TO THE HONORABLE MEMBERS OF THE 102ND GENERAL ASSEMBLY

Firearm Owners Identification Card Act (430 ILCS 65/4(a-26)) Fingerprint Reuse Report

January 1, 2022

The Illinois State Police (ISP) respectfully submits this report pursuant to Section 4(a-26) of the Firearm Owners Identification Card (FOID) Act (430 ILCS 65/4(a-26)). This report is due to the General Assembly by January 1, 2022. Specifically, the ISP was to research, explore, and report on the feasibility of permitting voluntarily submitted fingerprints obtained for purposes other than Firearm Owner's Identification Card enforcement that are contained in the Illinois State Police database for purposes of this Act.

Voluntarily submitted fingerprints obtained for purposes other than FOID Card enforcement can be classified into two categories. First, where an applicant previously submitted their fingerprints for a non-firearm related event (i.e., employment). Second, where an applicant previously submitted their fingerprints to the ISP for a firearm concealed carry license. The fundamental issue is whether existing law and policy recommendations approved by the FBI Director would permit the ISP to use the previously submitted fingerprints in determining whether the applicant would qualify for the automatic renewal of the FOID Card.

TO THE HONORABLE MEMBERS OF THE 102ND GENERAL ASSEMBLY

Executive Summary

Issue:

Whether or not it is lawfully permissible to reuse fingerprints for a purpose (i.e., FOID application) other than the one in which they were originally collected and submitted (non-criminal, but to include employment, licensure backgrounds, etc.).

Response:

Existing law, rules, and approved policy/procedures do not permit the subsequent use of previously submitted fingerprints for an authorized purpose other than for which the fingerprints were originally collected and submitted. Pursuant to the Memorandum of Understanding (MOU) between the ISP and the National Crime Prevention and Privacy Compact Council (Compact Council), the ISP has agreed that the use of the Interstate Identification Index (III) System for noncriminal justice purposes and the use of records obtained from the III System for such purposes will be governed by rules and regulations established by the National Crime Prevention and Privacy Compact Act of 1998 (Compact) and the Compact Council.

The ISP contacted the FBI Compact Officer, Chasity Anderson, on Friday, August 13, 2021, to seek a determination concerning whether or not the current reuse policy permits the use of fingerprints previously submitted to the ISP for a firearm concealed carry license for a related purpose, Firearm Owner's Identification (FOID) Card applicants. The ISP was informed the current reuse policy remains in effect and does not permit the reuse of prints for a purpose other than for which they were originally submitted until such time as the reuse policy is revisited. Ms. Anderson further advised as the question pertains to an FBI CJIS Advisory Policy Board (APB) policy regarding the reuse of fingerprints for a noncriminal justice purpose, research would need to be conducted and a topic paper drafted for consideration by the Compact Council and APB. On Thursday, October 14, 2021, the FBI CJIS Division Compact Team advised it is anticipated that the topic paper will be presented to the Compact Council and APB in the Fall of 2022. Subsequently, recommendations from the Council and APB concerning the reuse policy will be advanced to the FBI Director for consideration and approval.

The ISP contacted the FBI's Criminal Justice Information Law Unit on Thursday, July 29, 2021, in order to request approval of the recently passed legislation authorizing submission of fingerprints for and use of federal criminal history information for FOID purposes. The Unit acknowledged receipt of the request and advised it may take up to 150 days before we receive

a response concerning enacted legislation. On September 23, 2021, the ISP confirmed with the FBI that the request for approval as submitted on July 29, 2021, associated with the recent FOID and FCCL legislation has been assigned within the Unit for review. As of December 14, 2021, the ISP has not received a definitive response from the FBI regarding this matter.

TO THE HONORABLE MEMBERS OF THE 102ND GENERAL ASSEMBLY

Specific Legal Research and Findings

RELEVANT LAW AND POLICY

The National Crime Prevention and Privacy Compact Act of 1998[1]

- Criminal history records are shared and exchanged for criminal justice and legally authorized noncriminal (employment, licensing) justice purposes through the Interstate Identification Index (III) System.
- Establishes a Council to promulgate rules and procedures for the effective operation and use of the III System for noncriminal justice purposes.
- "Noncriminal justice purposes" means use of criminal history records for purposes authorized by Federal or State law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.
- Compact Council's mission is to enhance public safety through noncriminal justice background checks based on positive identification, while protecting individual privacy rights.
- Administration of this Compact shall not interfere with the management and control of the Director of the FBI over the FBI's collection and dissemination of criminal history records and the advisory function of the FBI's advisory policy board chartered under the Federal Advisory Committee Act (5 U.S.C. App.) for all purposes other than noncriminal justice.
- Records obtained may only be used for the official purpose for which the record was requested and requires fingerprints to be submitted **contemporaneously** with the request for criminal history information

Privacy Act of 1974[2]

- The FBI is vested with the power and authority to approve and conduct exchanges of identification records with officials of state and local governments for the purposes of employment or licensure pursuant to Public Law 92-544.
- Requires authorized governmental and non-governmental agencies/officials that conduct a national fingerprint-based criminal history record check on an applicant for a noncriminal justice (employment or licensure) purpose to ensure an applicant is provided certain notices in writing and that the results of the background check are handled in a manner that protects the applicant's privacy.

