

PALM BEACH COUNTY
BOARD OF COUNTY COMMISSIONERS
AGENDA ITEM SUMMARY

Meeting Date: July 2, 2024 [X] Consent [] Regular
[] Ordinance [] Public Hearing

Department: Facilities Development & Operations

I. EXECUTIVE BRIEF

Motion and Title: Staff recommends motion to:

A) **Approve** a Criminal History Record Check User Agreement for Non-Criminal Justice Purposes (“Agreement”) with the Florida Department of Law Enforcement (“FDLE”). FDLE’s services are provided on an as-needed basis, but based upon last year’s use, it is estimated that expenditures for the remainder of this fiscal year will total approximately \$19,000, and

B) **Authorize** the County Administrator or designee, which in this case shall be the Director of Facilities Development & Operations (“FDO”) to execute the Agreement on behalf of the Board of County Commissioners (“Board”); and to execute future amendments to or updated versions of this Agreement with FDLE, upon review and approval by the County Attorney’s Office.

Summary: The Palm Beach County Criminal History Record Check Ordinance requires criminal history record checks of certain persons requiring access to facilities that the Board has determined to be critical to public safety or security and/or critical to criminal justice information security. This Agreement is FDLE’s standard agreement with governmental agencies to provide access to criminal history records and it details the fees for FDLE’s services, the procedures for submitting fingerprints and the retention, privacy and security requirements for criminal history records. **(FDO ESS) Countywide (MWJ)**

Background and Justification: On August 19, 2003, the Board of County Commissioners adopted Ordinance No. 2003-030, as amended by Ordinance No. 2008-007 and 2013-023, to establish the County’s program for conducting criminal history record checks on contractors, vendors, repair and delivery persons who seek unescorted access to certain County facilities. At the time this Ordinance was adopted, the County entered into an earlier version of this FDLE standard Agreement. FDLE has established and maintains intrastate systems for the collection, compilation, and dissemination of state criminal history records and information in accordance with Section 943.05(2), Florida Statutes, and, additionally, is authorized and does in fact participate in federal and interstate criminal history records systems pursuant to Section 943.054, Florida Statutes. The County shall use the criminal history records acquired under this Agreement for the purpose of screening applicants to determine their suitability for employment, volunteering or a vendor having unescorted access to certain facilities.

Attachments:

- 1. FDLE Agreement

Recommended By:  
Department Director Date
Approved By:  
County Administrator Date

II. FISCAL IMPACT ANALYSIS

A. Five Year Summary of Fiscal Impact:

Fiscal Years	2024	2025	2026	2027	2028
Capital Expenditures					
Operating Costs	<u>\$19,000</u>	<u>\$50,000</u>	<u>\$52,000</u>	<u>\$54,000</u>	<u>\$56,000</u>
External Revenues					
In-Kind Match (County)	_____	_____	_____	_____	_____
NET FISCAL IMPACT*	<u>\$19,000</u>	<u>\$50,000</u>	<u>\$52,000</u>	<u>\$54,000</u>	<u>\$56,000</u>
# ADDITIONAL FTE POSITIONS (Cumulative)	_____	_____	_____	_____	_____
Is Item Included in Current Budget:	Yes	<u>X</u>	No	_____	
Is this item using Federal Funds:	Yes	_____	No	<u>X</u>	
Is this item using State Funds:	Yes	_____	No	<u>X</u>	

Budget Account No: Fund 0001 Dept 410 Unit 4130 Object 4901

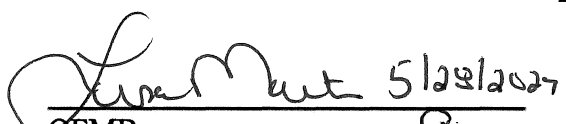

B. Recommended Sources of Funds/Summary of Fiscal Impact:

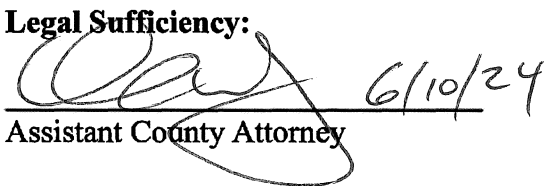
Services are provided on an as-needed basis and the expenditures above are estimated based on last year's use and included in the operating budget. The previous contract commenced August 19, 2003 and this replacement contract is ongoing and can be suspended/terminated by either party at any time.

C. Departmental Fiscal Review: 

III. REVIEW COMMENTS

A. OFMB Fiscal and/or Contract Development Comments:

 OFMB 5/28/2024 EJW 5-28-24	 Contract Development and Control 6/5/24 MK 6/5/24
--	---

B. Legal Sufficiency:

 Assistant County Attorney
 6/10/24

C. Other Department Review:

 Department Director

This summary is not to be used as a basis for payment.



