OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued April 13, 2023

Department of Criminal Justice Information Services

For the period July 1, 2020 through June 30, 2021

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

April 13, 2023

Jamison Gagnon, Commissioner
Department of Criminal Justice Information Services
200 Arlington Street, Suite 2200
Chelsea, MA 02150

Dear Commissioner Gagnon:

I am pleased to provide to you the results of the enclosed performance audit of the Department of Criminal Justice Information Services. As is typically the case, this report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2020 through June 30, 2021. As you know, my audit team discussed the contents of this report with agency managers. This report reflects those comments.

I appreciate you and all your efforts at the Department of Criminal Justice Information Services. The cooperation and assistance provided to my staff during the audit went a long way toward a smooth process. Thank you for encouraging and making available your team. I am available to discuss this audit if you or your team have any questions.

Sincerely,

Diana DiZoglio
Auditor of the Commonwealth

cc: Terrence Reidy, Secretary of the Executive Office of the Public Safety and Security
Michaela Dunne, Deputy Commissioner of the Department of Criminal Justice Information Services
Agapi Stratakias, General Counsel of the Department of Criminal Justice Information Services

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CJIS	Criminal Justice Information System
CMR	Code of Massachusetts Regulations
CORI	Criminal Offender Record Information
CSSOA	Criminal Justice Information System Single Sign on Application
DCJIS	Department of Criminal Justice Information Services
FBI	Federal Bureau of Investigation
MMARS	Massachusetts Management Accounting and Reporting System
PCS	Project and Constituent Services

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 the Department of Criminal Justice Information Services (DCJIS) for the period July 1, 2020 through June 30, 2021. The purpose of our audit was to determine whether DCJIS does the following:

- maintains its Criminal Offender Record Information (CORI) database, iCORI,[1] in accordance with Section 167A(f) of Chapter 6 of the General Laws
- performs audits of non–law enforcement CORI requestors to confirm that each requestor has security protection over the information obtained through the iCORI database in accordance with Section 2.21(4)(d) of Title 803 of the Code of Massachusetts Regulations, which was effective during the audit period
- ensures that all authorized law enforcement personnel who have access to criminal justice information complete cybersecurity awareness training in accordance with Sections 5.2.1 through 5.2.3 of the United States Department of Justice Federal Bureau of Investigation's "Criminal Justice Information Services (CJIS) Security Policy," dated June 1, 2020
- reconciles funds received for CORI requests to the Massachusetts Management Accounting and Reporting System (MMARS) in accordance with the Office of the Comptroller of the Commonwealth's "Cash Recognition and Reconciliation Policy," dated July 1, 2004.

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

Finding 1 **Page 12**	DCJIS does not perform audits of non–law enforcement CORI requestors to ensure that this information is properly stored and safeguarded.
Recommendations **Page 12**	1. DCJIS should require its audit team to perform audits to assess whether non–law enforcement requestors properly store and safeguard the CORI they obtain from DCJIS. 2. DCJIS should develop and implement policies and procedures that require its audit team to perform audits to assess whether non–law enforcement requestors have properly stored and safeguarded CORI.

1. This database contains Massachusetts-only criminal activity and personally identifiable information such as names, birthdates, addresses, and social security numbers.

Finding 2 **Page 15**	DCJIS did not ensure that Criminal Justice Information System Single Sign On Application (CSSOA) users completed cybersecurity awareness training.
Recommendations **Page 16**	1. DCJIS should ensure that CSSOA users complete initial cybersecurity awareness training within six months of their initial access to CSSOA and biennially thereafter. 2. DCJIS should continually monitor that both new and existing CSSOA users have completed the required cybersecurity awareness training.
Finding 3 **Page 18**	DCJIS does not reconcile all revenue recorded in the iCORI database.
Recommendations **Page 18**	1. DCJIS should investigate and resolve the $22,343 variance. 2. DCJIS should develop policies and procedures that require its employees to perform regular reconciliations of the revenue recorded in its iCORI database to revenue recorded in MMARS.

OVERVIEW OF AUDITED ENTITY

The Criminal History Systems Board was created in 1972 by Sections 167 through 178 of Chapter 6 of the Massachusetts General Laws. Chapter 256 of the Acts of 2010 (referred to as the Criminal Offender Record Information [CORI] Reform) renamed it as the Department of Criminal Justice Information Services (DCJIS). DCJIS was established within the state's Executive Office of Public Safety and Security, pursuant to Section 167A of Chapter 6 of the General Laws, on November 4, 2010. This new legislation also allowed the general public to gain access, through the internet, to CORI. Since 2012, the public has been able to request CORI on DCJIS's website through the iCORI database.

