer vacation season, from May through September.

The current District Attorney was sworn into office on January 4, 2023, as the first new administration in 20 years and only the third administration since CIDAO was established in 1971.

According to its 2024 internal control plan, CIDAO's mission statement is as follows: "The Cape and Islands District Attorney's office, in partnership with the communities we serve, is dedicated to the pursuit of truth and justice, protection of the innocent, and ensuring the safety of the public."

During fiscal years 2023 and 2024, CIDAO received state appropriations of $5,838,807 and $6,647,739, respectively. CIDAO had 67 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 provides district attorneys' offices, including CIDAO, with the ability to do the following:

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

During the audit period, 129 SAECKs were collected in CIDAO's jurisdiction and entered into the Track-Kit system.

Further, EOPSS's website provides the following guidance:

> *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 agencies to follow these policies and procedures. Section 6.2 of EOTSS's Information Security Risk Management Standard IS.010 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 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.

CIDAO used the KnowBe4 training platform during the entire audit period (fiscal years 2023 and 2024) to administer cybersecurity awareness training.

Settlements and Judgments

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 states,

> *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 CIDAO for the period of July 1, 2019 through June 30, 2024.

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

The regulation requires 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 agencies use a Non-Tort Settlement/Judgment Payment Authorization Form (referred to in this report as an 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, the amount of any attorney 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 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 Cape and Islands District Attorney's Office (CIDAO) for the period July 1, 2022 through June 30, 2024. When examining employee settlement agreements entered into by CIDAO, 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 the CIDAO 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 1 and Other Matters**
2. Did CIDAO 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 Management Standard IS.010 with regard to cybersecurity awareness training?	**No; see Finding 3**
3. Did CIDAO 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 CTR in accordance with Sections 5.06 and 5.09 of Title 815 of the Code of Massachusetts Regulations (CMR)?	**No; see Finding 2**

To accomplish our audit objectives, we gained an understanding of the CIDAO internal control environment relevant to our objectives by reviewing applicable policies, procedures, and its internal control plan, as well as by interviewing CIDAO officials. We also reviewed Track-Kit system user manuals, which included user roles for prosecuting attorneys. We evaluated the design and implementation, and tested the operating effectiveness, of internal controls related to the monitoring of employee training, as

well as the approval of executed employee settlement agreements. See Findings 1, 2, and 3 for more information.

Statewide SAECK Tracking System

To determine whether CIDAO 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. CIDAO informed us that it did not have any documented internal policies and procedures for how it should use the Track-Kit system.
- We interviewed the first assistant district attorney and the information technology director about CIDAO's use of the Track-Kit system. We were informed that CIDAO does not and has not used it.
- While CIDAO did have access to the Track-Kit system dashboard, we determined that CIDAO did not have access to SAECK data within its jurisdiction within the Track-Kit system. It appears that CIDAO did not have access to the data for SAECKS because CIDAO never requested this data from the Executive Office of Public Safety and Security (EOPSS). Once CIDAO gained access to the data for SAECKS within the Track-Kit system during the course of our audit, we observed that there were 129 SAECKs collected within CIDAO's jurisdiction during the audit period in the Track-Kit system.
- We observed a sandbox[2] version of the prosecuting attorney and survivor portals within the Track-Kit system from EOPSS.
- We reviewed Track-Kit system access logs from CIDAO and determined that there were 14 active user accounts. We determined that 10 of the 14 user accounts were for former employees. Further, no active users accessed the Track-Kit system during the audit period.

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

Cybersecurity Awareness Training

To determine whether CIDAO adhered to Sections 6.2.3 and 6.2.4 of EOTSS's Information Security Risk Management Standard IS.010 with regard to cybersecurity awareness training, we reviewed the KnowBe4

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

training result data to determine whether employees completed the required annual cybersecurity awareness training. To do this, we obtained the following from CIDAO:

- a list of the 89 unique CIDAO employees who were employed during the audit period, including the 22 CIDAO employees who were hired during the audit period; and
- cybersecurity awareness training records covering the audit period.

We then compared our lists of employees' names to our lists of training records to determine whether there was an annual cybersecurity awareness training completion date recorded for each employee on our lists. Because there was no specific training program for newly hired employees during the audit period, we checked the names of all newly hired employees in the KnowBe4 training records to determine whether they completed a training within 30 days of their new hire orientation as required by the EOTSS Standard.

We determined the following through our review:

- In fiscal year 2023, 61 out of 75 employees did not complete annual cybersecurity awareness training.
- In fiscal year 2024, 65 out of 80 employees did not complete annual cybersecurity awareness training.
- During the audit period, 21 out of 22 newly hired employees did not complete cybersecurity awareness training within 30 days of their new hire orientation.

