CALIFORNIA DEPARTMENT OF JUSTICE

APPLICANT AGENCY

POLICIES ▲ PRACTICES

PROCEDURES

BUREAU OF CRIMINAL INFORMATION & ANALYSIS

CALIFORNIA DEPARTMENT OF JUSTICE

BUREAU OF CRIMINAL INFORMATION & ANALYSIS

APPLICANT AGENCY

POLICIES ▲ PRACTICES

PROCEDURES

VERSION 1.0 - JANUARY 2024

Table of Contents

Introduction

Mission Statement

The California Justice Information Services (CJIS) Division of the California Department of Justice (DOJ) must provide accurate, timely, and comprehensive criminal history and analysis data to our client agencies, which include California's police and sheriff's departments, district attorneys, and local, state, and regulatory agencies.

Purpose

California's applicant agencies are local, state, and regulatory agencies statutorily authorized to conduct fingerprint-based, criminal offender record information (CORI) background checks to determine the suitability of persons applying for licensure or employment. This document provides applicant agencies with clearly defined policies, practices, and procedures for the use, retention, security, destruction, and dissemination of both state and federal CORI obtained from fingerprint-based background checks. All applicant agencies with access to CORI must understand and operate within the security requirements set by DOJ and the Federal Bureau of Investigation (FBI).

This document serves as a resource for information and provides answers to questions that may surface from using CORI. As such, the *Applicant Agency Policies, Practices & Procedures* will be updated as changes in policies, technology, and law occur.

DOJ Program Roles and Responsibilities

Applicant and Record Quality Services Branch

The Applicant and Record Quality Services Branch (ARQSB) is made up of the Applicant Services Program, the Record Quality Services Program, and the Authorization and Certification Program. These programs assist applicant agencies with disseminating CORI, ensuring the accuracy of the CORI disseminated, and approving requests for access to CORI.

Applicant Services Program

The Applicant Services Program (ASP) is responsible for the dissemination of state and federal CORI for fingerprint-based background checks to authorized agencies or individuals.

The ASP also provides information related to substantiated reports of child abuse or severe neglect from the Child Abuse Central Index (CACI) to law enforcement agencies, county welfare departments, tribal agencies, or county probation departments that conduct child abuse investigations. The information is provided to designated social welfare agencies to help screen applicants for licensing or employment in childcare facilities and foster homes. It is also used to aid in investigations for other possible child placements and adoptions.

Record Quality Services Program

The Record Quality Services Program (RQSP) is responsible for ensuring the accuracy and quality of the CORI disseminated to applicant agencies, organizations, and individuals for criminal and noncriminal justice purposes. In accordance with California Penal Code sections 11120 through 11127, the RQSP processes applicant requests for copies of their own CORI and responds to CORI challenges, known as Claims of Alleged Inaccuracy or Incompleteness. The RQSP also locates, researches, reconciles, and resolves missing or ambiguous entries on criminal history records.

Authorization and Certification Program

The Authorization and Certification Program (ACP) is the main source of support for all applicant agencies. The Noncriminal Justice Access Oversight Section (NCJAOS) focuses on approving agency requests for access to state CORI, coordinating the approval of access to federal CORI, and confirming designated Custodians of Records. The NCJAOS also provides technical support with the Applicant Agency Justice Connection (AAJC), the web-based portal used to view and manage background check results.

The Training and Administrative Support Section (TASS) was established in 2021 and is devoted to improving awareness of the roles and responsibilities associated with accessing CORI. The TASS actively monitors the changes in state and federal statutory authorities and coordinates and facilitates applicant agency audits. This section also produces and maintains all the educational and training resources and video tutorials available for applicant agencies. Upon request, the TASS provides one-on-one training support for agencies through video conferencing.

The FBI's Roles and Responsibilities

The FBI's CJIS Audit Unit

The FBI Criminal Justice Information Services (CJIS) Audit Unit (CAU) conducts audits of each CJIS System Agency (CSA) every three years to verify compliance with applicable statutes, regulations, and policies. For the State of California, DOJ is the CSA. To assess each state's overall compliance, the CAU selects several criminal justice agencies and noncriminal justice agencies throughout the state to participate in the audit of the CSA.

The CAU assists applicant agencies with compliance, evaluating policies, procedures, and practices and their effectiveness. They help with improving and ensuring the integrity of system data as well as protecting and safeguarding CORI.

The Office of General Counsel's Criminal Justice Information Law Unit

The Criminal Justice Information Law Unit (CJILU) provides legal advice and support to the FBI CJIS Division. Its contributions concern the sharing of federal CORI among different programs including, but not limited to, the National Crime Information Center, the Next Generation Identification, and the National Instant Criminal Background Check System.

For applicant agencies, CJILU plays a role in authorizing access to federal CORI for fingerprint-based background checks. Statutory authorities must be submitted to CJILU for review and meet specific criteria before access to federal CORI can be granted. If approved, an agency's statutory authority will be recorded by CJILU for future auditing purposes.

Authority to Conduct Fingerprint-Based Background Checks

Statutory Authority Overview

Statutory authority refers to the authority delegated to a government or local agency enacted by a law passed by Congress or a state legislature. An agency must possess the statutory authority to obtain access to state CORI.

Access to federal CORI may also be permitted, however, all requests for federal CORI must be reviewed and approved by the FBI's CJILU before this information can be made available to a requesting agency.

Applicant agencies are responsible for notifying DOJ if and when their authorizing statutory authority changes. Coordination with the NCJAOS allows for proper review of the changes proposed, so authorization can be maintained.