According to the Commonwealth Budget's website,

> *The mission of the Department of Criminal Justice Information Services (DCJIS) is to . . . [provide] timely and accurate criminal justice information and services to authorized law enforcement and non-criminal justice agencies and individuals in support of promoting the public safety and security of the Commonwealth of Massachusetts.*

DCJIS is overseen by a commissioner, who is appointed by the Secretary of the Executive Office of Public Safety and Security. DCJIS manages and administers the Commonwealth's iCORI database, Firearms Records Bureau database, Statewide Applicant Fingerprint Identification Services, and Post-conviction Victim Notification Program. According to its website, DCJIS serves the following groups:

- *Law enforcement personnel*
- *Victims of crimes*
- *Governmental entities*
- *Private organizations*
- *Employers*
- *Firearms dealers*
- *Firearms license holders*
- *The general public*

Additionally, there is a criminal record review board within DCJIS. Section 168 of Chapter 6 of the General Laws states,

> *[This criminal review board consists] of the following persons: the secretary of public safety and security, who shall serve as chair, the attorney general, the secretary of labor and workforce development, the chair of the Massachusetts sentencing commission, the chief counsel for the committee for public counsel services, the chair of the parole board, the commissioner of correction, the commissioner of probation, the commissioner of youth services, the colonel of state police and the presidents of the Massachusetts District Attorneys Association, the Massachusetts Sheriffs' Association and the Massachusetts Chiefs of Police Association, or their designees, all of whom shall serve ex officio, and 5 persons to be appointed by the governor, 1 of whom shall represent private users of criminal offender record information, 1 of whom shall be a victim of crime, 1 of whom shall have experience in the areas of workforce development or ex-offender rehabilitation or economic development and 2 of whom shall be persons who have experience in issues relating to personal privacy. Upon the expiration of the term of any appointive member, [the member's] successor shall be appointed in a like manner for a term of 3 years.*

This board reviews and investigates complaints alleging violations of CORI laws or regulations.

The DCJIS commissioner directs strategic planning for DCJIS and sets operational priorities for the 40 employees in its office at 200 Arlington Street in Chelsea. DCJIS had a budget of $6,824,479 for fiscal year 2021, and it collected $10,173,495 from CORI requests during the same period.

DCJIS is organized into the following units: Legal Services, Law Enforcement and Civil Information Services, Fiscal Services, and Human Resources. Within the Law Enforcement and Civil Information Services Unit, there are the following groups with varying responsibilities:

- The Firearms Records Bureau maintains a database of registered firearms, gun dealers, machine gun licenses, and issued firearm identification cards in Massachusetts.
- The Victim Services Unit provides assistance to victims of crimes through resources, referrals, crisis intervention, and safety planning and notifies victims in advance when the offenders who committed the crimes are going to be released from prison.
- The Statewide Applicant Fingerprint Identification Services Unit processes fingerprint-based criminal record checks for non–criminal justice agencies.
- The Project and Constituent Services (PCS) Unit provides CORI to DCJIS-approved, non–criminal justice agencies, such as schools, daycare centers, home healthcare organizations, youth athletic organizations, and municipal government agencies. Individuals can also obtain copies of their own criminal records from the PCS Unit. The PCS Unit processes an average of 85,000 requests per month. The PCS Unit does the following:

  - assists with correcting inaccurate criminal records; investigates complaints of improper access to or dissemination of CORI; and provides legal assistance on matters regarding CORI law to police, prosecutors, judges, and the public

  - helps ensure that DCJIS-approved, non–criminal justice agencies with access to the iCORI database understand the purposes for which they are authorized to access CORI

  - assists individuals and agencies with the reading and interpretation of CORI reports; how CORI affects potential employment; the responsibilities of employers regarding access, review, storage, and dissemination of CORI; the relevance of a criminal record to the duties and qualifications of job positions; and how to interpret and use the CORI they receive in a fair and objective manner.

- The Criminal Justice Information System (CJIS) Support Services Unit offers—to law enforcement and criminal justice agencies in the state—access 24-hours a day, seven days a week to the National Crime Information Center and the International Public Safety and Justice Network, which store state and interstate criminal history record information, missing and wanted person files, driver's license and motor vehicle information, and other critical criminal justice information.

CORI Request Process

DCJIS provides and maintains an electronic application on its website that members of the public and organizations can use to request criminal background checks on individuals. Individuals or organizations that do not have online access may request CORI through the mail. DCJIS employees enter any mailed requests into the iCORI database.

