Managing and Monitoring External Database Access and Abuse of Criminal Justice Data in the Criminal Justice System

Patrick Barrentine

Abstract

The Florida Department of Corrections (FDC) supervises offenders released to the community on probation, community control, sex offender probation or conditional release supervision. In order to supervise these cases across the state, probation officers are granted access to third party databases maintained by their criminal justice partners, to access arrest information, prior records, driver's license information, etc. Utilizing best practices for monitoring and tracking databases each probation officer has access to will assist in ensuring these permissions are removed upon the separation of the employee from an Agency. This will reduce the possibility that criminal justice information could be accessed and/or abused by a former employee.

Introduction

The Florida Department of Corrections is the largest agency in the criminal justice system in Florida. The Department consists of more than 24,000 full-time employees tasked with the safety and security of inmates and offenders under their care, custody and control. Of those, the Office of Community Corrections has 2,796 appropriated full-time positions. Two thousand one hundred ninety-six of these positions are designated as correctional probation officers, who are tasked with supervising the approximate 166,000 offenders on some form of community supervision. (Florida Department of Corrections, community corrections document, pg. 2, 02/19)

The state of Florida consists of 67 counties divided into 20 criminal court circuits. Each county within each circuit may have one or more unique systems to which the officer has access, to assist in monitoring the offenders under their control. The systems are run by other criminal justice agencies in the local area and may include Florida Criminal Information Center (FCIC), clerk of court case management system, state attorney's office case management system, driver's license database, and law enforcement database.

Each of these databases grants our staff third party access to research arrests, criminal history and possibly to file affidavits for arrest electronically. This information is restricted, so staff are granted access based on their employment as a probation officer. No centralized or uniform way to track the access probation officers have in each county/circuit presently exists. When an employee leaves the agency, a security access request is submitted to remove them from the FDC system. This will terminate their access to certain databases that are monitored centrally by the Florida Department of Corrections. What happens to the access to the databases?

This study intends to review best practices in monitoring access to external databases in the criminal justice system. What is the approval process to allow employees access to third party systems? How can access be effectively tracked? What are some types of abuse of criminal justice data? What are the potential disciplinary actions for abuse of access? How do criminal justice organizations insure all access to all systems are terminated once an employee separates from an Agency?

Literature Review

The records management system (RMS) is an integral part of any law enforcement agency's operations. An RMS maintains records of documents, files, and information regarding all law enforcement activity for the agency. This information is the backbone of the Agency's data management, including shared information from other resources. (Dunworth, 2001)

Record keeping for all law enforcement agencies was based almost completely on paper records prior to the 1970's. This changed during the 1980's with the migration to keeping and managing some records on mainframe computers. At this time, only a limited number of agencies were participating based on the cost of access to the computer systems. Many agencies would share access to the computer system to reduce costs. (Dunworth, 2001) As recently as 2001, many law enforcement agencies only have partial computerization of record keeping. In these situations, crime statistics and arrests must be calculated manually. (Dunworth, 2001)

Dunworth reports that as early as 2001, some agencies began to transition to a fully automated records management system. This system can be linked with a computer aided dispatch (CAD) system, to further assist officers responding in the field. The system would also interface with outside databases such as the National Crime Information Center (NCIC) and FCIC. The integration of these systems creates new abilities to analyze crime, provide information to make good decisions and to assist in determining deployment needs for the agency. (Dunworth, 2001)

Substantial support exists for making certain types of a person's criminal records available outside of the criminal justice system, for occasions when the public would benefit from releasing the information. Exceptions approved for disclosing criminal conviction records might include: potential employers, government licensing agencies and other entities of this nature. The public does not support the release of records in which there was only an arrest, and no conviction in a court of law. (International, 2000)

The majority of adults believe that private sector companies granted access to an individual's criminal history should be required to follow the same rules that are required of government agencies which access the same data. Approximately 70 percent express concern that private companies would have access to this data. They feel that only government agencies should have access to this information. (International, 2000)

The definition of information sharing is exchanging or giving users access to explicit data in any form, through information and communication technology. (Praditya & Janssen, 2015) Privacy concerns are based on legal guidelines which are designed to protect confidentiality and prevent unauthorized access to an individual's information. Any sharing of information must be held within the confines of the law. (Plecas, McCormick, Levine, Neal, & Cohen, 2010)

The focus of this research will be on the sharing of individual's criminal history and criminal justice records between law enforcement agencies, and the access granted to each individual officer. Training may be required to allow access to certain databases, for example, a Criminal Justice Information Services (CJIS) certification is required to access records from databases such as FCIC and NCIC. Officers are required to renew their certification every two years to prove they are knowledgeable about the types of information they access, and to whom they can disseminate the information in the performance of their duties. CJIS exchanges criminal justice information with partners such as automated fingerprint systems, crime statistics, and gun purchase background checks. (Anonymous, 2019)

In Florida, officers use many databases to access criminal records and information. Some of these databases are monitored directly by an oversite agency, such as the Florida Department of Law Enforcement (FDLE) that monitors FCIC and NCIC access. Officers additionally have access to the driver and vehicle information database (DAVID) through the Florida Department of Highway Safety and Motor Vehicles. This system allows for immediate retrieval of driver and motor vehicle information, which can be accessed from any computer with internet access. Additionally, each individual must apply for access, which is subsequently approved by their agency point of contact. (Florida DHSMV, 2019) The agency point of contact allows the agency to monitor abuse by staff. This type of tracking will ensure that if an employee separates, the agency can remove access to this database.

DAVID has been abused by officers in the past, to utilize the information for personal reasons, rather than their professional duties as law enforcement officers. Abuse of the system can lead to disciplinary action, up to and including dismissal as well as removal of the law enforcement certification by the FDLE Bureau of Criminal Justice Standards and Training.

A Tampa Bay Times article states that at least eight cases out of a total of 432 inquiries were deemed as misuse where officers accessed the system clearly for personal use. Examples were to investigate fellow officers, to track spouses or significant others, and to gain information for use in child custody and other family court cases. (Altman, 2016)

Further documenting the abuse of the DAVID database, News 4 in Jacksonville reported on unnecessary searches conducted on employees of the news station. In it, multiple news anchors were searched by the Jacksonville Sheriff's Office, including accessing the historical photographs in the database. This was uncovered after a community activist brought the story to them that he had been searched more than 200 times during a five-year period. News 4 employees' records access was determined after a public records request was submitted and returned. Six employees of the news station were reported as having had their records reviewed. (Gardner, 2017)

Abuse of law enforcement access to databases is not isolated to Florida. A New York Times story revealed details of a New York police officer accepting money for information. The story describes how now-retired sergeant Ronald Buell accepted money from a private investigator. In exchange, Buell provided information regarding witnesses and defendants from cases with which the private investigator was involved. According to the story, Buell used his access to the NCIC database at least 15 times during a two-year period to gather information contained in at least 11 federal prosecution cases in

New York. The former sergeant tried to cover his illegal database searches by indicating the NCIC searches were part of an investigation into home invasion robberies. These robberies were part of a “police investigation” that did not exist. (Weiser, 2014)

The capabilities of law enforcement are increasingly dependent on technology. Officers have access to databases from their patrol vehicles based on record management systems and computer aided dispatch systems. The need to share information is also becoming more relevant, with increased demands to share records between local, state and federal agency databases. This demand necessitates the creation of common policies regarding criminal information, information sharing standards, and developing databases or repositories for the shared information. (Hollywood & Winkelman, 2015)

Hollywood and Winkelman have found that some of the key factors to improving information sharing are: improved records management systems, development of repositories for shared criminal justice information, and shared systems such as a third party host to maintain hardware and software. (Hollywood & Winkelman, 2015)

As part of the Department of Justice global advisory committee authorization act of 2011, the National Sheriff’s Association supported information sharing. The ability to collaborate and establish database interoperability and information sharing is vital to partnerships between local, state and federal law enforcement agencies. (Garlock, 2011)