State Authority

Various California laws authorize governmental and private agencies to conduct fingerprint-based background checks to help determine the suitability of a person applying for adoption, certification, employment, licensing, or permitting purposes. The following list identifies statutory authorities used to access state CORI for the most common agency types:

- **School Contractor Employers:** California Education Code sections 33192, 33195.3, and 45125.1
- **Youth Organization, AmeriCorps & Human Resource Agencies:** California Penal Code section 11105.3
- **Contract/Proprietary Security Organizations:** California Penal Code section 11105.4
- **City, County, Special Districts or Joint Powers Authorities:** California Penal Code section 11105(b)(11)
- **Federally Recognized Tribes/Designated Agencies:** California Penal Code section 11105.08
- **Public/Private Schools:** California Education Code sections 45125 and 44237
- **Government Agencies, Federal Agencies, Financial Institutions, Public Utilities**: California Penal Code section 11105

If an agency does not fall within these common agency types and needs assistance determining their statutory authority, please submit an inquiry to the NCJAOS at ORIQuestions@doj.ca.gov for further assistance.

Federal Authority, Pub. L. 92-544

Access to federal CORI is permitted when a state statute or local ordinance:

- Requires or authorizes the fingerprinting of applicants
- Expressly or by implication authorizes the use of FBI records for the screening of applicants
- Identifies a specific category of applicants, avoiding over-breadth
- Is not against public policy
- Does not authorize the receipt of federal CORI by a private entity
- Is approved by the FBI CJILU

Drafted Legislation

State agencies seeking to establish authority for access to federal CORI are encouraged to submit their proposed legislation to DOJ at ORIQuestions@doj.ca.gov. Once received, DOJ will verify whether it meets the above requirements. With time permitting, DOJ will forward the proposed legislation to the FBI's CJILU for their review. It may take up to 90 days to complete the review. Agencies seeking to modify existing authorizing statutes are encouraged to undergo the same review process to avoid adversely affecting the status of their established authorities.

Enacted Legislation

State agencies that enact legislation concerning access to federal CORI must submit the enacted legislation to DOJ at ORIQuestions@doj.ca.gov. Once received, DOJ will forward it to the FBI's CJILU for

their review. It may take up to 180 days to complete the review. If the enacted legislation is denied by the FBI's CJILU — often as a result of not obtaining preliminary approval through the proposed legislation review process — DOJ will work with the affected agency to make appropriate changes to the legislation.

For more information concerning these review processes, please contact the NCJAOS at ORIQuestions@doj.ca.gov for further assistance.

The Authorization Process

New Agency Application

Before any applicants for an agency can fingerprint for a background check, an agency must first apply to DOJ to become an authorized applicant agency. Approval is based on a review of their cited statutory authority. The statutory authority will specify the level of service (CA only or CA and FBI) an agency will receive.

To request authorization to receive CORI, agencies must first submit an *Application for CORI Authorization* (BCIA 9001), obtained on the DOJ website at: https://oag.ca.gov/fingerprints/agencies. The application will require a written description of the services the agency provides, supporting the authority to conduct fingerprint-based background checks. An application will be denied if there is no statutory authority.

Additionally, a Custodian of Records (COR) representative must be designated. The COR serves as the primary contact for DOJ, actively representing their agency in all matters in regard to accessing, securing, storing, disseminating, and destroying the CORI furnished to their agency. The designated COR will need to complete the *Custodian of Records Application for Confirmation* (BCIA 8374-9007). Agencies that wish to become authorized may review additional information and obtain an application on the DOJ website at: https://oag.ca.gov/fingerprints/agencies.

Once preliminarily authorized, the agency will be instructed by the NCJAOS to complete any supplemental documents and tasks required. Agencies failing to submit the applicable documents in seven calendar days or by any other provided deadline will be denied.

Custodian of Records Confirmation

Every agency that receives CORI from DOJ must designate at least one COR for their agency. Pursuant to California Penal Code section 11102.2(b), DOJ maintains a confirmation process for individuals designated by applicant agencies to serve as a COR. An applicant must be fingerprinted under the applicant type, "Custdn Records 11102.2 PC" and confirmed by DOJ to serve as an agency COR. If multiple CORs are desired, an agency may add as many representatives as they believe necessary.

Once instructed to complete the confirmation process, the *Request for Live Scan Service (Custodian of Records)* (BCIA 8016 CUS) will be provided to the designated COR that is listed on the *Custodian of Records Application for Confirmation* (BCIA 8374-9007). The form should be completed and taken to a local Live Scan site for the designated COR to be fingerprinted. Live Scan locations can be found on the DOJ website at: https://oag.ca.gov/fingerprints/locations. All fees for fingerprinting performing a state and federal background check, and COR confirmation will be collected at the Live Scan site.

Out-of-state COR applicants must submit an original FD-258 fingerprint hard card, as Live Scan is not available outside of California. As part of the confirmation process DOJ will mail the COR applicant two prefilled FD-258 fingerprint cards with instructions. Fingerprinting using the FD-258 is usually available from a local police or sheriff's department, or from private vendors that provide fingerprinting services.

Once completed, the designated COR will need to send two completed fingerprint cards back to the NCJAOS section at the provided address, with a check for $79.00 made payable to the Department of Justice.

Regardless of how the fingerprint-based background check is completed, manually or electronically, DOJ will retain the fingerprints for subsequent arrest and disposition notifications under California Penal Code section 11105.2.

Criminal justice agency personnel who have undergone a state and federal fingerprint-based background check are exempt from the fingerprinting process. This will be verified by a DOJ employee before confirming the applicant.