An organization needs to first submit an application, and if approved by DCJIS, they can request CORI based on the specific requestor type. An individual can submit a request for their own information, or an organization can submit a request about an individual for various reasons such as employment, volunteering, or housing. There is a $25 fee to process a request.

If a request yields results, the requestor receives details of the requested individual's Massachusetts criminal history. If a request does not yield results, the requestor receives a notification that no criminal history was found. In requests where there are results for the same or similar names (e.g., multiple John Does and Jon Doe), the system adds the request into a candidate screener queue for a DCJIS employee to review manually to ensure that the CORI report contains information on the correct individual.

DCJIS has two full-time employees dedicated to processing mailed requests. Additionally, DCJIS has other employees in call centers who are trained to handle mailed requests during busy periods. On average,

there are approximately 70 mailed requests a day. All requests for CORI, submitted by mail or electronically, must be processed and returned to the requestor within 10 days.

During the audit period, there were 1,019,597 CORI requests from 9,814 organizations and 36,481 individuals. These 9,814 organizations comprise 62 requestor categories. Some of these categories were public and private schools, businesses, Massachusetts state agencies, hospitals, children's programs and volunteer organizations, religious organizations, Massachusetts housing authorities, and Massachusetts municipal governments.

In cases where an employee of a media organization makes a CORI request about an individual, the organization requesting the information must pay a $50 fee. The CORI contains convictions that fall within the below offense types and timeframes as listed in DCJIS's "What You Need to Know about Massachusetts Criminal Records" document:

1. *misdemeanor convictions for one year following the date of disposition or date of release from incarceration or custody, whichever is later;*
2. *felony convictions . . . for two years following the date of disposition or date of release from incarceration or custody, whichever is later;*
3. *felony convictions . . . punishable by five or more years in state prison provided, however, that such offense shall only be available for ten years following the date of disposition or date of release from incarceration or custody, whichever is later;*
4. *and all convictions for murder, voluntary manslaughter, involuntary manslaughter, and sex offenses (as defined in M.G.L. c. 6, § 178C) punishable by a term of incarceration in state prison, unless sealed, including information relating to those offenses for which the subject was adjudicated as an adult while younger than 18 years old; and*
5. *any cases where the individual has been found not guilty by reason of insanity*

DCJIS employees review the CORI request and perform an additional review to ensure the accuracy of the CORI before releasing the information to the requestor. During the review, these employees perform an internet search about the subject of the CORI. If this search reveals recent media coverage regarding the individual, the request is forwarded to DCJIS's general counsel for further review before the CORI report is released to the requesting individual or organization.

iCORI Revenue Reconciliation Process

If a request is submitted by mail, a DCJIS employee separates the payment from the request. This employee records the payment information (date, money order number, amount, and type of CORI requestor) in a Microsoft Excel spreadsheet. A different DCJIS employee reviews the payment information to ensure accuracy and adds their initials to the spreadsheet. At the end of each day that mailed requests are received, DCJIS's budget director deposits all payments into the bank. The requests are also entered into the iCORI database to capture each requestor's personal information, the date the request was received, and the payment amount.

CORI requests submitted online start in the iCORI database. Payments are processed using a third-party payment system, nCourt, which processes the payment and deposits the funds into DCJIS's bank. At the end of each month, DCJIS employees transfer the payment information to the Massachusetts Management Accounting and Reporting System (MMARS). Each day, nCourt sends a reconciliation report that includes daily funds collected and the requestors' names to DCJIS. DCJIS records the daily nCourt totals and request dates into the same Microsoft Excel spreadsheet used for CORI requests received by mail.

At the end of each month, DCJIS reconciles the nCourt reconciliation reports and the Micrsoft Excel spreadsheet to its bank statement and MMARS.

Security Protection over CORI

Any person or organization that requests CORI from DCJIS is subject to audit by DCJIS to ensure, in part, that the requestor properly stores and safeguards CORI in accordance with Section 2.21(4)(d) of Title 803 of the Code of Massachusetts Regulations, which was effective during the audit period.

DCJIS has established an audit team within the CJIS Support Services Unit that performs audits on approximately 650 agencies—including federal agencies, Massachusetts law enforcement government agencies (e.g., state police, correctional institutions, and the Department of Children and Families), and local police departments across the Commonwealth—that have access to the CJIS Single Sign on Application (CSSOA) criminal record history database. These audits include a review of data quality information, cybersecurity awareness training completion records, and access to areas where CORI and the United States Department of Justice Federal Bureau of Investigation (FBI) data are located and a determination about whether criminal information is stored properly.