For this objective, we found certain issues during our testing. See Finding 3 for more information.

Employee Settlement Agreements

To determine whether CIDAO 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 interviewed CIDAO's first assistant district attorney and its director of Human Resources. They stated that CIDAO follows CTR's Settlements and Judgments Policy for any employee settlement agreements involving monetary payments.
- We inquired about internal policies and procedures regarding entering into, approving, and processing employee settlements. We were informed that CIDAO did not have any documented policies.

- We inquired about internal policies and procedures regarding the use of non-disclosure, non-disparagement, non-publication, and similarly restrictive language in employee settlement agreements. We were informed that CIDAO did not have any documented policies.

For the one separation agreement we discovered during our data reliability analysis, we determined whether the settlement was processed in accordance with CTR's Settlements and Judgments Policy by requesting, and reviewing where applicable, the following supporting documentation:

- the executed settlement agreement, signed by the appropriate parties;
- the SJ Authorization Form, complete with approval signatures and accurate payment amounts; and
- email correspondence from CTR approving CIDAO's claim payment.

For this objective, we found certain issues; namely, during our testing, CIDAO did not provide the SJ Authorization Form or the email correspondence from CTR containing the approval. We noted that CIDAO did not have a documented, transparent, or accountable process related to employee settlement agreements. This is evidenced by the settlement agreement that CIDAO failed to report to us when we requested a list. See Finding 2 for more information.

We did not identify any restrictive language in our review of the employee settlement agreement.

Data Reliability Assessment

Cybersecurity Awareness Training

We obtained cybersecurity awareness training completion data from the KnowBe4 system covering the audit period, consisting of 133 training records. To determine the reliability of the training data, we ensured that training dates were within the audit period, checked for blank fields, and checked for duplicate records within the data. We reviewed System and Organization Control 2 reports[3] 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.

3. A System and Organization Control 2 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.

Employee Lists

We obtained from CIDAO management a list of all 89 CIDAO employees who were employed during the audit period. To ensure the accuracy of the list, we verified employee names, identification numbers, and employment date information for a sample of 10 employees against CIDAO personnel files. To ensure the completeness of the list, we traced employee names, identification numbers, and employment date information from a sample of 10 personnel files to the employee list. As part of our review, we also checked the list for employment start and end dates outside the audit period, blank fields, and duplicate records within the list.

Employee Settlement Agreements

We requested a list of employee settlement agreements from a five-year period (July 1, 2019 through June 30, 2024). CIDAO told us that it had not entered into any employee settlement agreements since the new administration took office in January 2023 and was not aware of whether the office had entered into any employee settlement agreements under the prior administration.

To corroborate CIDAO's statements, we contacted CTR to determine whether any employee settlement agreements were reported for CIDAO in the CTR Settlement and Judgment Access Database during the extended audit period of July 1, 2019 through June 30, 2024. CTR confirmed that there were no records of employee settlements executed by CIDAO in the database. We examined the personnel folders for all CIDAO employees who separated from CIDAO in the five-year period for evidence of complaints, grievances, or settlement agreements and found none. We then ran a query from the Commonwealth Information Warehouse[4] of all legal expenses paid by CIDAO for the extended audit period. Using this data, we requested supporting invoices for all legal expenses that were over $3,000. We examined the invoices and identified time charges for work on an employee separation agreement. We requested a copy of the separation agreement from CIDAO. We contacted CTR and requested a determination of whether the language of the agreement constituted a settlement agreement that should have been reported to CTR prior to payment, as required by 815 CMR 5.09. CTR determined that the separation agreement should have been reported to CTR prior to payment.

4. 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.

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 Cape and Islands 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 Cape and Islands District Attorney's Office (CIDAO) did not promptly revoke former employees' access rights to the Track-Kit system. Specifically, of the 14 active user accounts for the Track-Kit system, 10 of these users were former employees. Additionally, CIDAO did not complete certain data fields (i.e., the assignment of CIDAO'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 CIDAO 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 CIDAO does not assign its contact information to SAECKs, then the Track-Kit System is not being used as intended under statute. Having CIDAO 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 [CIDAO 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."