Once the applicant's fingerprints are processed, the confirmation status will either be approved or denied. Confirmation will be denied or revoked in accordance with California Penal Code section 11102.2. A COR confirmation, denial, or revocation letter will initially be mailed by DOJ to the designated agency and COR identified on the BCIA 8374-9007.

Requesting a Billing Number

Agencies will be provided with billing procedures and the *Billing Account Application* (CJIS 9000), as part of the authorization application obtained on the DOJ website at: https://oag.ca.gov/fingerprints/agencies. Applicant agencies are not required to utilize this service if their applicants will pay the Live Scan fees at the Live Scan site. Applicant agencies who wish to be billed for fingerprints submitted through Live Scan must complete the CJIS 9000.

The submission of this document will result in the assignment of a unique billing number that the Live Scan operator must enter during Live Scan transactions. Once the authorization process is complete, the billing number will be provided.

CORI Security Policy Form

The *CORI Security Requirements* (BCIA 9007) is provided during the COR confirmation process and outlines the importance of maintaining the security of CORI. The COR is responsible for ensuring the agency's policies and procedures for accessing, securing, storing, disseminating, and destroying CORI comply with the FBI *CJIS Security Policy.*

The Agency Head is responsible for overseeing the administration of CORI and the COR(s) confirmed for their agency. Each COR and their Agency Head are required to acknowledge, sign, and return this form.

Employee Statement Form

Any personnel (other than an agency COR) accessing or viewing CORI, must sign the *Employee Statement* (BCIA 9006) to acknowledge understanding of the laws prohibiting the misuse of CORI. The misuse of CORI may violate constitutional rights of privacy and may result in the suspension or loss of employment and prosecution for state and federal crimes. The signed form must be kept on file by the COR and not returned to DOJ, and may be obtained as part of the authorization application on the DOJ website at: https://oag.ca.gov/fingerprints/agencies

Authorized Recipient User Agreement

Before conducting background checks, all applicant agencies must sign the *Authorized Recipient User Agreement* (BCIA 9005) obtained as part of the authorization application on the DOJ website at: https://oag.ca.gov/fingerprints/agencies. DOJ and the authorized applicant agency must comply with all applicable state and federal laws, rules, and regulations relating to the receipt, use, and dissemination of CORI derived from the systems of DOJ and the FBI.

This form is entered into by DOJ and the Authorized Recipient (otherwise known as the authorized applicant agency) to set forth the terms and conditions under which CORI will be provided to the authorized applicant agency as an employer, licensing agency, or other agency authorized by state and/or federal statute. This form must be acknowledged and signed by the Agency Head. Additionally, a copy of the form must be kept on file by the authorized applicant agency.

Contract for California Subsequent Arrest and Disposition Notifications

Applicant agencies authorized by state or federal law may participate in the California Subsequent Notification Service to assist in fulfilling employment, licensing, or certification responsibilities under California Penal Code section 11105.2. This optional service allows agencies to receive updated criminal arrest and disposition notifications for applicants who fingerprinted for their agency. There is no fee to participate in the California Subsequent Arrest and Disposition Notification Service.

The *Contract for California Subsequent Arrest and Disposition Notifications* (BCIA 8049), provided as part of the authorization application on the DOJ website at: https://oag.ca.gov/fingerprints/agencies, is entered into by DOJ and the applicant agency to set forth the terms and conditions under which the subscribing agency and COR(s) must comply to utilize the service. This form must be signed by the Agency Head and kept on file by the authorized applicant agency.

Background Check Requirement Verification Form

Agencies applying for authorization as a School Contractor will be provided the *Background Check Requirement Verification* form as part of the school contractor authorization application on the DOJ website at: https://oag.ca.gov/fingerprints/agencies. The Background Check Requirement Verification form must be completed by the contracting school district or school the contractor will be serving. The form verifies that the school district or school requires a background check before allowing the contractor to begin working on school grounds.

Originating Agency Identifier and Mail Code Assignment

The final step of the authorization process is receiving an assigned Originating Agency Identifier (ORI) and mail code. These assignments are unique to each agency and are used for identification and access purposes. An agency's ORI and mail code will be associated with every fingerprint submission.

An ORI comes in two forms. The first is the most common form and is assigned to noncriminal justice agencies. This ORI is a five-character identifier beginning with the letter "A" and is followed by four numbers.

The FBI assigns a nine-character identifier to law enforcement agencies authorized to access FBI, CJIS Division Systems. For these agencies, DOJ will designate the same nine-character ORI for fingerprinting for *noncriminal* justice purposes.

For California, all law enforcement ORIs assigned by the FBI begin with the letters "CA." All ORIs assigned by the FBI for Superior Courts of California are assigned a six-character identifier, beginning with the letter "J."

A mail code is a five-digit identifier used for accessing the results of fingerprint-based background checks within the AAJC Portal. Agencies are assigned a single mail code where all fingerprint-based background check results will be delivered to the agency inside the AAJC Portal. If needed, an agency may request additional mail codes to separate fingerprint-based background check results by applicant type (e.g., employee, licensee, volunteer). However, due to system limitations, additional mail codes cannot be provided to separate fingerprint-based background check results for a single applicant type. If an agency

requires the separation of fingerprint-based background check results for a single applicant type, the agency may be assigned multiple ORIs. Each ORI will be assigned its own mail code.

Welcome Email

Once the authorization process is complete, the applicant agency COR will receive an email approving their Application for CORI Authorization. The email will include the agency's ORI(s), mail code(s), billing number (if requested), authorized applicant type(s), and further information for accessing the agency's background check results and CJIS Security Awareness Training.