DCJIS has developed a policy on physical security that each individual or organization that has received CORI from DCJIS must follow, which includes securing applications and CORI reports in locked filing cabinets or in encrypted computer files and only allowing access to authorized users.

Cybersecurity Awareness Training

DCJIS developed, and maintains and monitors, CSSOA. The database contains Massachusetts criminal and motor vehicle history and national criminal and motor vehicle history from the FBI. DCJIS has made this application and data available to approximately 650 federal and state agencies and police departments, including municipal, state, and university police departments.

The FBI has established that all CSSOA users with access to federal criminal justice information must complete cybersecurity awareness training within six months of initial access and biennially thereafter. DCJIS audits all agencies that have access to CSSOA at least once every three years. DCJIS stated in a meeting to us that part of the audit includes a review of law enforcement agencies' cybersecurity awareness training completion certificates to ensure that all users have completed the mandatory awareness training (see Finding 2).

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 Department of Criminal Justice Information Services (DCJIS) for the period July 1, 2020 through June 30, 2021.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Below is a list of our audit objectives, indicating each question we intended our audit to answer; the conclusion we reached regarding each objective; and, if applicable, where each objective is discussed in the audit findings.

Objective	Conclusion
1. Does DCJIS maintain its Criminal Offender Record Information (CORI) database, iCORI, in accordance with Section 167A(f) of Chapter 6 of the General Laws and DCJIS's request turnaround policy, as published on its website?	**Yes**
2. Does DCJIS perform audits of CORI requestors to confirm that non–law enforcement CORI requestors have security protection over the information obtained through the iCORI database in accordance with Section 2.21(4)(d) of Title 803 of the Code of Massachusetts Regulations, which was effective during the audit period?	**No; see Finding 1**
3. Does DCJIS ensure that all Criminal Justice Information System Single Sign On Application (CSSOA) users who have access to criminal justice information complete cybersecurity awareness training in accordance with Section 5.2.1 through 5.2.3 of the United States Department of Justice Federal Bureau of Investigation's "Criminal Justice Information Services (CJIS) Security Policy," dated June 1, 2020?	**No; see Finding 2**
4. Does DCJIS reconcile funds received for CORI requests to the Massachusetts Management Accounting and Reporting System (MMARS) in accordance with the Office of the Comptroller of the Commonwealth's "Cash Recognition and Reconciliation Policy," dated July 1, 2004?	**No; see Finding 3**

To achieve our audit objectives, we gained an understanding of DCJIS's internal control environment related to the objectives by reviewing applicable agency policies and procedures, as well as conducting inquiries with DCJIS's employees and management. We evaluated the design of controls over CORI

request backlogs, CORI requestor audits, cybersecurity awareness training for law enforcement personnel with access to CSSOA, and reconciliation of CORI revenue data.

CORI Request Backlogs

We extracted all 1,019,597 CORI requests from individuals and organizations during the audit period from the iCORI database. We analyzed 100% of the CORI requests by comparing the CORI request date to the date the CORI request was completed and provided to the requestor to determine whether CORI requests were completed within the 10 business days required. We identified 37 instances where a request took longer than 10 business days to complete.

We examined all 37 requests that exceeded the 10-business day requirement to determine whether the delays were substantiated.

Audits

We requested the list of audits DCJIS performed on CORI requestors (non–law enforcement agencies) from DCJIS management. We analyzed the types of agencies / organizations that requested CORI through the iCORI database to determine the number of CORI requests by agency / organization type.

Cybersecurity Awareness Training for CSSOA Users

We selected a random, statistical sample of 131 law enforcement personnel from a population of 22,855 who use CSSOA—with a 90% confidence level, 15% tolerable error rate, and a 50% expected error rate—to determine whether those individuals completed cybersecurity awareness training within six months of first accessing the data and biennially thereafter. We examined copies of training completion certificates to determine whether selected users completed the cybersecurity awareness training within the established timeframes.

iCORI Revenue Reconciliation

We compared DCJIS reconciliations of revenue collected for CORI requests from DCJIS's bank statements to MMARS revenue reports. We performed a reconciliation of revenue recorded in the iCORI database to MMARS to ensure that collected revenue was properly accounted for in accordance with the Office of the Comptroller of the Commonwealth's "Cash Recognition and Reconciliation Policy."

Data Reliability Assessment

iCORI Database

To determine the reliability of the data in the iCORI database, we tested selected information system controls (access controls, security management, configuration management, contingency planning, and segregation of duties). We conducted electronic tests, including checking for sequential gaps and duplicates, on request identification numbers. We also determined whether all data fell within the audit period.

For those law enforcement agencies accessing CSSOA, we reconciled the number of law enforcement agencies to the law enforcement agency list used by the DCJIS audit team.