The ability and willingness to share criminal justice information is centrally important to developing an understanding of criminal behavior. This assists in the ability to develop new ways to prevent and reduce crime. (Plecas, McCormick, Levine, Neal, & Cohen, 2010) A program was developed to allow police to create a report, submit it electronically to the prosecutor, who could then share the information with the court.
This increased efficiency by improving the flow of communication and increased public safety by rapidly getting information to stakeholders. (Plecas, McCormick, Levine, Neal, & Cohen, 2010) When developing a shared database or management system, it is imperative to set boundaries and agreements at the beginning, including the scope. This is where you set your participants, define your mission, identify privacy and security, and issue rules for the program. (Ericson, 2004)

The Los Angeles Police Department made an attempt to move their operation to a cloud-based system, hosted by Google. In 2009, the City of Los Angeles, California entered an agreement with prime contractor CSC. The agreement included transitioning local government systems, including the email for Los Angeles Police Department, to Gmail hosted by Google. (Sternstein, 2011)

The issue at hand is with the Criminal Justice Information Services (CJIS) security procedures, which were created by the Federal Bureau of Investigation (FBI). Security of cloud-based data is the major issue. Only a private cloud would be acceptable and only if the owner would agree to abide by the standards set by the FBI. Criminal justice information should not be shared over email in general. However, CJIS policy is very strict and is monitored to ensure compliance. (Sternstein, 2011)

With the great amount of access officers have to an individual’s personal information, what safeguards do we have in place to ensure that the ability to access databases is removed when the employee separates from the agency? What local databases do officers have access to that is not tracked by the State, which only require the officer’s supervisor to approve the access?

The Pinellas County Sheriff's Office has a system called VIPAR, short for Virtual Inmate Processing and Reporting. This allows officers to complete electronically signed arrest affidavits, review arrest records, juvenile records, etc. Officers apply for access to the system based on their professional duties in Pinellas County, Florida as a law enforcement officer, corrections officer, or correctional probation officer.

Technology is believed to increase law enforcement's ability to identify persons of interest, to monitor offenders, to improve the collection of evidence and, in the end, to assist to resolve cases. This technology can assist in identifying persons of interest, or places of interest which have an increased likelihood of involvement in crime. These persons or places can then be targeted by law enforcement to clear pending cases, or ultimately reduce crime and increase recidivism. (Lum, Koper, & Willis, 2017, Vol. 20(2))

Technology alone does not create outcomes in clearing investigations in law enforcement. What is more relevant in regard to technology is how the information is analyzed, organized, and utilized by law enforcement officers and civilian employees. The agency leadership, as well as subcultures within the organization, can impede the uses and outcomes of technology. (Lum, Koper, & Willis, 2017, Vol. 20(2))

The sharing and integration of information is a new challenge for public agencies, and in particular law enforcement agencies. Traditionally, government agencies have entrenched themselves within silos. They would gather information but were hesitant to share any of the information with outside agencies. Integration between local, state, and federal law enforcement agencies is being viewed as a way to increase effectiveness. (Gil-Garcia, Schneider, Pardo, & Cresswell, 2005)

Successful partnerships that have done well at integrating at the county and state levels have stated that a strong foundation based on trust and strong relationships was more important to the process than any particular technology. To this, a strong and organized governance structure was a factor in the success of integration initiatives. (Gil-Garcia, Schneider, Pardo, & Cresswell, 2005)

An officer is required to re-certify the CJIS certification every two years, to maintain FCIC and NCIC access for criminal records including arrest data and warrants. If an officer has access to DAVID, there is an agency point of contact to confirm staff access, as well as regular audits of the system for abuse. Gang database access, state attorney databases, clerk of court data management systems and county sheriff's computer systems are used to look up offense reports and complete arrest affidavits.

The Florida Supreme Court provided an administrative order, which spells out clearly the level of access individuals can be granted based on their role. The court adopted standards for access to electronic records in 2014 under Administrative Order Supreme Court (AOSC) 14-19. This order included a matrix to provide carefully structured levels of access to electronic court records. These levels include general public, user groups with specialized credentials, judges, and court and clerks' office staff, based on statutes and court rules. (Canady, 2019)

Florida Supreme Court Chief Justice Canady and the Access Governance Board of the Florida Courts Technology Commission further recommended updating language to include a gatekeeper authorized by an Agency head, to add, update, and delete user or Agency information to manage access and ensure security. In addition, they further recommend removing an attorney's access to someone's records after they are no longer the attorney on record. (Canady, 2019)

The Florida courts have identified three access methods for viewing electronic court records. Direct access via application to internal live data, web-based application for replicated or live data with security, and web-based portal for public viewing of replicated data. This portal will have variable levels of security that will be based on the role or credentials of the user. The access will further be determined by the matrix provided to govern the amount of access to be provided by the courts. The most access will be granted to judges and authorized court and clerk of court personnel. (Court, 2019)

The Florida Courts Technology Commission and the Clerk of Courts must develop an agreement for users that defines their responsibilities. The clerk may use an online agreement or a written agreement, but the document must be notarized for each user role. The clerk will retain agreements submitted in paper form. Applicants will be given a username and password to be able to access information based on their role, beyond general public information. (Court, 2019)

Methods

The purpose of this research was to identify how criminal justice organizations insure access to all criminal justice databases are terminated once the employee separates as well as monitor the abuse of criminal justice data through this access. This includes identifying best practices in the approval process to gain access to third party databases, how to effectively track access to third party systems in the agency, discovering whether the agency had recent cases of abuse of criminal justice data and the potential disciplinary actions for abuse of access.

Data was gathered through surveys given to members of the Florida Department of Corrections Community Corrections, as well as state, county and local law enforcement agencies. Survey questions were developed to determine if officers in the selected agencies had access to third party criminal justice databases. Does the agency have a point of contact to approve and remove access for agency personnel? Questions were also developed to determine if the agency had recent abuse of criminal justice data, and what range of disciplinary action is being considered or given.

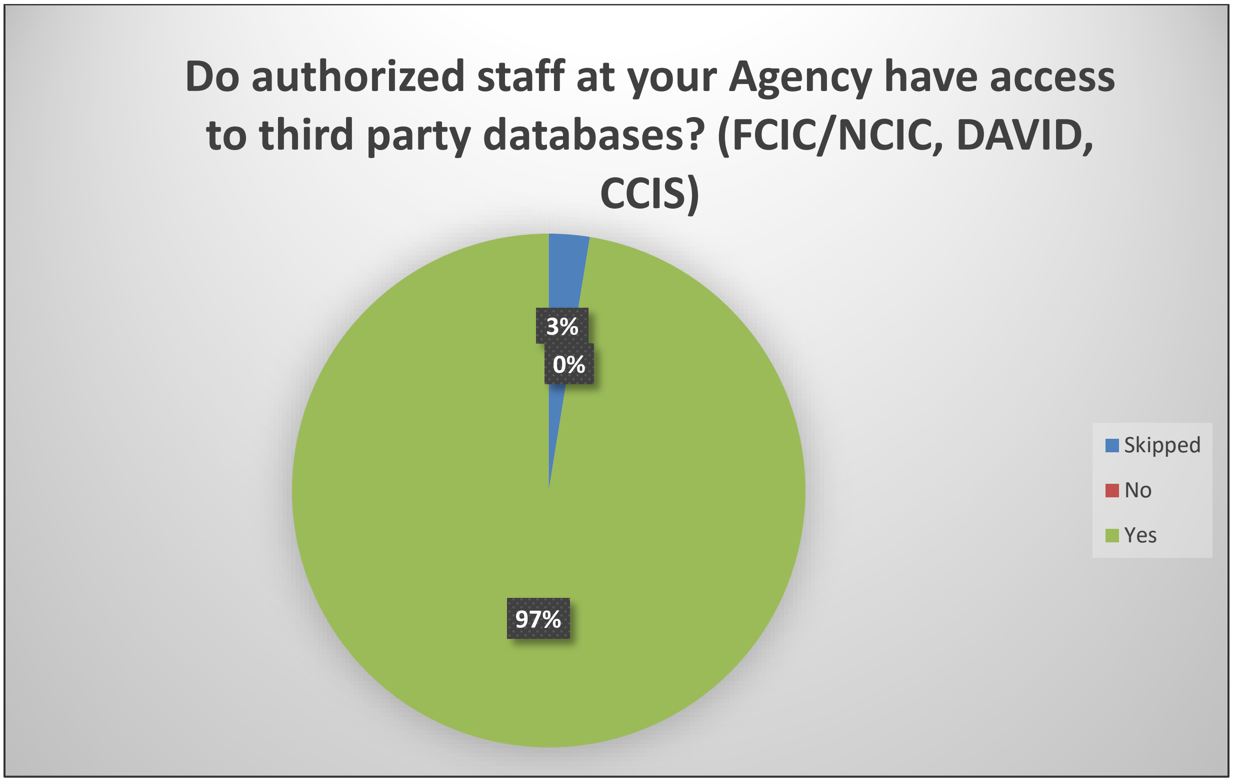
This survey was anonymous in order to encourage truthful responses and to increase the response rate. Any information regarding the identity of staff members that have received discipline will remain anonymous in this study. Responses regarding monitoring third party access will assist in identifying best practices for this process. A weakness to the data collection is that some Agencies may still be reluctant to self-report that they do not track officer/authorized staff member access to criminal justice information databases. Further, they may not choose to reveal that they do not notify their partners when an employee separates from their Agency.