Criminal Justice Information Services
Criminal History Services

Criminal History Record Check User Agreement for Non-Criminal Justice Purposes

Customer/Agency Name: CNTY - PALM BEACH COUNTY

User ORI: FL922890Z

- I. This Agreement, entered into between the Florida Department of Law Enforcement (hereinafter referred to as FDLE), an agency of the state of Florida with headquarters in Tallahassee, Florida, and CNTY- PALM BEACH COUNTY (hereinafter referred to as the User), located at 2633 VISTA PARKWAY WEST PALM BEACH, FL 33411, recites that:
 - A. User is an agency of the state of Florida, established by law and required/authorized to submit fingerprint images and review resultant criminal history records as part of the screening process for purposes of state employment, licensing, permitting, granting access, registration, or certification pursuant to Section(s) ORD NO 2003 030, 2014 004, Florida Statutes (F.S.), which statute(s) has/have been approved by the United States Department of Justice (DOJ) pursuant to Public Law 92-544, 86 Stat. 1115 and 28 C.F.R. Section 20.33, and form(s) the legal basis for User's access to criminal history record information derived from the systems of the DOJ. The following Originating Agency Identifier (ORI) number has been assigned and will be used for the approved submissions: FL922890Z.
 - B. FDLE has established and maintains intrastate systems for the collection, compilation, and dissemination of state criminal history records and information in accordance with Subsection 943.05(2), F.S., and, additionally, is authorized and does in fact participate in federal and interstate criminal history records systems pursuant to Section 943.054, F.S.
 - C. FDLE and its user agencies are subject to and must comply with pertinent state and federal laws relating to the obtaining, use, and dissemination of records and

record information derived from the systems of FDLE and the DOJ (Chapter 943, F.S., Chapter 11C-6, F.A.C., Title 28, Part 20 C.F.R.).

- D. The National Crime Prevention and Privacy Compact (Compact) Act of 1998 established an infrastructure by which states can exchange criminal records for non-criminal justice purposes according to laws of the requesting state and provide reciprocity among the states to share records without charging each other for the information. The Compact also established a Council to monitor the effective use of the Interstate Identification Index (III) system for Federal-State exchange to ensure rules and procedures for effective and proper operations for Non-Criminal Justices purposes. The Council requires each state to adhere to national standards concerning record dissemination, use, system security, and other duly established standards, including those that enhance the accuracy and privacy of such records. The Federal Bureau of Investigation (FBI) shall conduct a triennial audit of each state to ensure compliance with Compact policies. Failure to remain compliant with Compact policies by each state could result in sanctions levied by the Council or ultimately loss of access to criminal history information contributed by other states through the III.
- E. User is required to obtain and FDLE is required and willing to provide such services as long as proper reimbursement is made and strict compliance with all applicable federal and state laws, rules, and regulations is observed.

II. Now, therefore in light of the foregoing representations and the promises, conditions, and terms, more fully set forth hereinafter or incorporated by references and made a part hereof, the FDLE and User do mutually agree as follows:

- A. FDLE agrees to:
 - 1. Assist User concerning the privacy and security requirements imposed by state and federal laws; provide User with copies of all relevant laws, rules, and/or regulations as well as updates as they occur; and, offer periodic training for User's personnel;
 - 2. Provide User with such state criminal history records and information as reported to, processed, and contained in its systems and legally available to the User; and,
 - 3. Act as an intermediary between User and the DOJ, securing for the use and benefit of User such federal and multi-state criminal history records or information as may be available to User under federal laws and regulations.
- B. User agrees to:
 - 1. Provide FDLE with properly executed applicant fingerprint submissions.