MMARS

In 2018 and 2022, the Office of the State Auditor performed data reliability assessments of MMARS that focused on testing selected system controls (access controls, configuration management, contingency planning, and segregation of duties). As part of our current audit, we asked DCJIS management for the agency's cybersecurity awareness policy and personnel screening policy and procedures. We tested one of the two employee files of the DCJIS employees who had access to MMARS during the audit period to determine whether DCJIS had completed the employee's background check and whether the employee had completed cybersecurity awareness training.

Based on the results of our data reliability assessments, we determined that the information obtained for our audit period was sufficiently reliable for the purpose of our audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Department of Criminal Justice Information Services does not perform audits of non–law enforcement Criminal Offender Record Information requestors to ensure that this information is properly stored and safeguarded.

The Department of Criminal Justice Information Services (DCJIS) does not perform audits of non–law enforcement Criminal Offender Record Information (CORI) requestors to ensure that this information is properly stored and safeguarded.

If DCJIS does not audit these CORI requestors, there is a higher-than-acceptable risk that an individual's personally identifiable information may be used for such things as identity theft or fraud.

Authoritative Guidance

Section 2.21 of Title 803 of the Code of Massachusetts Regulations (CMR), which was effective during the audit period, states,

> *(1) Requests for CORI are subject to audit by the DCJIS. . . .*
>
> *(4) During an audit, DCJIS audit staff shall assess the requestor's compliance with statutory and regulatory requirements, including, but not limited to: . . .*
>
> *(d) if the requestor is properly storing and safeguarding CORI;*

Reasons for Issue

DCJIS does not have policies and procedures that require its audit team to perform audits to assess whether non–law enforcement requestors have properly stored and safeguarded CORI.

Recommendations

1. DCJIS should require its audit team to perform audits to assess whether non–law enforcement requestors properly store and safeguard the CORI they obtain from DCJIS.
2. DCJIS should develop and implement policies and procedures that require its audit team to perform audits to assess whether non–law enforcement requestors have properly stored and safeguarded CORI.

Auditee's Response

The Office of the State Auditor's ("SAO") first audit finding notes that DCJIS does not perform audits of non-law enforcement CORI requestors to ensure that this information is properly stored and safeguarded. The finding also recommends that DCJIS redirect its small staff of six assigned to audit the approximately 650 criminal justice agencies, to perform non-criminal justice audits. Respectfully, DCJIS believes that its current approach to ensuring compliance is more effective and does not find the recommendations provided by the SAO to be feasible given the current DCJIS staff and resources.

DCJIS is a small state agency with [a fiscal year] 2023 budget of $5.9M and fewer than forty employees, and yet it performs many important functions, and in doing so, it generates approximately $16 million in annual revenue for the Commonwealth of Massachusetts.

In accordance with the SAO's engagement letter, dated July 29, 2021, the audit time period for the audit spanned from July 1, 2020, to June 30, 2021 (the "Audit Period"). It is worth noting that the Audit Period selected by the SAO falls entirely within the period of the [2019 coronavirus pandemic] and the resulting state of emergency declared by Governor Baker from March 10, 2020, to June 15, 2021. . . .

DCJIS's performance during the pandemic demonstrates its effectiveness in serving the people of the Commonwealth. The ongoing health crisis required DCJIS to adapt immediately to drastic changes in work life. These changes affected not only DCJIS's own employees but also the requestors and subjects of CORI. To ensure the provision of CORI to those employers and others entitled by law to receive it, DCJIS implemented emergency regulations and then permanent regulations which permitted remote verification of identity under certain circumstances. Throughout the pandemic, DCJIS seamlessly continued to process CORI requests which assisted the onboarding of new employees and the provision of housing across the Commonwealth.

The SAO's audit findings demonstrate the success of these efforts. As the SAO's audit revealed, DCJIS processed 1,019,600 iCORI requests during the Audit Period. All but nine requests—about 0.0000088% of the total—were processed within ten business days, the timeframe described on DCJIS's website. All but five requests were processed within eleven business days. Each of these five requests required additional research or was otherwise subject to manual review.

The SAO finds that DCJIS should perform random audits of organizations using iCORI. In particular, the SAO wants DCJIS to perform random checks of how CORI reports are stored and safeguarded by non-criminal justice iCORI users. DCJIS appreciates the SAO's recommendation but respectfully disagrees that random audits of iCORI users are the most effective way to police the system. It is simply not feasible for DCJIS to conduct random audits of the 181,179 individual iCORI accounts and 32,091 organization accounts that are registered for DCJIS' iCORI service. Rather, DCJIS believes its multi-tiered approach to promoting the security of CORI is both more effective and comports with the intent of the legislature when it passed the CORI Reform Law in 2010.