Results

The survey was sent to 40 individuals, identified from a sampling of the criminal justice community. The sample included 20 Community Corrections Circuit Administrators, two managers of Felony Criminal Courts for Clerk of Courts, and representatives from 18 state, county and local law enforcement Agencies. Responses were received from 39 of the 40 surveyed, for a response rate of 97.5 percent. Of those respondents, thirty-eight (94.8 %) answered all 11 questions, and thirty-nine (100 %) answered 9 questions, or (81.8 %) of the survey questions.

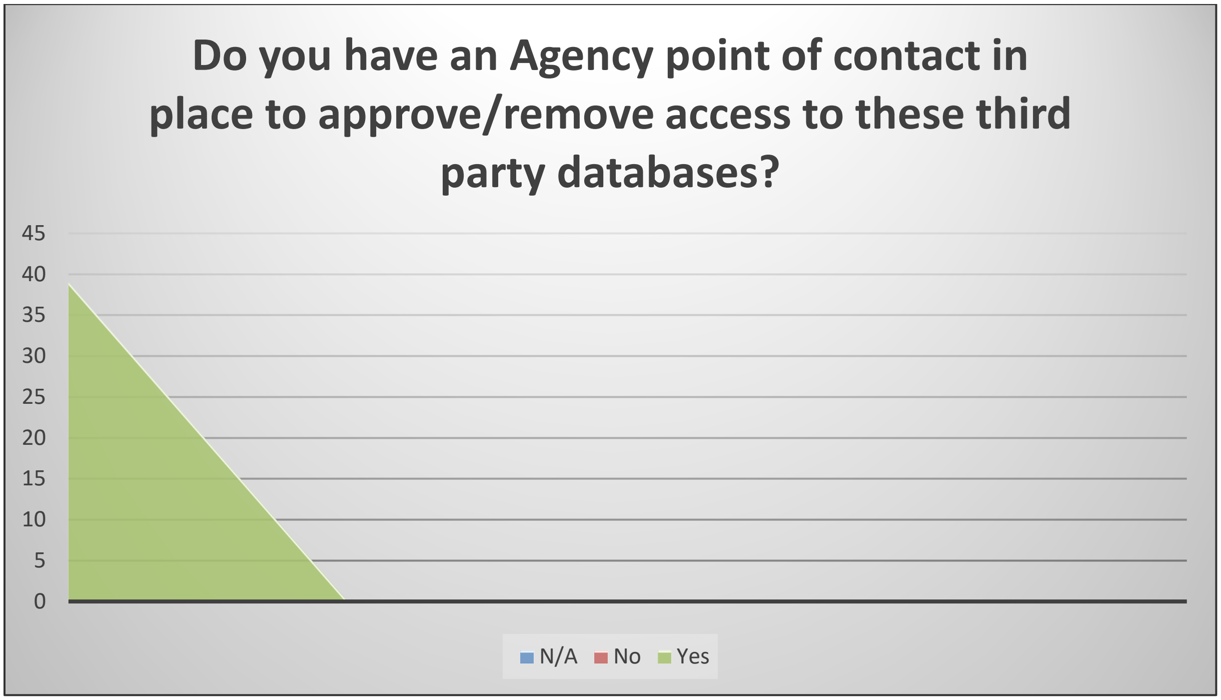
The first question asked the respondents if officers/authorized staff at their Agency have access to third party databases. The examples given were databases to include FCIC/NCIC, DAVID and CCIS. Thirty-eight (94.8 %) of respondents answered yes, that officers and authorized staff do have access to third party databases. One respondent skipped this question.

Table 1: Do officers/staff at your Agency have access to third party databases?



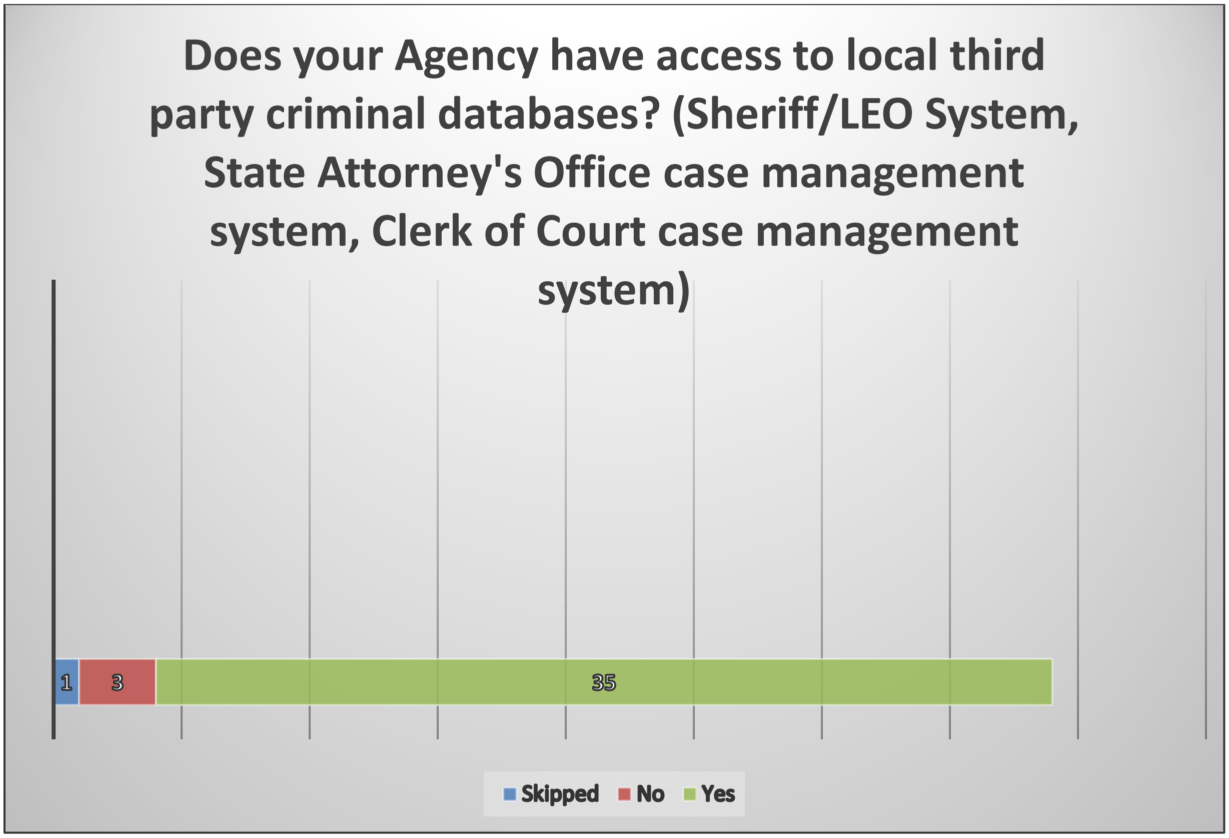
The second question asked respondents if their Agency has a point of contact in place to approve or remove access to these third-party databases. Thirty-nine of the respondents (100 %) answered that yes, their Agency has a point of contact in place to add or remove users.