Reasons for Issue

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

Recommendations

1. CIDAO 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 the system.
2. CIDAO 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

> *Section 18X(g) of Chapter 6A of the General Laws states that the District Attorney office "shall" participate in the state tracking system which is further defined by the Executive Office of Public Safety as developing policy to authorize access for new users of the system and to remove authorization from users who no longer require access. The Cape and Islands District Attorney's Office has no knowledge of whether such a policy existed under the previous administration. Once my administration took office, we worked to hire an additional member of the Information/Technology (IT) team as the department consisted of one individual previously. The second staff member was hired in January 2024, leaving 5 months of the audit period to have a fully staffed IT department and to start identifying and addressing Federal, State, and Local laws and regulations for our agency. After the audit period, the Cape and Islands District Attorney's Office has reached out to the Executive Office of Public Safety regarding the tracking program and has engaged in meetings to schedule appropriate training for our staff.*
>
> *Regarding the recommendation to assign [CIDAO contact information] to each SAECK within our jurisdiction in the Track-Kit system, as I am sure you are aware, SAECK kits are collected at the*

time of a forensic physical exam of a sexual assault victim. The District Attorney's Office is not made aware of the existence of a kit until criminal charges have been filed. There are many reasons why charges might not issue at the time the SAECK kit is collected. When this occurs, there is no mechanism for the District Attorney's Office to assign SAECK kit with no corresponding criminal case. As mentioned above, the Cape and Islands District Attorney's Office has already reached out to obtain training for our staff on the Track-Kit system, but that would be limited to kits that were connected to pending criminal cases.

I remain committed to working with my staff and yours to ensure we remain compliant.

Auditor's Reply

In its response, CIDAO focuses on developing a policy to authorize access for new users of the system and to remove authorization from users who no longer require access. Section 18X(g) of Chapter 6A of the General Laws requires district attorneys' offices to participate in the Track-Kit System "for the purpose of tracking the status of all sexual assault evidence kits."

As a first step, we applaud CIDAO for reaching out to EOPSS and, as part of these conversations, we encourage CIDAO to work with EOPSS to clearly define and standardize CIDAO's role in the Track-Kit system. We note for context that we have recently audited multiple district attorney offices and are currently auditing others. The issue of these offices' responsibilities under Section 18X(g) of Chapter 6A of the General Laws appears to be broadly misunderstood relative to the plain language reading of the law, making this additional definition and standardization valuable to multiple agencies of the Commonwealth.

Regarding the training of employees in the use of the Track-Kit system, CIDAO appears to be taking steps to address some of the issues raised in this finding. We will follow up on this matter in approximately six months, as part of our post-audit review process.

We understand that CIDAO cannot assign its contact information to a kit unless criminal charges have been filed. We urge CIDAO to assign its contact information to a survivor's kit as soon as possible once those criminal charges have been filed, in order to comply with the law.

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

We found that CIDAO should properly report all instances of monetary employee settlement agreements to the Office of the Comptroller of the Commonwealth (CTR). Specifically, CIDAO did not report a

monetary employee settlement agreement to the Office of the Comptroller of the Commonwealth (CTR) before making payment. This employee settlement agreement was not brought to our attention when we made the request for a list of employee settlement agreements and was discovered as part of our data reliability analysis. The employee settlement agreement was finalized on November 6, 2019, for the amount of $17,015.32. The agreement did not specify any allegations; did not include non-disclosure, non-disparagement, or similarly restrictive clauses; and was paid using CIDAO funds.

We also discovered two severance payments for $14,000 and $3,500 that CIDAO paid to two former employees and did not report to CTR. We identified these payments after reviewing emails between CTR and CIDAO in which CTR asked about the nature of these payments. CIDAO told CTR that one of the two payments was part of a severance agreement between CIDAO and the employee. However, CIDAO was unable to provide written documentation for either of the severance agreements. According to CTR, severance agreements should also be reported when they include payments outside of regular compensation (i.e., outside of wages or unused vacation time).

During the audit, CIDAO told us that it had an undocumented process to handle employee settlement agreements. 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. Additionally, if CIDAO does not maintain documentation regarding severance agreements, then it cannot determine whether the severance agreements included a release of future claims clause that would then require CIDAO to report the agreements to CTR.

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 [CTR] 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 CIDAO 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

CIDAO management told us that they were not aware of the requirement to report the employee settlement agreement to CTR before making payment, despite having communicated with CTR before making the payment. Additionally, CIDAO management told us that they were not aware they needed to report severance agreements to CTR.

Recommendations

1. CIDAO 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.

2. CIDAO should maintain all records related to all types of employee settlement and severance agreements, particularly those that include a written release of future claims against CIDAO, in accordance with Massachusetts public records laws and the Massachusetts Records Retention Schedule.

3. CIDAO should work with CTR to ensure that CIDAO understands the reporting requirements for all types of monetary employee settlement and severance agreements and ensure that CIDAO reports those agreements to CTR.

Auditee's Response

The Cape and Islands District Attorney's Office strongly disputes this finding. The audit finding includes that there was an employee settlement finalized on November 6, 2019. While I was not the District Attorney at that time and was not involved in that settlement, it remains outside of the identified audit period. The remainder of the audit findings addresses two severance payments made by this office prior to January 2023 when I became District Attorney. These severance payments were identified as "severance payments" and not settlements payments and are therefore outside of the audit scope of the documents requested by staff for purposes of the audit. As to these severance payments, I was not the District Attorney and was not involved in them, but regardless, they are outside of the scope of the audit.