Getting Started

The AAJC Portal

The AAJC Portal provides authorized applicant agencies with a secure web-enabled portal to assist in managing their fingerprint-based background check results. The tools within the AAJC Portal allow authorized users to submit agency change requests, check the status of background checks, retrieve background check responses, and access information related to the fingerprint-based background check process.

Before initially accessing the AAJC Portal, every authorized user will need to register their account. Each user will receive an email from donotreply@doj.ca.gov. The email will include their User ID and temporary password, with the hyperlink to the registration page. Users will also receive an onboarding email from aajcsupport@doj.ca.gov providing additional information including the AAJC External User Guide and MFA Guide to reference for completing the registration process.

Multi-Factor Authentication

To gain access to the AAJC Portal, all authorized users must register their accounts and complete Multi-Factor Authentication (MFA) enrollment through PingID.

New users should follow the MFA Guide provided in the onboarding email to assist in registering new and existing accounts to the MFA PingID application. Both your mobile device and email can be set up for your account but only one can be selected as the primary authentication type when logging into the account. This will enable MFA to ensure secure AAJC Portal access. The user will be prompted for their username, password, and a secondary authentication token with each new login. DOJ requires MFA to validate the identity of every AAJC user and to ensure the security of the CORI results in the AAJC Portal.

Security Awareness Training

Basic security awareness training is required for all personnel who have access to or view CORI. It must be completed within six months of initial assignment and every year thereafter. DOJ utilizes an online testing system called CJIS Online to help facilitate and track this training requirement. The training is self-paced, is not timed, and may be accessed through www.cjisonline.com.

Upon first logging in, the user will be asked to change their password and verify their contact information. The security awareness training can be found under the Certifications tab. Once completed, there is no need to send the certificate to DOJ. Each COR's certification date will be reflected under the Resources Tab in the AAJC Portal within 24-48 hours.

Each applicant agency COR will also be granted administrative account privileges within CJIS Online, reflecting as an "Agency Admin" on their CJIS Online profile. Administrative account privileges will allow CORs to assign security awareness training to their agency's administrative personnel and manage their training records for compliance purposes. It is the responsibility of the applicant agency COR(s) to grant

access to CJIS Online and track the Level 2 security awareness training required for their administrative personnel.

Criminal justice agencies may demonstrate compliance through nexTEST or CJIS Online. However, it is still imperative that CORs of criminal justice agencies, who have completed a nexTEST Level 2 or greater certification, submit a copy of their current certificate to DOJ. Criminal justice agency CORs will still be subject to recertification every two years based upon their nexTEST certification date.

For additional information about the topics covered in each level of security awareness training, please reference the FBI *CJIS Security Policy.*

Conducting Fingerprint-Based Background Checks

Understanding the Request for Live Scan Service

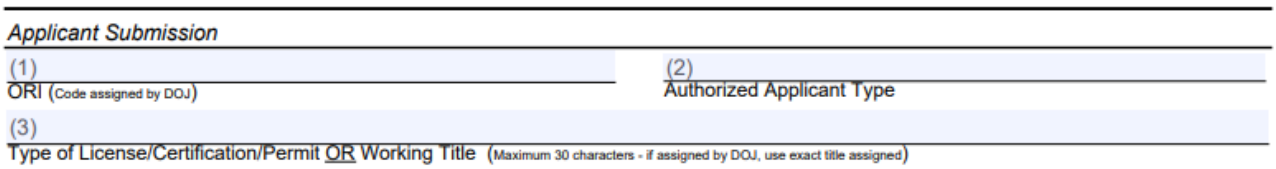
The *Request for Live Scan Service* (BCIA 8016) is the standard form used by all applicant agencies to capture applicant data associated with a Live Scan fingerprint transaction. Live Scan is the primary system used for the electronic submission of applicant fingerprints for fingerprint-based background checks and responses. Live Scan technology replaces the manual rolling process that requires ink and an original FD-258 fingerprint hard card to record a person's fingerprint patterns. Live Scan allows fingerprints to be digitally scanned through an electronic process. Fingerprint image data is electronically transferred, in combination with personal descriptor information, to DOJ. This transfer of information takes place in seconds, compared to the days required to send fingerprint hard cards through the U.S. mail.

For applicants residing in California, Live Scan is the only approved method for submitting fingerprints for a criminal history background check. No other forms will be accepted.

Completing the BCIA 8016 accurately is essential for any agency to receive its results quickly. For questions about completing the BCIA 8016, please contact ORIQuestions@doj.ca.gov. To obtain a fillable version of the BCIA 8016, please visit the DOJ website at: https://oag.ca.gov/fingerprints/forms or navigate to the Resources widget on the AAJC home page to download the form. For a list of sites offering Live Scan fingerprinting services to the public, please visit the DOJ website at: https://oag.ca.gov/fingerprints/locations.

Applicant Submission

The Applicant Submission section of the BCIA 8016 includes information specific to the Live Scan request.



(1) **ORI (Originating Agency Identifier):** Enter the unique number assigned by DOJ for the agency. This number is used to identify each applicant agency and must be assigned before submitting fingerprints. **Please note:** DOJ ORI utilized during the COR confirmation process should only be used by DOJ programs authorized to use it. If a COR needs to confirm their agency's ORI number, please contact ORIQuestions@doj.ca.gov.