Table 2: Is there an Agency point of contact to approve/remove database access



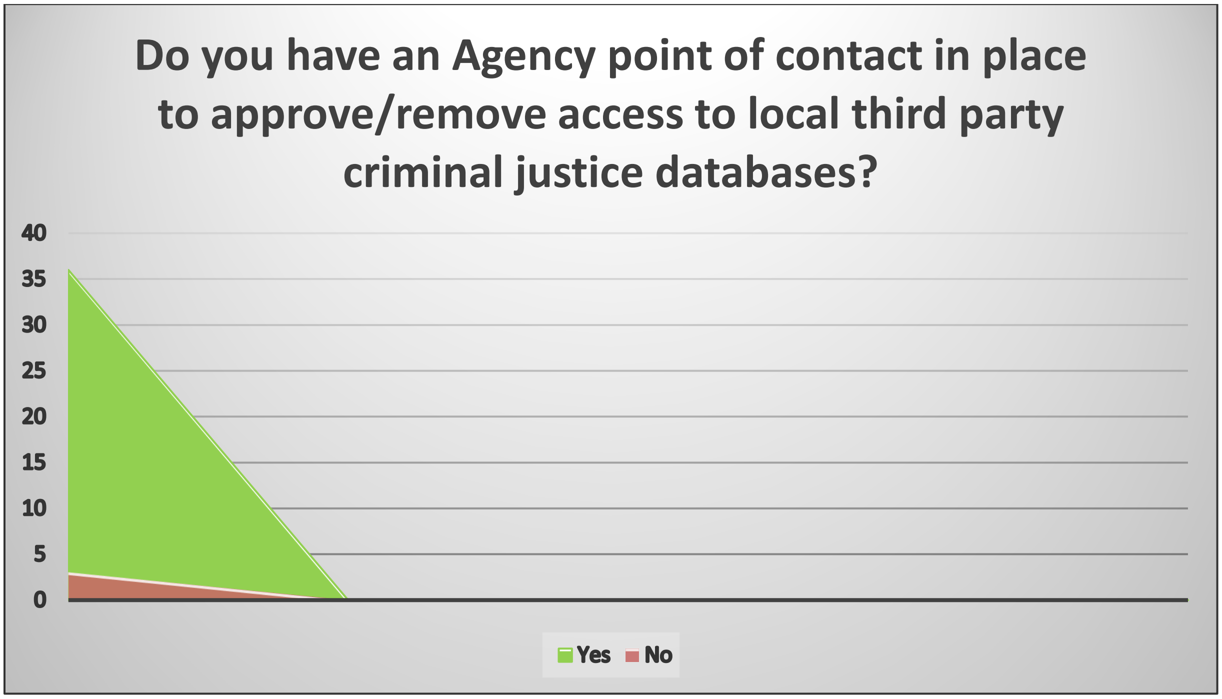
The third question asked the respondents to identify if their Agency has access to local third-party criminal justice databases. Examples given for this question included a Sheriff's Office/LEO system, State Attorney's Office case management system, and Clerk of Court case management system access. Thirty-five of the respondents (92.11 %) indicated that yes, their Agency has access to local third-party criminal justice databases. Three of the respondents (7.89%) indicated no, their Agency does not have access to local third-party databases.

Table 3: Do officers/staff at your Agency have access to local third party databases



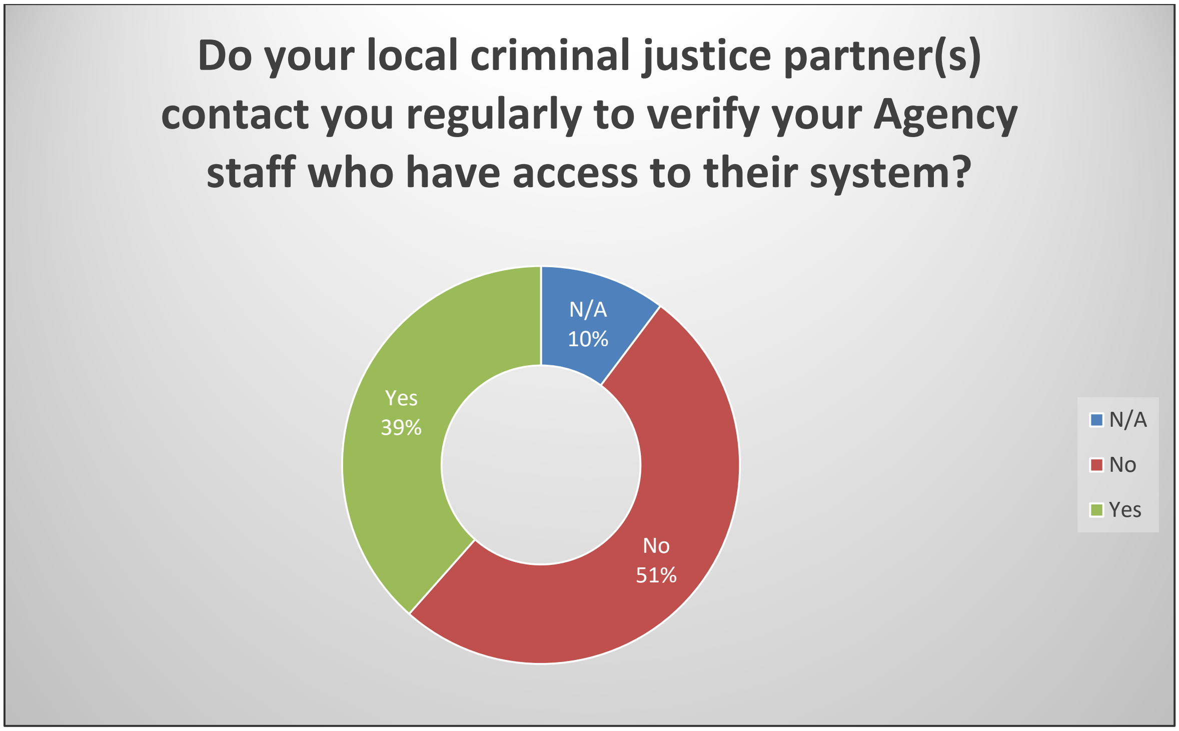
The fourth question asked the respondents to identify if their Agency has a point of contact in place to approve or remove access to local third-party criminal justice databases. Thirty-six (92.31%) of the respondents indicated that yes, their Agency does have a point of contact to approve or remove access for local databases. Three respondents (7.69%) indicated that no, their agency does not have a point of contact to remove local third-party criminal justice database access.

Table 4: Is there an Agency point of contact to approve/remove local database access?