The Cape and Islands District Attorney's Office does have a contract with an employment firm to assist with all employment law issues that arise in our day-to-day work. The ability to work with a law firm specializing in employment law allows us to ensure that should there be any issues with employees there is a well-documented and transparent process for all. This is true for any employee settlement agreement, should one ever be needed regardless of whether they contain non-disclosure, non-disparagement, or similarly restrictive clauses. Any settlements or employee actions are and will be well documented and transparent.

Auditor's Reply

CIDAO suggests the employee settlement agreement identified during the course of the audit was outside of the audit period. As stated in the "Executive Summary" and the "Audit Objectives, Scope, and Methodology," the audit period for this specific objective was July 1, 2019 through June 30, 2024. A settlement agreement executed in November 2019 would fall within the audit period.

Severance agreements can also serve as settlement agreements in instances where the employer offers severance pay as an incentive for an employee to sign a severance agreement, waiving any potential legal claims. As stated in the finding, CIDAO's email referenced a mutual agreement between itself and the employee.

When we inquired with CTR about this agreement, it was explained that if severance payments were made outside of the normal course of business and there was an agreement that included a release of future claims, CIDAO would need to report the agreement to CTR. CIDAO could not produce any documentation for the mutual agreement, including the terms of the subsequent severance payments. As a result, we brought the matter to CIDAO's attention to ensure compliance with CTR's "Settlement and Judgment Policy." These severance payments are well within the scope of the audit. CIDAO mentions a well-documented and transparent process for dealing with employee issues that would also be true for employee settlement agreements, but a policy specific to the use of settlement agreements, including any requests for non-disclosure, non-disparagement, or similarly restrictive clauses, was not provided to our office.

We agree that these settlement agreements were executed before the swearing in of the current District Attorney. Our audit is of the governmental institution of CIDAO, and not the District Attorney. Government institutions should follow proper processes and procedures, retain appropriate documentation, and perform other functions regardless of who serves as their elected leader. The fact that CIDAO did not do this during the audit period (July 1, 2019 through June 30, 2024) does not reflect the actions of the current district attorney, but we raise these issues so agency leadership and management know about and can address these issues going forward. We recommend that CIDAO implement our recommendations, and we will follow up on them in approximately six months as part of our post audit review process.

3. The Cape and Islands District Attorney's Office should ensure that all employees complete cybersecurity awareness training when hired and annually thereafter.

CIDAO should have provided annual cybersecurity awareness training to all its employees during the audit period. Additionally, the agency did not have sufficient policies to require that this training be administered to its active employees.

We found that 61 out of 75 CIDAO employees did not complete the required annual training for fiscal year 2023, and 65 out of 80 CIDAO employees did not complete the required annual training for fiscal year 2024.

We also found that 21 out of 22 CIDAO employees who were hired during the audit period did not complete training within the required 30 days of new hire orientation.

Without educating its employees on their responsibility to protect the security of information assets, CIDAO exposes itself to a higher 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 CIDAO is not required to follow these standards because it is not an executive branch agency, we consider them best practices.

Reasons for Issue

CIDAO management told us in an interview that CIDAO was not aware of the EOTSS training standards. Additionally, CIDAO management stated that the current administration had no knowledge of the prior administration's policies regarding cybersecurity awareness training because the outgoing administration denied the incoming administration's request to hold transition meetings.

Recommendations

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

2. CIDAO should design and implement policies and procedures to ensure that its employees complete cybersecurity awareness training. Additionally, CIDAO should retain copies of cybersecurity awareness training certificates as evidence that its employees completed the training.

Auditee's Response

Several months after taking office, the Cape and Islands District Attorney's Office leadership team became aware that there was no compliance with cybersecurity under the previous administration. Aware of our obligation and the importance of cybersecurity, the Cape and Islands District Attorney's Office first worked to staff the [information technology] department, as identified above, and then began the process of identifying the requirements and implementation of Cybersecurity training for our staff, which have since been completed.

Auditor's Reply

CIDAO appears to be taking steps to address the issues raised in this finding. 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 Cape and Islands District Attorney's Office (CIDAO), 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 kits. Specifically, 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."

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 [CIDAO 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. Additionally, EOPSS offered trainings in the use of the Track-Kit system to various district attorney offices in 2019, outside the audit period, but we found that only one active user from CIDAO 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 attorney offices. CIDAO management told us during interviews that the agency rarely used the Track-Kit system and provided user activity logs during the audit period that supported their statements. 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.

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