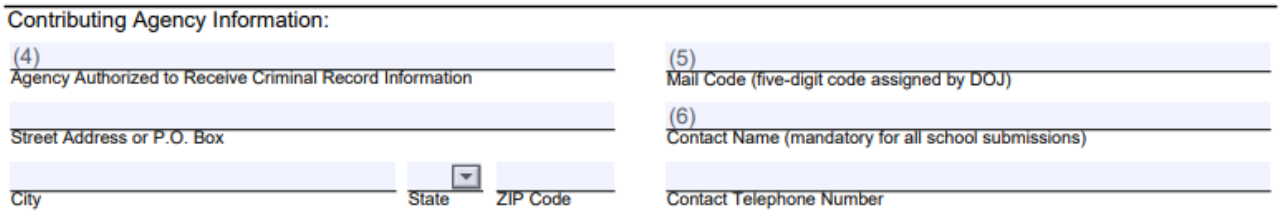
(2) **Authorized Applicant Type:** Each applicant agency has assigned applicant type(s) they are permitted to use. The applicant type determines the dissemination criteria used in preparing the

response. Since agencies may have more than one authorized application type, it is important to enter the correct one. Examples include: Employee 11105.3 PC; City or County Employee; Classified School Employee; and Non-Sworn LEA Personnel.

(3) **Type of License/Certification/Permit OR Working Title:** This section may be referred to as the "reason-fingerprinted field." Enter the specific statute or resolution authorizing your agency to conduct fingerprint background checks. If an FBI level of service is being requested, please use the **exact** information assigned.

Contributing Agency Information

The Contributing Agency Information section of the BCIA 8016 includes information specific to the applicant agency.



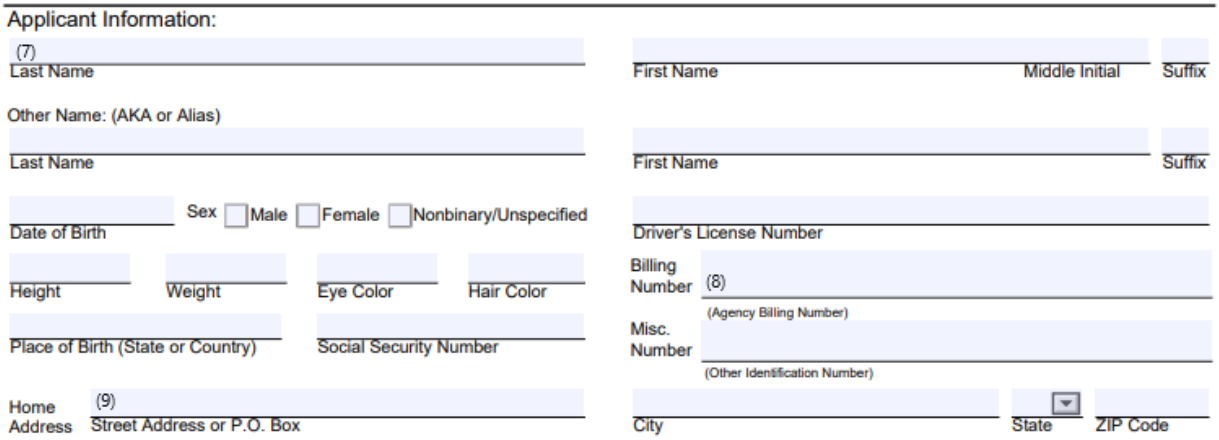
(4) **Contributing Agency Information:** Enter the agency's name and address. Please ensure the mailing address listed matches DOJ's records.

(5) **Mail Code:** Enter the unique number assigned by DOJ for accessing the results of fingerprint-based background checks. An incorrect code may cause the response to be sent to the wrong agency. If no mail code is provided, the response will be mailed.

(6) **Contact Information:** Enter the name and phone number of the COR for the applicant agency. This is a mandatory field for applicants requiring a CACI check.

Applicant Information

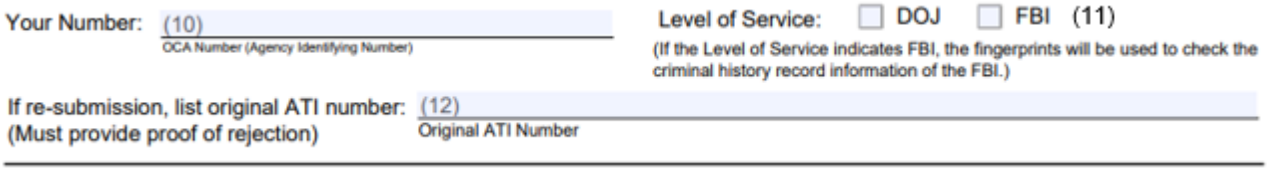
The Applicant Information section of the BCIA 8016 includes information specific to the applicant requesting the Live Scan.



(7) **Applicant Information:** Enter the name and personal identifying information of the applicant requesting a Live Scan. The applicant must provide a valid driver's license number.

(8) **Billing Number:** Enter the unique billing number assigned by DOJ. If the agency does not have a billing number, the applicant should be prepared to pay all fees associated with the transaction.

(9) **Home Address:** Enter the home address of the applicant. This is mandatory for: (1) applicants requiring a CACI check, and (2) applicants subject to any statute mandating notification to the applicant as well as the agency.



(10) **Your Number/OCA (Originating Case Agency) Number:** Some agencies assign a unique number to each applicant. This field is provided for the agency's convenience to help match the response to the correct applicant, which may be helpful if an agency has applicants with similar names. This section is optional and may be left blank. Only 20 characters are allowed.

(11) **Level of Service:** Check the appropriate level(s) of service. Please note that an agency must be authorized by statute to receive the information requested. In addition, the applicant type will dictate the level(s) of service permitted. In those situations where the FBI level of service is permitted, the COR **must** check the FBI box or the agency will not receive a response from the FBI.