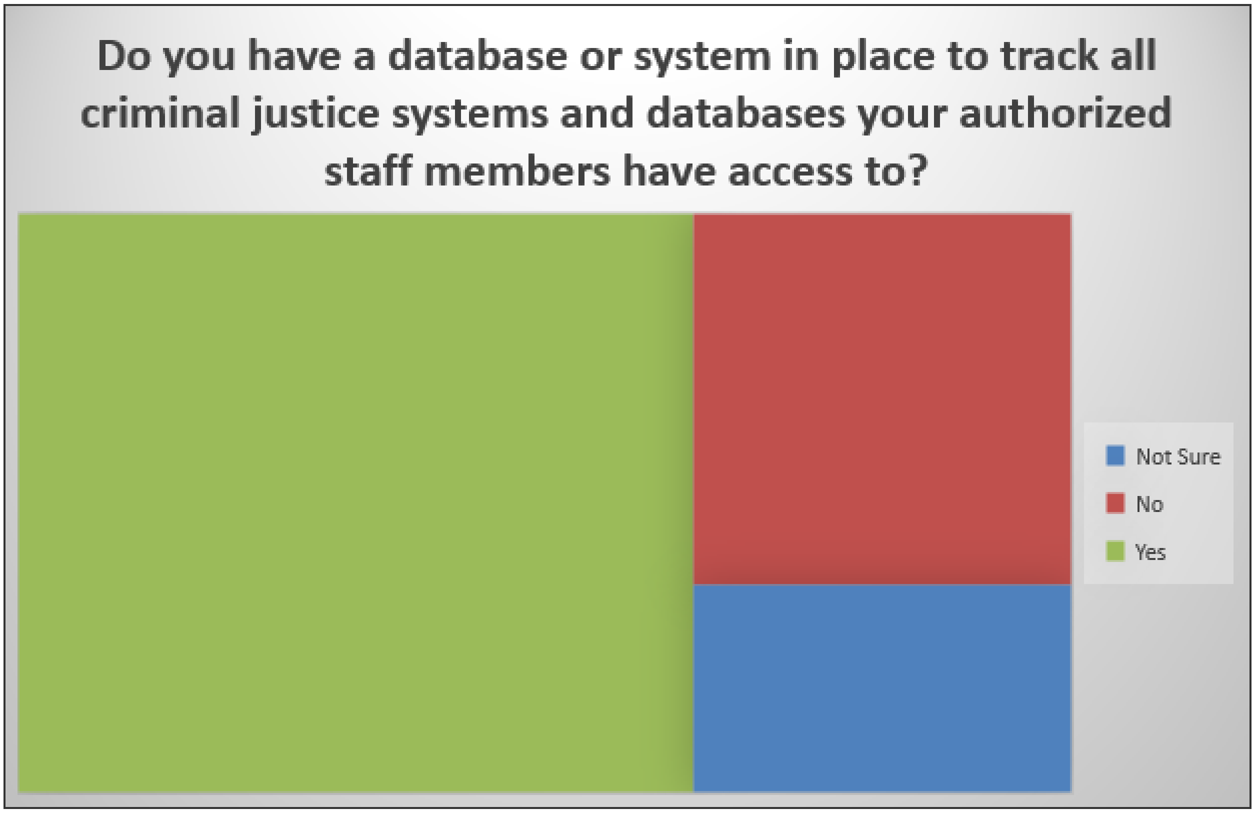
The fifth question asked respondents if they are contacted regularly by their local criminal justice partners to verify their Agency staff who currently have access to that Agency's database. Fifteen of the respondents (38.46%) indicated that yes, their local partners do contact them regularly to verify who has access to their system. Twenty (51.28%) of the respondents reported that no, their local partners do not contact them regularly to verify their Agency staff who have access to the other Agency's system. Four respondents (10.26%) responded not applicable to their Agency.

Table 5: Do your criminal justice partners contact you to verify users regularly?



The sixth question asked respondents to identify if their Agency has a database or system in place to track all criminal justice systems and databases their officers/ authorized staff members have access to. For this question, 25 respondents (64.10%) stated that yes, their Agency has a database or system to track all criminal justice systems and databases for which staff have access. Nine respondents (23.08%) indicated that their Agency does not have a system or database in place to track this. Five respondents (12.82%) indicated that they are not sure if their Agency has a system in place to track all databases their staff have access to.

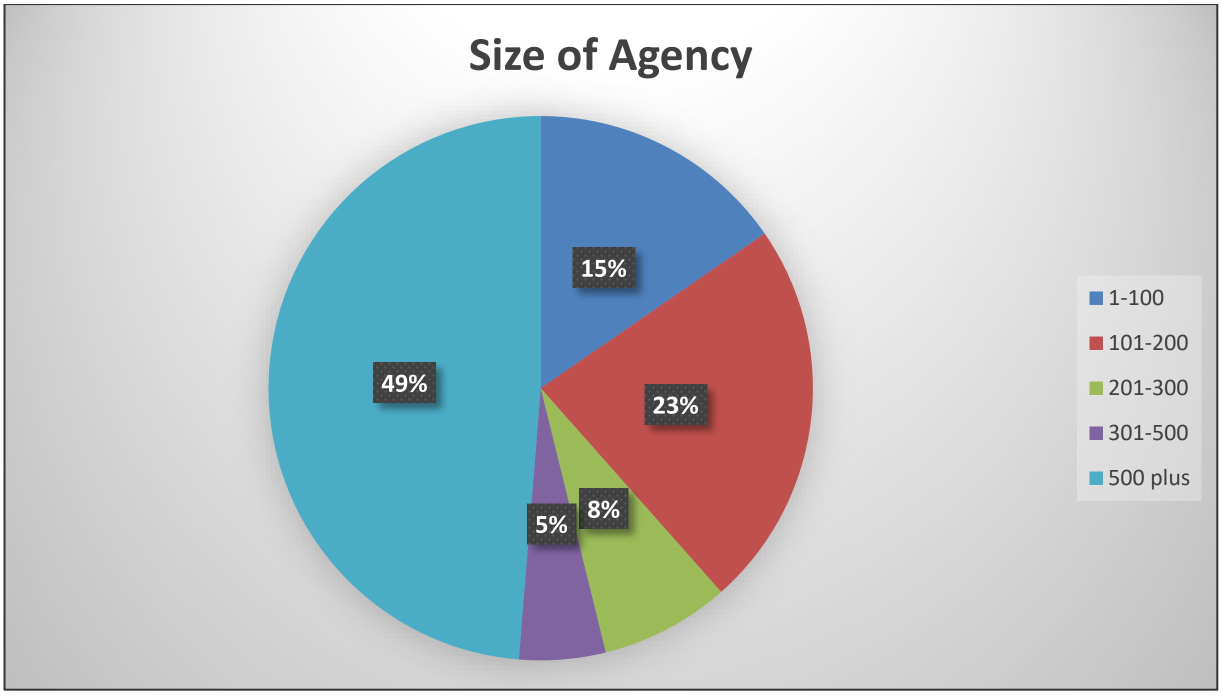
Table 6: Do you have a system to track databases authorized for staff members?



The seventh question asked respondents to identify if their Agency notifies criminal justice partners when an employee separates from their Agency, and immediately remove access. Thirty-four respondents (87.18%) indicated that yes, their Agency does notify their criminal justice partners when an employee separates, and immediately remove access. Five respondents (12.82%) stated that no, they do not notify their criminal justice partners when an employee separates from their Agency.

Question eight discussed the size of the respondents' Agency. Six respondents (15.38%) were from an Agency of 100 or less. Nine respondents (23.08%) represented an Agency of 101 to 200. Three respondents (7.69%) were from an Agency 201 to 300. Two respondents (5.13%) were from an agency of 301 to 500. The majority of respondents polled, nineteen (48.72%), were from an Agency of 500 plus.