As an initial matter, it is unclear what standard the SAO is auditing to when it makes this recommendation. The CORI laws and regulations do not require DCJIS to perform random audits of iCORI users. On the contrary, [Section 172 of Chapter 6 of the Massachusetts General Laws]

and 803 CMR 2.23 both state that CORI requests are "subject to audit" by DCJIS, language which conveys that such audits are discretionary.

Moreover, the sheer number of organizations using iCORI makes random audits impractical and inefficient. There are 181,179 individual accounts and 32,091 organizational accounts in the iCORI system. This broad access to CORI was part and parcel of the legislature's CORI Reform Law. As just one example, in [Section 172(a)(3) of Chapter 6 of the General Laws], the legislature made CORI available to any employer.

As a result of this broad access, it is more efficient for DCJIS in policing the iCORI system to focus on areas where there are real questions of inappropriate use. And that is what DCJIS does.

This approach is consistent with the legislative intent of the CORI Reform Law. In passing CORI Reform, the legislature provided a mechanism for policing the system: self-audits. [Section 172(g) of Chapter 6 of the General Laws]. With these self-audits, an individual can see anyone outside of law enforcement who is checking his or her CORI. DCJIS provides these self-audits to any individual who requests them, as described in 803 CMR 2.25. And where a self-audit shows someone that his or her CORI has been accessed inappropriately, the person can file a complaint. 803 CMR 2.27. DCJIS investigates complaints regarding any violation of the CORI laws and regulations, and it also investigates complaints about inaccurate CORI. 803 CMR 2.26, 2.27. Where the investigations reveal a violation of the CORI laws and regulations, then DCJIS prosecutes the matter before the Criminal Record Review Board, which is empowered to impose civil penalties. [Section 168 of Chapter 6 of the General Laws]; 803 CMR 2.28.

DCJIS also uses technological tools to police the system. Rules within the iCORI system flag potential violations of the CORI laws and regulations and the iCORI Terms of Service. In particular, the system can detect login and password sharing and upon detection, the iCORI account at issue is automatically disabled.

Even with all these protections in place, DCJIS does not rest upon its efforts to police violations but proactively trains large numbers of iCORI users. In calendar year 2022 alone, DCJIS trained 1,544 individuals in the proper use of the iCORI system and in applying the laws and regulations governing CORI access. . . . Since 2019, DCJIS has trained 2,753 individuals. In addition to formal training, DCJIS responds to calls every day from members of the public about proper use of the iCORI system.

DCJIS chooses to police its system with this combination of proactive formal and informal training, technological tools, and the policing mechanisms determined by the legislature. DCJIS's approach flows from and is consistent with the intentions of the legislature manifested in the language of the CORI laws. Moreover, as a practical matter, it would be inefficient to divert time and resources from efforts to educate and from efforts to investigate known problems. It is entirely unclear what additional benefit would be conferred by diverting these resources toward randomly auditing what would necessarily be an insignificant fraction of the over 200,000 existing iCORI accounts.

Therefore, while DCJIS appreciates the SAO's efforts and is grateful for the SAO's audit, it respectfully finds that SAO's finding is simply not feasible based on staff and resources available to DCJIS as this time.

Auditor's Reply

The Office of the State Auditor acknowledges that the use of auditing as stated in 803 CMR 2.23 is discretionary; however, in our review, we found that this control measure had not been used one single time, and we were informed that it has been rarely used, if at all, because of the noted staffing constraints. We recognize and agree that staff members and their time is a concern to ensure accountability; however, we believe that there exists a need to select random non–law enforcement CORI requestors, based on risk level determined by DCJIS, to ensure that information is securely stored. To accomplish this, we encourage DCJIS to consider seeking adequate funding through the Legislature and administration to allow for the appropriate qualified staff levels so as to perform these tasks. By doing so, DCJIS would reduce the possibility that personally identifiable information would be accessed or compromised by individuals who are not authorized to access it.

2. DCJIS did not ensure that Criminal Justice Information System Single Sign On Application users completed cybersecurity awareness training.

DCJIS did not ensure that Criminal Justice Information System Single Sign On Application (CSSOA) users completed cybersecurity awareness training. We found 39 of the 131 law enforcement employees in our sample who worked at law enforcement agencies during the audit period did not complete biennial training on time. Our test revealed that 21 law enforcement employees completed their training late, with missed due dates ranging from 11 days to 9 years. As of June 30, 2021, the remaining 18 employees had not completed biennial training, with missed due dates ranging from 122 days to 9 years. Based on our testing, no less than 5,310 (23.233%) employees did not complete cybersecurity awareness training.