(12) **Original ATI Number: ONLY USED FOR RE-SUBMISSIONS.** If the applicant's fingerprints were previously rejected and are now being resubmitted, the ATI number from the original BCIA 8016 must be included. Failure to do so may result in another processing fee for the transaction. The ATI number can be found on the last line of the BCIA 8016. It is entered by the Live Scan operator when the transaction is completed.

Applicant Notification

An agency must inform all applicants of their privacy rights.

With any form used to collect personal information from applicants, every applicant agency is mandated to provide a notice informing an individual of the following:

- Whether the submission of such personal information is mandatory or voluntary
- The consequences, if any, of not providing all or any part of the requested personal information
- The principal purpose or purposes within the agency for which the personal information is to be used

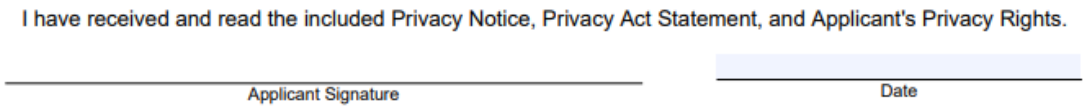
These requirements can be met by the DOJ Privacy Notice that is part of the BCIA 8016 form.

Also, the FBI is authorized to acquire, preserve, and exchange fingerprints and associated information. The FBI's Privacy Act Statement, which is also contained in the BCIA 8016 form, informs applicants of this authority and advises that the submission of fingerprints and associated information is voluntary. It also states that failure to submit information may affect the completion or approval of an application. This notice further advises applicants on how their information will be used, retained, and shared.

An applicant who is the subject of a federal fingerprint-based background check for a noncriminal justice purpose has certain rights under federal law. These rights, which include the opportunity to complete or challenge the accuracy of their criminal history record and the right to expect that officials receiving the

results of the criminal history record check will use it only for authorized purposes, are delineated in the Noncriminal Justice Applicant's Privacy Rights, which is also part of the BCIA 8016 form.

These state and federal privacy notices are included on the BCIA 8016 for an agency's convenience. All applicants must acknowledge they have been provided adequate written notice before a Live Scan or hard card fingerprinting, by certifying the acknowledgment with their signature on the BCIA 8016.

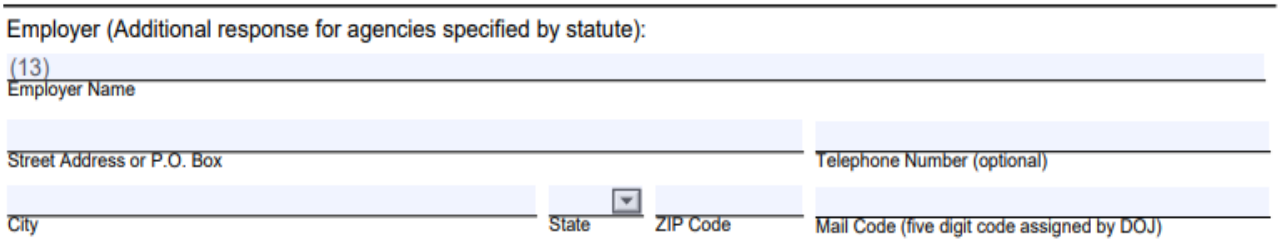

I have received and read the included Privacy Notice, Privacy Act Statement, and Applicant's Privacy Rights.

Applicant Signature

Date

Employer Section

The Employer Section is required for dual responses permissible by statute and does not apply to most agencies. DOJ will compile and electronically disseminate a primary response to the contributing agency information at the top of the form, and electronically disseminate a dual response to the secondary certified agency entered below.


Employer (Additional response for agencies specified by statute):

(13)
Employer Name

Street Address or P.O. Box

Telephone Number (optional)

City

State

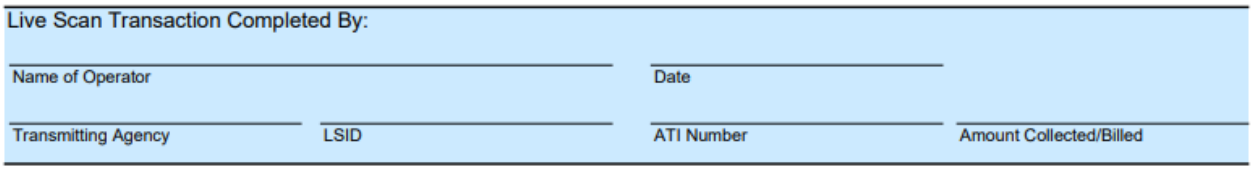
ZIP Code

Mail Code (five digit code assigned by DOJ)

(13) **Employer:** If applicable, enter the name and address of the secondary certified agency. It is important to enter the mail code assigned to the secondary certified agency for accessing the results of fingerprint-based background checks. An incorrect code may cause the response to be sent to the wrong agency. Agencies to whom this section applies include the Emergency Medical Services Authority or a facility licensed by the Department of Social Services.

Live Scan Transaction Information

The Live Scan Transaction Information Section of the BCIA 8016 is used to capture all the information related to the Live Scan transaction and the Live Scan site. The Live Scan operator will complete this section.


Live Scan Transaction Completed By:

Name of Operator

Date

Transmitting Agency

LSID

ATI Number

Amount Collected/Billed

- **Name of the Operator:** The name of the Live Scan operator submitting the Live Scan transaction.
- **Date:** The date the Live Scan transaction took place.
- **Transmitting Agency:** The Live Scan site, police department, or the county sheriff's office submitting the Live Scan to DOJ.
- **LSID:** The Live Scan ID number for the Live Scan machine, similar to a serial number.