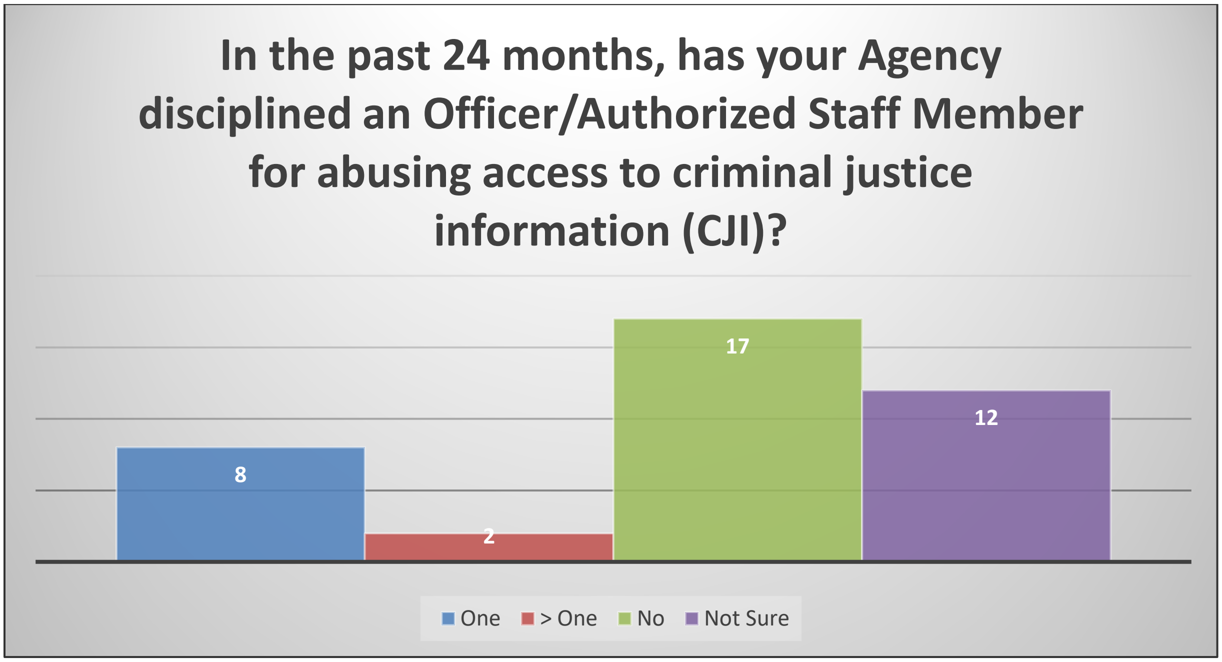
Table 8: Size of Agency



The next three questions shifted from access granted to an officer or authorized staff member to abuse of access granted. These questions asked about abuse of criminal justice data by officers or staff members from their Agency. The response choices for these questions ranged from: Yes, one officer/authorized staff member; Yes, more than one officer/authorized staff member; No, and not sure.

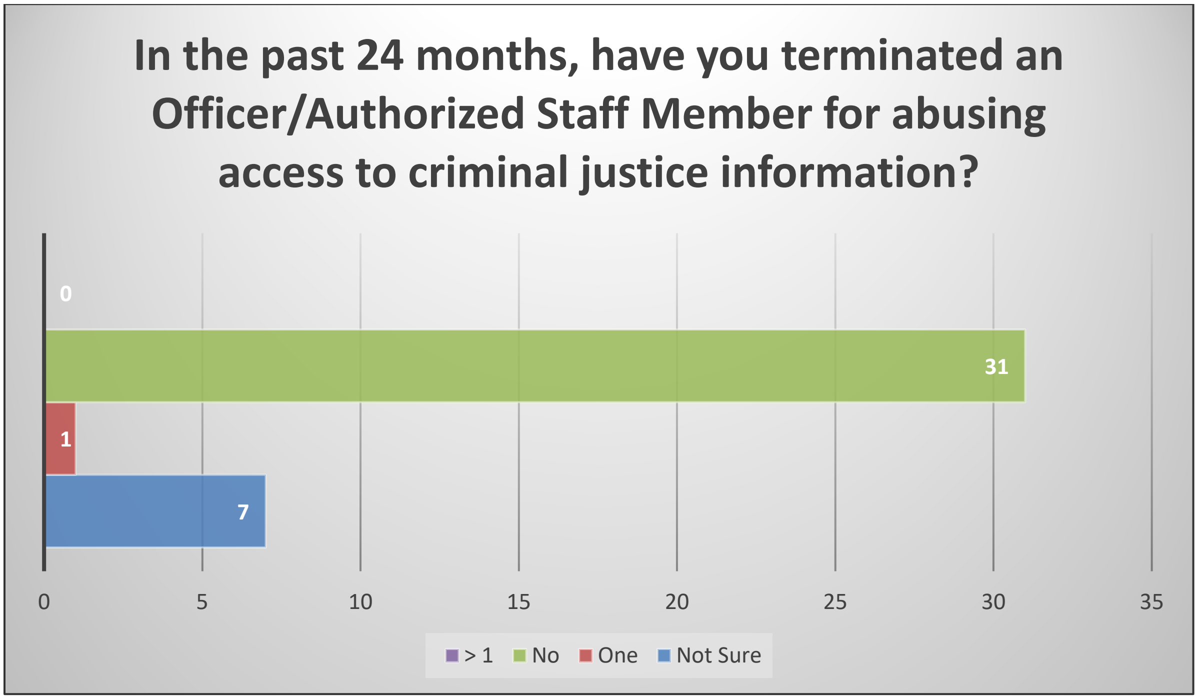
The ninth question asked respondents if, in the past 24 months, their Agency had disciplined an officer or authorized staff member for abusing access to criminal justice information (CJI). Eight of the respondents (20.51%) indicated that they had disciplined one officer or authorized staff member in the past 24 months. Two respondents (5.13%) indicated that yes, they had disciplined more than one officer or authorized staff member. Seventeen respondents (43.59%) indicated that no, they had not disciplined an officer or authorized staff member and twelve respondents (30.77%) indicated that they were not sure.

Table 9: Officer/ Authorized Staff disciplined for abusing criminal justice information



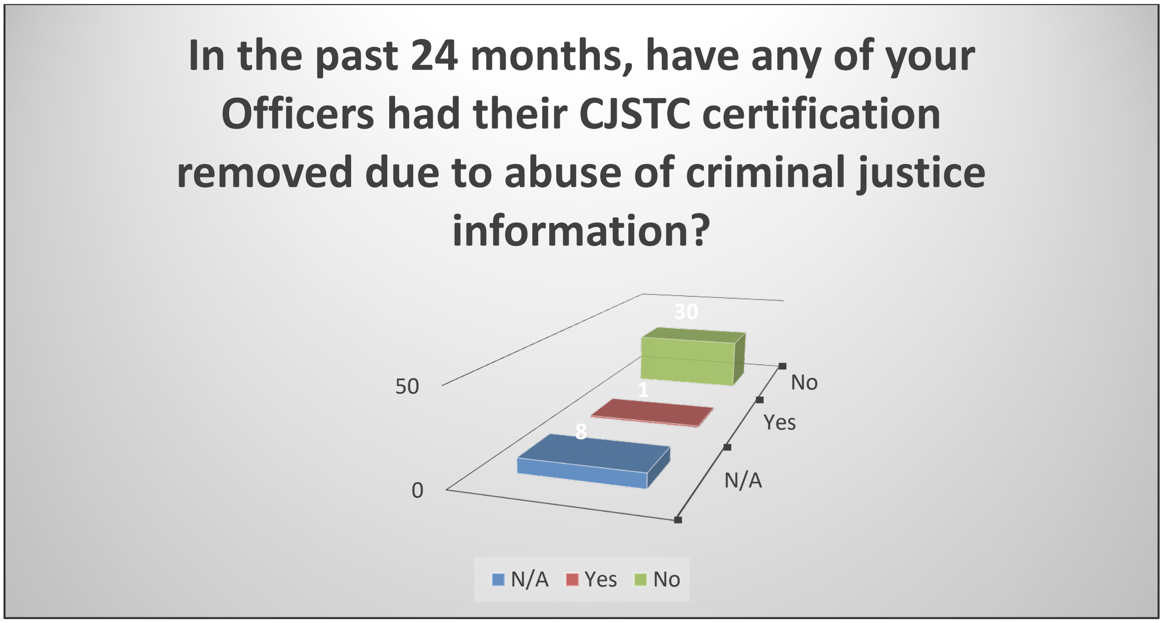
Question 10 asked respondents if their Agency had terminated an officer or authorized staff member for abusing access to criminal justice information in the past 24 months. One respondent (2.56%) reported that yes, they had terminated one officer or authorized staff member in the past 24 months for abusing access to criminal justice information. The majority of respondents, thirty-one (79.49%) reported no, they had not terminated a staff member for this in the past 24 months. Seven respondents (17.95%) indicated they were not sure.

Table 10: Officer/authorized staff terminated for abusing criminal justice information



The eleventh and final question on the survey asked if their Agency has had an officer have their CJSTC Certification removed due to abuse of criminal justice information in the past 24 months. One respondent (2.56%) reported that yes, they had an officer who had their CJSTC Certification removed due to abuse of criminal justice information. The majority of respondents, thirty (76.92%) reported no, none of their officers had their certification removed and eight respondents (20.51%) indicated that this question was not applicable to them.