Not completing cybersecurity awareness training may lead to user error and compromise the integrity and security of CSSOA, which DCJIS manages.

Authoritative Guidance

Section 5.2.1 of the United States Department of Justice Federal Bureau of Investigation's (FBI's) "Criminal Justice Information Services (CJIS) Security Policy," issued on June 1, 2020, states, "Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to . . . a physically secure location," which applies to CSSOA users.

Reasons for Issue

DCJIS management told us that they review training completion certificates as part of the audit process every three years, but DCJIS does not continually monitor whether CSSOA users complete cybersecurity awareness training within six months of their initial access to CSSOA and biennially thereafter.

Recommendations

1. DCJIS should ensure that CSSOA users complete initial cybersecurity awareness training within six months of their initial access to CSSOA and biennially thereafter.
2. DCJIS should continually monitor that both new and existing CSSOA users have completed the required cybersecurity awareness training.

Auditee's Response

The SAO finds that DCJIS needs to take steps to ensure that users of the Criminal Justice Information Systems ("CJIS") are in compliance with the security awareness training requirements in Section 5.2 of the FBI CJIS Security Policy by completing training within six months of being hired and then biennially thereafter.

Again, it is unclear what standard DCJIS is being audited to. State regulations at 803 CMR 7.07 place this burden not upon DCJIS but upon the law enforcement agencies and individual users of the CJIS system. The Massachusetts CJIS User Agreement does the same at Section 3.2.

Nevertheless, in reference to the first audit recommendation, DCJIS notes that completion of CJIS Security Awareness Training is a pre-requisite to gaining access to CJIS. Therefore, CJIS user accounts are not activated by DCJIS until such time as a user completes training. As such, DCJIS, although not required to do so, ensures that all CJIS users complete initial training prior to being granted access privileges to CJIS. DCJIS staff also provides regular training of CJIS users. In calendar year 2022, DCJIS held 17 training sessions and trained approximately 171 users.

In regard to the second audit recommendation, DCJIS audits law enforcement agencies' compliance with the security awareness training requirements of the FBI CJIS Security Policy. This analysis is performed during DCJIS's triennial audit of each Massachusetts law enforcement agency with access to CJIS. These audits are the most efficient way for DCJIS to monitor compliance with the security awareness training requirements. As personnel from DCJIS's CJIS Support Unit explained in interviews with SAO auditors on December 2 and December 16, 2021, there are simply too many CJIS users for DCJIS to actively monitor each individual user's training status in real time. Moreover, whether and when an officer is required to retake the training will depend on personnel information in the possession of the police department. For example, a police officer's certificate of compliance may expire, but if the officer is on leave from his job and does not have access to CJIS, then he does not need to retake the test. The information necessary to determine when a user needs to take the training rests with the individual user's agency and not with DCJIS. Consequently, it is most effective for DCJIS to determine compliance during audits of the agencies.

Therefore, while DCJIS appreciates the SAO's efforts and is grateful for the SAO's audit, it respectfully disagrees with the SAO's finding on this point. Nevertheless, on August 29, 2022, DCJIS took the additional step of sending out a notification to all Massachusetts chiefs of police and law enforcement agency heads. The notification was sent electronically in the form of a letter which was also posted on DCJIS's extranet. The letter reminds all recipients in detail about the security awareness training requirements imposed upon them by 803 CMR 7.07 and by the Massachusetts CJIS User Agreement. The letter further reminds all recipients that DCJIS will continue to audit their agencies to these requirements.

Auditor's Reply

We commend DCJIS on taking the step of issuing a letter on its extranet to Massachusetts police chiefs and law enforcement agencies regarding cybersecurity awareness training and encourage DCJIS to develop a system that continually monitors whether CSSOA users complete cybersecurity training in a timely manner. However, we disagree with DCJIS on who is ultimately responsible for ensuring that all CSSOA users complete the mandatory biennial cybersecurity awareness training.

As noted in both Section 5.2.1 of the FBI's "Criminal Justice Information Services (CJIS) Security Policy" and 803 CMR 7.07(1), DCJIS is responsible for the administration and management of CSSOA. Section 5.2.1 of the FBI's "Criminal Justice Information Services (CJIS) Security Policy" states,

[DCJIS] may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

According to 803 CMR 7.07, DCJIS "shall be responsible for overseeing access to all FBI systems and information by Massachusetts agencies, as well as for ensuring system security, training, policy compliance, and auditing."