- **Applicant Transaction Identifier (ATI) Number:** A 10-digit number, generated by the Live Scan device, used to identify the specific transaction. The sequence of an ATI number is one alpha character, three numbers, three alpha characters, and three numbers.
- **Amount Collected/Billed:** This is the amount charged based on the fee schedule for the Live Scan transaction and the fingerprint-rolling fee.

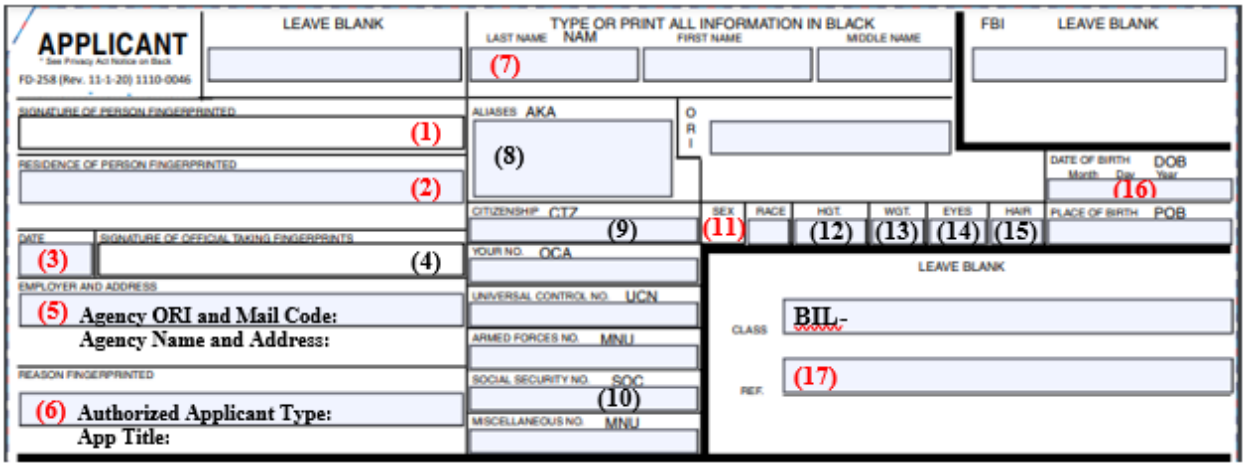
Fingerprint Hard Cards

Live Scans cannot be transmitted outside of California. If the applicant resides outside California they must be fingerprinted on an original FD-258 fingerprint hard card. The FD-258 must be an original form on card stock to be processed by DOJ. A downloaded version of the FD-258 will not be accepted. Completing the FD-258 accurately is essential for an agency to receive its results quickly. See instructions on the back of the FD-258 on how to obtain classifiable fingerprints. To download the instructions below, navigate to the Resources widget on the AAJC home page.

An agency must inform all applicants of their privacy rights including when a fingerprint hard card is used. Please refer to the *Applicant Notification* section for more information.

Completing the Fingerprint Hard Card

Before having the applicant's fingerprints taken, the applicant agency should complete the fingerprint card according to the numbered instructions. The applicant can complete the remaining information before visiting the fingerprint location. All fields **bolded** in **red** are <u>mandatory</u> and must be filled out on the fingerprint card completely. Please print legibly, preferably using black ink.



(1) **Signature of the Person Fingerprinted (Mandatory):** The applicant must sign this section when their fingerprints are applied to the card. The signature should be their full legal name, and it must be signed in the presence of the agent taking their fingerprints. Do **<u>not</u>** have the applicant sign the fingerprint hard card until told to do so at the fingerprinting location.

(2) **Residence of the Person Fingerprinted (Mandatory):** Enter the residence of the applicant being fingerprinted.

(3) **Date (Mandatory)**: Enter the date the fingerprints were taken.

(4) **Signature of Official Taking Fingerprints:** Signed by the agent or fingerprint roller.

(5) **Employer and Address (Mandatory):** Enter the unique ORI and mail code for the applicant agency, in addition to the complete name and address for the agency. **Please note:** For transactions with a secondary certified agency, the complete name and address should be entered on the back of the fingerprint card.

(6) **Reason Fingerprinted (Mandatory):** Enter the authorized applicant type and applicant title. The applicant type must be one for which the submitting agency is authorized. If a COR is unsure of what applicant types are authorized for their agency, please e-mail ORIQuestions@doj.ca.gov for assistance. The applicant title is the specific job title, license, certificate, or permit being requested. If FBI level of service is being requested, please use the **exact** type of license assigned.

(7) **Name (NAM) (Mandatory):** Enter the applicant's full name (Last, First, Middle).

(8) **Aliases (AKA):** Enter any aliases (including maiden name) that the applicant is known by.

(9) **Your Number (OCA):** Some agencies assign a unique number to each applicant. This field is provided for the agency's convenience to help match the response to the correct applicant, which may be helpful if an agency has applicants with similar names. This section is optional and may be left blank. Only 20 characters are allowed.

(10) **Social Security Number (SOC):** Enter the applicant's social security number. If the applicant does not have an assigned social security number, leave blank.

(11) **Sex (Mandatory):** Enter the sex of the applicant.

SEX	CODE
Female	F
Male	M
Other	X

(12) **Height:** Enter the height of the applicant in feet and inches (e.g., 5'5").

(13) **Weight:** Enter the weight of the applicant in pounds (e.g., 140).

(14) **Eyes:** Enter the eye color of the applicant.

EYE COLOR	CODE	EYE COLOR	CODE	EYE COLOR	CODE
Black	BLK	Blue	BLU	Brown	BRO
Green	GRN	Hazel	HAZ	Grey	GRY

(15) **Hair:** Enter the hair color of the applicant.