2. Keep all records necessary to facilitate a security audit by FDLE and to cooperate in such audits as FDLE or other authorities may deem necessary. Records which may be subject to audit are criminal history records and notification that an individual has no criminal history, internal policies and procedures articulating the provisions for physical and personnel security, and an executed copy of this user agreement.
3. As determined by type of criminal history request and method of submission, reimburse FDLE in a timely fashion, in accordance with Section 943.053(3)(e) F.S., upon proper presentation of billing for state services rendered. If user contracts with an authorized and properly registered third-party service provider or Livescan vendor for electronic submission of fingerprint-based criminal history requests, FDLE will collect payment for state services rendered directly from such service provider or vendor upon submission of each criminal history request.
4. As determined by type of criminal history request and method of submission, reimburse the FBI in a timely fashion, via FDLE, upon proper presentation of billing for federal services rendered. If user contracts with an authorized and properly registered third-party service provider or livescan vendor for electronic submission of fingerprint-based criminal history requests, FDLE will collect payment for federal services rendered directly from such service provider or vendor upon submission of each criminal history request.
5. As applicable, maintain adequate records and monitor allocated funds for payment of services under this agreement.
6. Ensure that the appropriate personnel are informed that the use of criminal history records and information derived from processed applicant fingerprint submissions are restricted and that such information should not be discussed with others or released to others except as specified in this agreement. Applicants should be informed that inappropriate release of non-Florida criminal history information is prohibited under pertinent federal regulations (28 C.F.R. Part 20), which are reflected in state law under Section 943.054, F.S. See Florida Attorney General's Opinion 99-1. Florida criminal history information should be used only for the purpose stated in the request. See Section 943.053(4), F.S., Section 435.09, F.S., and Rule Chapter 11-C, F.A.C.
7. Promptly advise FDLE of any violations of this agreement.
8. User shall maintain an updated Agency Contact Form with FDLE and provide upon request.

- III. Retention of Applicant Fingerprints for Applicant Fingerprint Retention and Notification Program (AFRNP) Participating Users
- A. FDLE shall enter and retain in the Biometric Identification System (BIS) the applicant fingerprints submitted for state and national criminal history checks, by agencies having specific statutory authorization, to participate in the AFRNP for current and prospective employees, contractors/vendors, volunteers, and persons seeking to be licensed or certified.
 - B. Such applicant fingerprints shall be submitted in an acceptable digitized format for entry into BIS, and shall be retained.
 - C. Users submitting applicant fingerprints in accordance with the authorizing statute shall notify individual applicants of the requirements of participation in the AFRNP.
 - D. When the subject of fingerprints submitted for retention under this program is identified with fingerprints from an incoming Florida arrest, as confirmed by fingerprint comparison, FDLE shall advise the user which submitted the applicant fingerprints of the arrest in writing (or other manner prescribed by FDLE). Arrests made in other states or by the federal government will not result in notification, as access to these arrests is restricted by federal law. The information on arrests for these applicants in other states and by the federal government is available only upon a fingerprint submission to FDLE which will be forwarded to the FBI. Additionally, while it is not expected to be a frequent occurrence, it should be understood that if the submitted fingerprints for an applicant were of sub-standard quality or if the fingerprints submitted on an arrested individual were of sub-standard quality, the identification of these persons as the same may not occur and an arrest notification may not be made. Additionally, until the arrest fingerprint submission is received by FDLE, FDLE will have no way to identify the arrested person as the individual retained in AFRNP.
 - E. The annual fee for participation in the AFRNP shall be \$6 per individual record retained. The initial entry of an applicant's fingerprints into the AFRNP database must be accompanied by a state and national criminal history records check. There is no additional fee for the first year of participation in the program. For each succeeding year, the \$6 per record annual fee will be charged. Governmental agencies will be billed for this fee annually in advance on the anniversary month of the individual applicant's initial entry into the program.
 - F. Prior to the payment of any individual retention fee, the user may inform FDLE in writing (or other manner prescribed by FDLE) of any person with retained fingerprints who is no longer employed, licensed, certified, or otherwise associated with the user in order that such person may be removed from the AFRNP database. With respect to any person previously entered in the database for which FDLE does not receive notification of removal within a minimum of ten

days prior to the anniversary date of the entry (i.e., the billing date), the annual fee must be paid.

IV. Privacy and Security

- A. User shall use criminal history records acquired hereunder only for the purpose of screening applicants to determine their suitability for employment, licensing, permitting, granting access, registration, certification or volunteering as specified under the statute enabling User to receive criminal history record information or in judicial or administrative hearings associated with one of the enumerated purposes.
- B. User shall provide to the applicant written notice that his/her fingerprints will be used to check the criminal history records of FDLE and the FBI. An example form can be found on the FBI's website: <https://www.fbi.gov/file-repository/compact-council-noncriminal-justice-applicants-privacy-rights.pdf/view>
- C. When a determination of the applicant's suitability for the job, license, or other benefit is based solely on the FDLE or FBI criminal history, the User shall provide the applicant the opportunity to complete or challenge the accuracy of the information in the record.
- D. User shall advise the applicant that procedures for obtaining a change, correction, or updating of an FDLE or FBI criminal history are set forth in Section 943.056, F.S., and Title 28, Code of Federal Regulations (CFR), Section 16.34. The User may provide a copy of the applicant's criminal history to the applicant for their review and possible challenge. An example can be found on the FBI's website: <https://www.fbi.gov/file-repository/compact-council-agency-privacy-requirements-for-ncj-applicants.pdf/view>
- E. User shall not deny the job, license, or other benefit based on information in the FDLE or FBI criminal history until the applicant has been afforded a reasonable time to correct or complete the record or has declined to do so.
- F. User shall establish and document the process/procedure it utilizes for how/when it gives the applicant notice, what constitutes "a reasonable time" for the applicant to correct the record, and any applicant appeal process that is afforded the applicant.
- G. User shall not duplicate and/or disseminate criminal history records acquired hereunder for use outside of User agency except as authorized by state and federal law. Sharing of criminal history records with other related agencies of the state of Florida is permitted by the FBI provided that:
 - 1. The other related agency is authorized to receive criminal history record information derived from the systems of the DOJ in the manner specified at paragraph I.A of the Agreement.