Table 11: Officer CJSTC certification removed for abusing criminal justice information



Discussion

The results of the survey show that there is a definite need to track access to third party criminal justice databases. One Agency identified during the survey that they had an officer lose their certification from the Criminal Justice Standards and Training Commission. For this to occur, the Commission would have a formal hearing that the officer is permitted to attend and present any relevant information before a ruling is made. This is only 2.5 percent of the group surveyed; however, another 20.5 percent answered that the question was not applicable. This could mean the respondent did not know this information for their Agency, which could increase these numbers substantially.

When it comes to termination of an officer or authorized staff member for abuse of access to criminal justice information, again, one respondent identified they had terminated an employee for abuse of criminal justice information. Additionally, 18 percent of the respondents indicated they were not sure of this information for their Agency. The majority of respondents confirmed that 80 percent of the Agencies polled had not terminated an employee for abuse of criminal justice information.

Twenty-five percent of the Agencies polled have disciplined one or more staff members for abusing criminal justice information in the past 24 months. This is a much greater indicator that there is a prevalent issue with the abuse of criminal justice information. These numbers indicate that potentially one out of every four officers or authorized staff members are committing an abuse of data that warrants disciplinary action.

One hundred percent of reporting Agencies indicated that their officers and authorized staff members have access to FCIC/NCIC, DAVID or CCIS, which are third party databases that contain criminal justice information. All Agencies have a designated point of contact to track these databases and approve or remove an employee’s access to them.

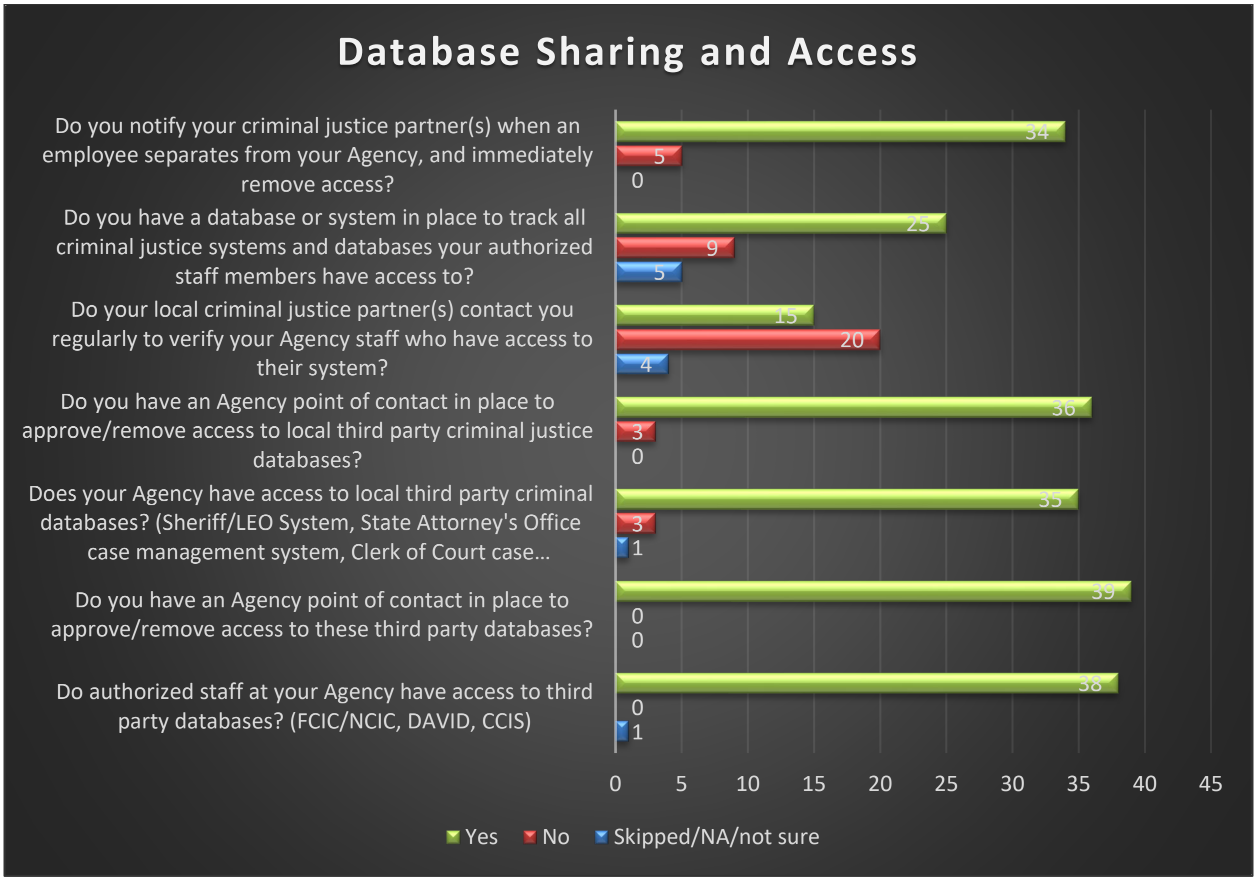
Ninety-two percent of Agencies indicated their employees have access to local third party databases such as a sheriff’s system, state attorney’s office case management system or clerk of court case management system. The same number of Agencies have a point of contact to track the local databases and approve or remove employee access.

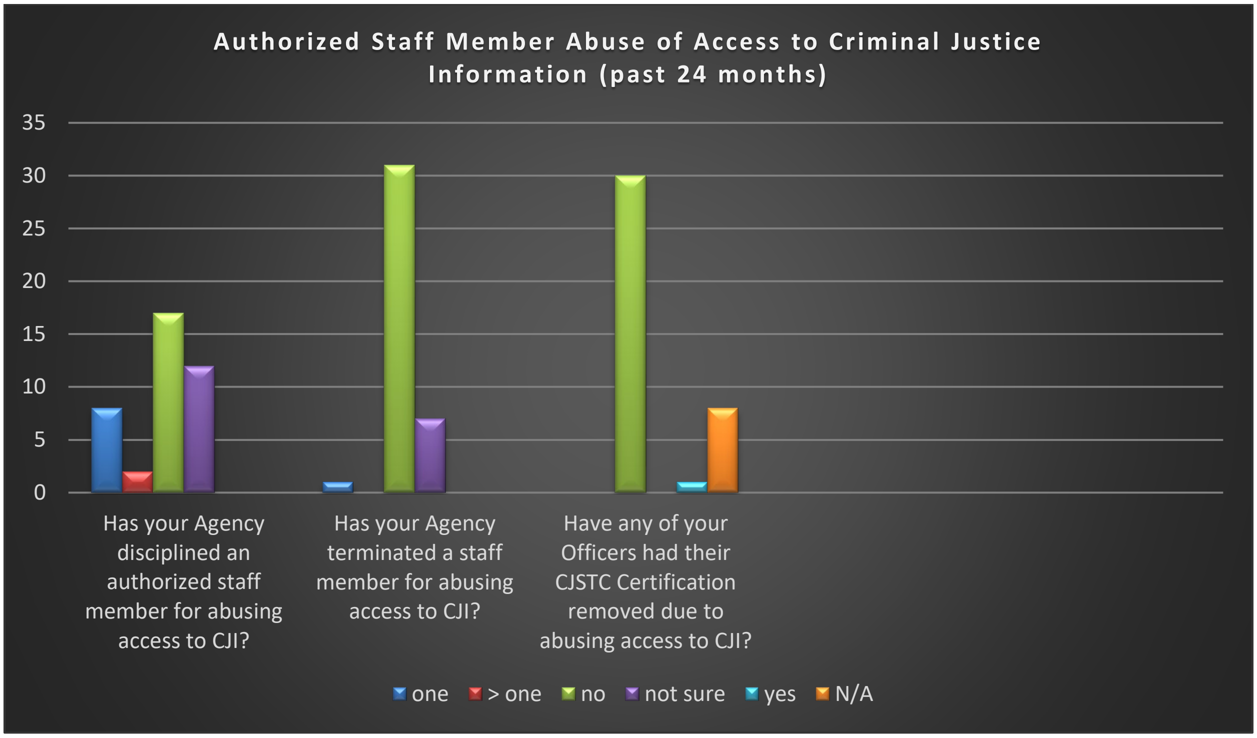
Fifty-one percent of Agencies do not get contacted by their criminal justice partners that grant them access to databases, to confirm their employees who have access to a data management system controlled by them. This is a concerning number, as there can be a large turnover for an Agency, based on current trends in criminal justice, yet an employee’s access to sensitive information may not be removed promptly if they separate from the Agency.