[1] 34 U.S.C. § 40311-40316; 28 CFR § 904.2 - Interpretation of the criminal history record screening requirement; 28 CFR § 901.2 - Interpretation of fingerprint submission requirements.

[2] 5 U.S.C. § 552a; 28 CFR 50.12 – Exchange of FBI Identification Records; 28 CFR 0.85(j) – General Functions

- Agencies must ensure that each applicant receives an adequate written FBI Privacy Act Statement (dated 2013 or later) when the applicant submits his/her fingerprints and associated personal information. The statement must explain the authority for collecting the applicant's fingerprints and associated information and whether the prints or associated information will be searched, shared, or retained.
- Requires agencies/officials to advise all applicants in writing the procedures for obtaining a change, correction, or update of an FBI criminal history record as set forth at 28 CFR 16.34.
- Agencies must provide the applicant the opportunity to complete or challenge the accuracy of the information in the FBI criminal history record.
- Officials must use the FBI criminal history record for authorized purposes only and cannot retain or disseminate it in violation of federal statute, regulation or executive order, or rule, procedure or standard established by the National Crime Prevention and Privacy Compact Council.

FBI Fingerprint Reuse Policy

- The FBI Advisory Policy Board recommended a change to the reuse of prints policy in 2010, and the FBI Director approved.
- In instances where fingerprints are submitted as a follow-up to an initial background check, such as a five-year reinvestigation, the previous policy required that a new set of fingerprints be taken. This changed the policy to allow the original fingerprints to be resubmitted as long as the submission is for the same purpose.
- Criminal Justice Information Systems (CJIS) Advisory Policy Board (APB) Recommendation #13: The APB moved to endorse the reuse of applicant fingerprints for the same purpose as the original fingerprint submission. NOTE: The Compact Council supported this solution; however, if the resubmission fingerprint is rejected twice, the contributor must submit a new set of fingerprints.

INPUT FROM FEDERAL GOVERNMENT REGARDING REUSE OF FINGERPRINTS

- In February 2021, the FBI Compact Officer, Chasity Anderson, advised the policy recommended by the FBI Advisory Policy Board and approved by the FBI Director regarding the reuse of prints does not authorize the reuse of applicant prints for a purpose other than for which the prints were originally submitted.
- On February 23, 2021, the Compact Council Chair, Leslie Moore, advised support for the reuse policy and stated she was not aware of any state that reuses stored prints for a purpose other than for which the prints were originally collected. She stated the reuse of applicant fingerprints for the same purpose as the original fingerprint submission is permitted but noted that in the event the resubmission fingerprint is rejected twice, the submission of a new set of fingerprints is required.
- On October 4, 2021, the FBI Compact Officer, Chasity Anderson, confirmed that until such

time as the policy recommended by the APB in 2010 is revisited, the current reuse policy will remain the policy governing the reuse of fingerprints for noncriminal justice purposes.

SPECIFIC CONCERNS REGARDING REUSE OF FINGERPRINTS

- **Subsequent reuse of previously collected and submitted prints would raise system integrity concerns.** The retransmission of previously transmitted fingerprint images stored in live scan equipment or in the ISP's ABIS database for a subsequent submission is prohibited in all of the Department's Agreements/MOU's with live scan vendors since this practice compromises the submitter's or requester's ability to affirm that a fingerprint or set of fingerprints actually belong to the person identified on the submission. Entities or vendors that collect and submit fingerprints agree to require each individual seeking to be fingerprinted to present a valid primary form of identification (i.e., driver's license or Secretary of State issued State Identification card) as another means of verifying the identity of the person being fingerprinted. Simply reusing stored prints would undermine the fingerprint collector's ability to perform this critical identity validation function. The potential negative consequences of reusing previously collected fingerprints is sufficiently outlined in the "Fingerprint Fraud Scenarios" section in the *Identity Verification Program Guide* prepared by the Compact Council. The scenarios underscore the crucial importance of identity verification by providing actual scenarios where applicants attempted and successfully circumvented the fingerprinting background process in order to obtain employment for positions of trust (teacher, health care worker).
- **Subsequent reuse of previously collected and submitted prints would raise privacy concerns.** Authorized governmental and non-governmental agencies/officials that conduct national fingerprint-based criminal history record checks on applicants for noncriminal justice (employment or licensure) purposes are required to ensure certain procedures are followed when the applicant submits his/her fingerprints. Reusing stored prints would undermine an agency's ability to fulfill these mandated privacy requirements and thereby violate Compact Council rules and regulations and the Privacy Act of 1974.