2. The applicant fingerprints submitted to FDLE lists the authorizing statute for each agency receiving such (directly or as shared) information in the "reason fingerprinted" block of the submission.
 3. The requesting agency and related agency have concurrent regulatory responsibilities and have a unity of purpose with respect to the use of criminal history record information.
- H. A Florida criminal history record that is provided by FDLE to User pursuant to Sections 624.34, 626.171, 626.172, 626.201, and 648.34(4), F.S., as approved by the FBI under P.L. 92-544, is not divisible into a state component that would be a public record under Section 943.053(3), F.S. User is prohibited from disclosing Florida criminal history records provided under this agreement pursuant to 28 C.F.R. 20.33, and User cannot disseminate any portion of these criminal history records except as specified in Section IV, paragraph (2), of this agreement. If User receives a public records request for such a record or records, FDLE will assist and work directly with User in responding to the request, and in defending any claim, demand, or suit, formal or informal, challenging that response, including any appeals.
- I. User has been approved to receive criminal history record information pursuant to specific statutory authority and shall not use criminal history record information acquired pursuant to such approval for any other purpose, pursuant to 28 CFR 50.12.
- J. User shall not use or rely upon a criminal history record or information which is or is likely to be out-of-date. If criminal activity is pertinent to and considered at time of record screening (whether initial or renewal), a current criminal history record must be requested and relied upon.
- K. User shall destroy criminal history records by shredding or incineration. If the destruction is contracted to a third party company, the destruction shall be witnessed by an approved employee of the User.
- L. User shall keep criminal history records acquired hereunder in a secure file, safe, or other security device, such as locked file cabinet in an access controlled area, and shall take such further steps as are necessary to ensure that the records are accessible only to those of its employees who have been instructed in their proper use and handling and have a need to examine such records.
- M. When FDLE is auditing non-criminal justice agencies, the entirety of the FBI CJIS Security Policy (CSP) will be used to establish compliance. Appendix J of the CSP is a guideline which identifies specific areas of compliance for non-criminal justice agencies. This policy can be found at the FBI website <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>. Significant areas are listed below:

1. Local Agency Security Officer (LASO) - User shall appoint a LASO to function as the point of contact in regard to security and audit related issues. The LASO shall coordinate CSP compliance for the non-criminal justice agency. (CSP section 3.2.9)
2. Agency User Agreements – CSP requires that FDLE have an agreement with the user agency that ensures compliance with the CSP (CSP section 5.1.1.6). Acceptance of this Agreement signifies the non-criminal justice User's agreement to comply with the CSP.
3. Security and Management Control Outsourcing Standard – Outsourcing which would allow an external entity to access criminal history information obtained and/or maintained by the User is not allowed. The User shall contact FDLE to obtain approval prior to entering into a contract or granting limited criminal history information access to another entity for purposes of creating or maintaining the computer system(s) needed to accept or house criminal history information. (CSP section 5.1.1.7)
4. Secondary Dissemination – The User shall only release/allow access to criminal history information to other qualified non-criminal justice agencies, pursuant to 28 CFR 50.12. Each release/access of a criminal history record shall be documented in a dissemination log. (CSP section 5.1.3) This log shall include:
 - a) Date of Dissemination
 - b) Applicant's Name
 - c) Provider's Name (Released By)
 - d) Requestor's Name & Agency (Released To)
 - e) SID/FBI Numbers
 - f) Reason for Dissemination (Why was this information requested? For what purpose?)
 - g) Statute Requiring/Allowing Sharing of Information
 - h) How the information was disseminated (email, fax, certified mail, etc.)
5. Security Awareness Training – User shall ensure that all persons who access/process/read, or maintain criminal history information or the systems used to process/store criminal history information, complete and remain current in the appropriate FDLE CJIS Online security awareness training. FDLE Field Support staff will assist in setting up an agency within