Of the Agencies included in this survey, only 64 percent have a system in place to track all criminal justice systems and databases to which an officer/authorized staff member has access. This leaves 23 percent that identified they do not have a system in place, and 13 percent that are not sure. As much as 36 percent may not have a system in place to track these databases.

Thirteen percent of the Agencies surveyed indicated they do not notify their criminal justice partners when an employee separates, and do not immediately remove access. This number again indicates a definite issue with tracking third party databases. These numbers may be lowered if a strong system is in place to track the databases to which each employee has access.

Table 12: Summary of Survey Question Results





Recommendations

Very little information was located regarding the management of third-party database access. A huge amount of information existed regarding the development of law enforcement databases, how to set up a governing body, and how to develop rules for access.

Not much information was available regarding how agencies track access to each database. Perhaps one way that an Agency could track access to third party databases would be to attach their approved access to their employee file, so that the designated representative would know which agencies would need to be notified of employee separation.

The Florida Department of Corrections, Community Corrections supervises offenders on community supervision in all 67 counties of the State of Florida. These 67 counties are divided into 20 judicial circuits. Several circuits cover as many as seven counties in their jurisdiction that could potentially have access to information. Each county would have a separate clerk of court, sheriff and local law enforcement agency. Each of these has the potential for multiple local third-party criminal justice data systems to which individual staff members can have access.

The Department of Corrections needs a tracking system that can be customized for each judicial circuit that can be utilized to track all databases to which an officer or staff member has access. This tracking system will need to be updated on a regular basis, and separating employees should be removed to a separate folder, after all reported access has been removed. Each Circuit will need to develop a list of all commonly accessed third party databases in their jurisdiction, and have a designee notify each of those agencies once an employee separates, to ensure the separating employee is removed immediately from access. Each Circuit will need a designee who is responsible for verifying whether an employee is still working for the agency, and for coordinating with third party agencies when they send a list of employees with access for review.

A system similar to electronic training might be developed for tracking database access for each employee. This would track the databases to which the employee is granted access and the date access is granted.

In addition, the Agencies who allow access to their databases should look at a regular tracking mechanism to ensure dormant accounts are either signed into or removed to ensure the person is still employed by the Agency. Only Agency emails should be allowed to be utilized for access. If the email is returned undeliverable, the third-party Agency should immediately suspend or terminate the access and email the point of contact for the Agency.

Circuit Administrator Patrick Barrentine began his employment with the Florida Department of Corrections in 1998 as a Correctional Probation Officer in Lakeland and progressed through the ranks as a Correctional Probation Senior Officer, Correctional Probation Specialist, Correctional Probation Supervisor and Correctional Probation Senior Supervisor. In July of 2014, Pat was appointed as Deputy Circuit Administrator of Pinellas and Pasco Counties, Community Corrections. In March of 2015, he was appointed as Circuit Administrator, and has served in the Sixth Judicial Circuit, Pinellas and Pasco since that time. Pat has a Bachelor's Degree in Political Science from the University of South Florida.

References

Altman, H. (2016, August 27). Misuse of state's driver database often for personal reasons. *Tampa Bay Times*. https://www.tampabay.com/news/publicsafety/states-driver-database-ripe-for-misuse/2291246.

Anonymous. (2019). *Law inforcement information sharing.* Director of National Inteligence, Office of.

Canady, C. T. (2019). *Administrative Order Supreme Court 19-20.* Tallahassee: Supreme Court of Florida.

Court, F. S. (2019). The standards for access to electronic court records and the access Security Matrix. Retreived from: *https://www.flcourts.org/Resources-Services/Court-Technology/Technology-Standards*, 1-10.

Dunworth, T. (2001). Criminal justice and the IT revolution. *Federal Probation*, *65*(2).

Ericson, L. (2004). Ownership is everything. *Law & Order*, 36.

Florida DHSMV. (2019). *Request security access to the DAVID system.* Florida Department of Highway Safety and Motor Vehicles.

Gardner, L. (2017). I-TEAM: Unauthorized searches made on law enforcement database. *News4Jax.com*. https://www.news4jax.com/news/investigations/i-team-unauthorized-searches-made-on-law-enforcement-database.

Garlock, S. (2011). *Government Affairs Update.* NSA Government Affairs.

Gil-Garcia, J. R., Schneider, C. A., Pardo, T. A., & Cresswell, A. M. (2005). Interorganizational information integration in the criminal justice enterprise: Preliminary lessons from state and county initiatives. *Proceedings of the 38th Hawaii International Conference on System Sciences- 2005* (p. 118.3). HICSS '05 Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) - Track 5 - Volume 05.

Hollywood, J. S., & Winkelman, Z. (2015). *Improving information sharing across law enforcement.* RAND Corporation.

International, O. R. (2000). *Privacy, technology and criminal justice information; Public attitudes toward uses of criminal history information.* Bureau of Justice Statistics, U.S. Department of Justice, SEARCH, The National Consortium for Justice Information Statistics.

Lum, C., Koper, C. S., & Willis, J. (2017). Understanding the limits of technology's impact on police effectiveness. *Police Quarterly*, *20*(2), 135-163.

Plecas, D., McCormick, A. V., Levine, J., Neal, P., & Cohen, I. M. (2010). *Evidence-based solution to information sharing between law enforcement agencies. Emerald Insight.*

Praditya, D., & Janssen, M. (2015). *Benefits and challenges in information sharing between the public and private sectors. Netherlands: Proceedings of the European Conference on e-Government, ECEG.*

Sternstein, A. (2011). Federal cyber rules halt LAPD's move to Google Apps. *Nextgov.com (online)*, https://www.nextgov.com/it-modernization/2011/10/federal-cyber-rules-halt-lapds-move-to-google-apps/50016/.

Weiser, B. (2014, October 22). 2 former new york police officers misused database, U.S. says. *New York Times*.

Appendix A

Survey Questions

Managing and Monitoring Criminal Justice Database Access and Abuse of Criminal Justice Information

1.) Do Officers/ Authorized Staff at your Agency have access to third party databases? (FCIC/NCIC, DAVID, CCIS)

2.) Do you have an Agency point of contact in place to approve/ remove access to these third party databases? (FCIC/NCIC, DAVID, CCIS)

3.) Does your Agency have access to LOCAL third party criminal justice databases? (Sheriff/ LEO System, State Attorney's Office case management system, Clerk of Court case management system, etc.)

4.) Do you have an Agency point of contact in place to approve/ remove access to LOCAL third party criminal justice databases? (Sheriff/ LEO System, State Attorney's Office case management system, Clerk of Court case management system, etc.)

5.) Does your local criminal justice partner/s contact you regularly to verify your Agency staff who have access to their system?

6.) Do you have a database or system in place to track all criminal justice systems and databases your Officers/ authorized staff members have access to?

7.) Do you notify your criminal justice partner/s when an employee separates from your Agency, and immediately remove access?

8.) How large is your Agency?
A.) 1-100
B.) 101-200
C.) 201-300
D.) 301-500
E.) 500 Plus

9.) In the past 24 months, has your Agency disciplined an Officer/ Authorized Staff Member for abusing access to criminal justice information (CJI)?

10.) In the past 24 months, have you terminated an Officer/ Authorized Staff Member for abusing access to criminal justice information?

11.) In the past 24 months, have any of your Officers had their CJSTC Certification removed due to abuse of criminal justice information?