Based on these requirements, DCJIS should not just trust that law enforcement agencies are ensuring their CSSOA users are being trained. Instead, DCJIS should verify on its own that the agencies' CSSOA users are being trained and follow up on any users with extended gaps in their training that DCJIS identifies in its audits. Because of the sensitive nature and types of information (such as personally identifiable information) in CSSOA, there is a heightened risk of unauthorized access to this information if users do not regularly receive cybersecurity awareness training.

3. DCJIS does not reconcile all revenue recorded in the iCORI database.

Although we found that DCJIS reconciles revenue information received from nCourt and its own spreadsheet containing records of payments from mailed CORI requests to its bank statements, DCJIS does not reconcile the revenue information in its iCORI database to the Massachusetts Management Accounting and Reporting System (MMARS). When we compared all CORI revenue recorded in DCJIS's iCORI database to what was recorded in MMARS, we found that the revenue in the iCORI database was $22,343 more than the revenue recorded in MMARS.

Because DCJIS does not perform reconciliations of all of the revenue recorded in its iCORI database, there is a higher-than-acceptable risk of variances occurring and going undetected.

Authoritative Guidance

The Office of the Comptroller of the Commonwealth's "Cash Recognition and Reconciliation Policy," issued July 1, 2004, requires that all state departments reconcile all received revenue in their internal accounting records to revenue reported in MMARS. It also states,

> *Daily system assurance must be performed by departments to ensure that there is a matching deposit for each cash transaction. This process involves comparing the results from all sources that produce or contain payments and deposit information, and ensuring that they match. These information sources should include . . . all relevant MMARS tables.*

Reasons for Issue

DCJIS does not have policies and procedures that require its employees to perform regular reconciliations of the revenue recorded in its iCORI database to revenue recorded in MMARS.

Recommendations

1. DCJIS should investigate and resolve the $22,343 variance.
2. DCJIS should develop policies and procedures that require its employees to perform regular reconciliations of the revenue recorded in its iCORI database to revenue recorded in MMARS.

Auditee's Response

> *The SAO finds that DCJIS does not perform a reconciliation of its CORI revenue. DCJIS strongly disagrees with this finding because it is factually inaccurate. DCJIS regularly reconciles revenue collected in accordance with policies and procedures explained in detail to the SAO in a meeting on June 16, 2022 and in a June 15, 2022 memorandum, "clarification regarding iCORI system."*

In support of the SAO finding, the SAO has pointed to a section of the Office of the Comptroller's Reconciliation Policy entitled "Reconciliation of Cash Receipts," which states in relevant part that reconciliation means "comparing the results from all sources that produce or contain payments and deposit information."

DCJIS simply does not use the iCORI system to reconcile its CORI fees, and so it is an error to refer to a "variance" between fee data in iCORI and MMARS. Instead, DCJIS records and reconciles CORI fees through the nCourt system and through a series of spreadsheets that log this information. To assist the SAO's audit, DCJIS produced CORI fee information from each of these sources. The reconciliation process used by DCJIS demonstrates that all fees collected have been accounted for and tracked. DCJIS confirmed during the audit with the SAO that the SAO was not concerned that anything is "amiss" pertaining to funds. Rather, the SAO was concerned that iCORI systems were not used to reconcile CORI funds.

DCJIS does not use iCORI to reconcile CORI fees because iCORI was never intended to perform accounting functions. DCJIS respectfully disagrees with the SAO finding that the above quoted language from the Office of the Comptroller requires DCJIS to use iCORI to reconcile CORI fees because it is the original system. The quoted language does not require that the original system be used. More importantly, the iCORI system was not designed to perform accounting functions. Rather, it was designed to receive requests for CORI and to ensure compliance with the CORI laws and regulations when releasing CORI reports.

Even so, DCJIS is grateful for the SAO's recommendation, and has discussed the feasibility of iCORI system enhancements with its vendor and has included this potential upgrade as part of its [information technology] capital improvement funding request for [fiscal year 2024].

Auditor's Reply

Although DCJIS may not have designed the iCORI database (which is used for recording CORI requests and generating fees) for reconciliation purposes, it is still the book of original entry[2] for the fees associated with requesting CORI. We acknowledge that amounts collected in MMARS are reconciled through nCourt and DCJIS's spreadsheet; however, the existence of the variance between the iCORI database and MMARS was never fully explained but was thought to be a timing issue. If the iCORI database contained all the transaction information that was ultimately transferred to the two other reconciling items, it too should be able to be reconciled to MMARS.

2. A book of original entry is a book or journal where an organization first records all its transactions.