CJIS Online access once a request is made by sending an e-mail to CJISIDT@fdle.state.fl.us. (CSP section 5.2.1.1)

6. Security Incident Response – User shall create and keep current a policy that defines the Specified User’s response procedures for security incident, relating to the system(s) used to access/store criminal history information. The procedures shall include notification of the FDLE. (CSP section 5.3)
7. Media Protection - User shall create and keep current a policy describing the procedures used to secure media (electronic or paper/hard copy) from unauthorized access/disclosure. The policy shall include, but not be limited to, destruction of electronic and paper media prior to further disposal, i.e., shredding before recycling, wiping a hard drive before disposing or returning to a vendor. (CSP section 5.8)
8. Controlled Area - The User shall designate appropriate areas for accessing, processing, and storing criminal history information. Access to such areas shall be limited to authorized personnel only, during access/processing. Electronic data stored in the controlled area shall be encrypted. (CSP section 5.9.2)
9. Formal Audits and Audit Record Retention – The User may be audited at any time and will be audited at least triennially by FDLE to ensure compliance with this agreement. The audit may either be on-site at the User’s location or via correspondence, at FDLE’s discretion. (CSP section 5.11) The User shall retain system generated audit logs, (either from the application and/or operating system level) for at least 365 days to ensure conformance to prescribed security and access requirements. The User may be selected for FBI audits. (CSP section 5.4.6)
10. Personnel Security – FDLE has determined that Florida Statutes do not enable the specifically required state and national fingerprint based records check mandated for non-criminal justice access to criminal history information. Therefore, compliance with these provisions does not require criminal history record checks of persons who access records. (CSP section 5.12)
11. Access Control/Encryption – The User shall ensure criminal history information is encrypted when transmitted or stored within a controlled area. Encryption shall meet the FIPS 140-2 standard. (CSP section 5.5.2.4)
12. Identification and Authentication – The User shall ensure access to systems used to process/store criminal history information requires individual authentication to verify that a user is authorized access to criminal history information. Passwords shall meet standards (CSP,

section 5.6.2.1). Advanced authentication shall be used for access originating from any controlled area. (refer to CSP section 5.6)

13. Configuration Management – The User shall maintain a network topological diagram depicting the system and network used to process or store criminal history information, and shall provide the diagram to FDLE/FBI during the audit process. (CSP section 5.7)
14. System and Communications Protection and Information Integrity – The User shall implement the proper safeguards to ensure the confidentiality and integrity of criminal history information (CSP section 5.10), to include, but not be limited to:
 - a) Encryption of data during transmission and at rest
 - b) Implementation of firewalls
 - c) Use of intrusion detection tools
 - d) Use of separate Virtual Local Area Network for voice over internet protocol
 - e) Adhering to proper patch management
 - f) Use of software to detect and eliminate malware, spam, and spyware

V. Provisions Incorporated

User shall be bound by applicable federal and state laws, federal regulations, and rules of FDLE dealing with criminal history information to the same extent that User would be if such provisions were fully set out herein. (Refer to Title 28, Chapter 1, Part 20, C.F.R., Chapter 943, F.S., and Chapter 11C-6, F.A.C.).

VI. Termination

Either FDLE or User may suspend the performance of services under this agreement when, in the reasonable estimation of FDLE or User, the other party has breached any material term of the agreement. Furthermore, upon FDLE becoming aware of violations of this agreement which jeopardize Florida's access to national criminal history information, FDLE shall have the option of suspending services under this agreement pending resolution of the problem. The violation of any material term of this agreement or of any substantive requirement or limitation imposed by federal or state statutes regulations, or rules referred to in this agreement shall be deemed a breach of a material term of the agreement. This agreement is also terminable upon the same grounds and

upon the occurrence or non-occurrence of such events that operate to suspend, annul, or void any other long-term contract entered into by a state agency.

This agreement supersedes any previous agreements, and may with notice to User be amended or superseded by FDLE as needed to comply with state or federal laws or regulations or administrative needs of FDLE.

IN WITNESS HEREOF, the parties hereto have caused this agreement to be executed by the proper officers and officials.

NAME OF USER AGENCY CNTY - PALM BEACH COUNTY

AGENCY HEAD ISAMI AYALA-COLLAZO **TITLE** DIRECTOR, FACILITIES DEVELOPMENT & OPERATIONS
(PLEASE PRINT) (PLEASE PRINT)

AGENCY HEAD _____
(SIGNATURE)

DATE _____

FLORIDA DEPARTMENT OF LAW ENFORCEMENT

BY _____ **TITLE** _____

DATE _____