HAIR COLOR	CODE	HAIR COLOR	CODE	HAIR COLOR	CODE	HAIR COLOR	CODE

Bald	BAL	Black	BLK	Blonde	BLN	Brown	BRO
Grey	GRY	Red	RED	Sandy	SDY	White	WHI

(16) **Date of Birth (DOB) (Mandatory):** Enter the month, day, and year of birth for the applicant.

(17) **Class: ONLY MANDATORY WHEN USED FOR RE-SUBMISSIONS**. If the fingerprints are reprints from a previously rejected transaction, enter the ATI number, provided on the "App Reject" or "FBI Reject" response sent to the agency.

(18) **Ref:** If the agency chooses to use their billing number for fees associated with the fingerprint submission, enter it here.

Submitting the Fingerprint Hard Card to DOJ

Once the fingerprint hard card has been completed by the applicant, the applicant agency must review the card and ensure that each area of the card is filled out completely and accurately. Next, the agency should submit the card under its unique ORI number to DOJ. The applicant should not submit the fingerprint hard card to DOJ directly.

Hard cards must be submitted with a billing transmittal form and the agency's method to remit payment (e.g., check, money order, billing number for their DOJ account). If an agency chooses to use its billing number and would like to be billed for the transaction, please use the *Applicant Transmittal Form* – Billing (JUS 204). For payment by check or money order, the agency would use the *Applicant Transmittal Form – Prepaid (Cash)* (JUS 203) and include the payment with the card and transmittal form. Both forms can be found on the DOJ website at: https://oag.ca.gov/fingerprints/forms.

The processing fees will vary based on agency type, applicant type, and level of service requested. Please refer to the *Applicant Fingerprinting Processing Fees* document and choose from the appropriate purpose of fingerprint submission and the appropriate level(s) of service to determine the corresponding fees. This document is on the DOJ website at: https://oag.ca.gov/fingerprints/forms.

Once all components are completed, the applicant agency will then mail the card, billing transmittal form, and any fees to:

California Department of Justice
Pre-Scan Unit, K-111
P.O. Box 903417
Sacramento, CA 94203-4170

Unable to Submit Fingerprints

Pursuant to California Penal Code section 11105.7, if the applicant is unable to submit legible fingerprints due to disability, illness, accident, or other circumstances beyond their control, they can complete the *Request for Department of Justice Name Check* (BCIA 9010). However, if the applicant can provide one or more fingerprint images, regardless of quality, they must do so. This section does not apply to persons who are unable to provide fingerprints because of actions they have taken to avoid submitting their fingerprints.

The BCIA 9010 should be submitted to a law enforcement agency for verification, along with photo identification. The law enforcement official will verify that the individual cannot be fingerprinted. Once verified and signed by an official, please refer to the *Applicant Fingerprinting Processing Fees* document and choose from the appropriate purpose of fingerprint submission and the appropriate level(s) of

service to determine the corresponding fees. This document can be found on the DOJ website at: https://oag.ca.gov/fingerprints/forms. The form and appropriate processing fees should be mailed to:

California Department of Justice
Bureau of Criminal Information & Analysis
Applicant Services Program
P.O. Box 903417
Sacramento, CA 94203-4170

Once the request is received, it will be reviewed. If approved, DOJ will use the available personal identifying data that the department deems appropriate and conduct a search to determine if the applicant has a criminal history. If the request is denied, the applicant agency will be notified and the applicant will need to be fingerprinted.

Fee Schedule

DOJ applicant processing fees for state and federal-level background checks are dependent on the type of agency, applicant type (employment, licensing, or certification), and level of service (CA only or CA and FBI). The Applicant Fingerprint Processing Fees reference document may be found at https://oag.ca.gov/fingerprints/forms.

Once Fingerprints are Submitted

Once a Live Scan transaction or fingerprint hard card submission is received by DOJ, the fingerprint images are used to automatically search against all other fingerprint images in the fingerprint database. If no fingerprint images match the applicant's fingerprints, the transaction is generally processed electronically within 48 to 72 hours. If not, the applicant agency is automatically sent a delayed notice response. The next response the applicant agency will receive is the completed response.

Delays

Delays may be caused for a variety of reasons. An applicant agency must diligently monitor and work accordingly to mitigate delays to receive a background check response for their applicants. If there is an error with the transaction or a delay notice response has not been received, re-fingerprinting the applicant or working with DOJ may be required to resolve the matter. In such a situation, applicant agencies may contact AppAgencyQuestions@doj.ca.gov with the applicant's name, ATI number, and the date the applicant fingerprinted.

The Applicant Background Check Status tool should be used to check the status of an applicant's fingerprint transaction. The only information required to perform a search is the ATI Number and applicant's Date of Birth. To check the status of an applicant, please visit the DOJ website at: https://applicantstatus.doj.ca.gov.

Preparing Responses for State-Level of Service

If an applicant's fingerprint images match fingerprint images in the database, the associated criminal history must be reviewed by a DOJ employee. The time required for this manual process can vary widely.

A DOJ employee first reviews the criminal history to determine if there is a corresponding disposition for each arrest. If there is, DOJ employee applies the dissemination criteria statutorily mandated for the applicant type. The response is sent electronically to the AAJC Portal, as long as a mail code was provided on the BCIA 8016; otherwise, the response will be sent through U.S. Mail.

If there is a missing disposition for an arrest, DOJ is mandated by statute and case law to perform a "genuine effort" to determine the disposition of each arrest that does not have a corresponding disposition. To fulfill this effort, DOJ must contact the booking police or sheriff's department to determine which agency apprehended the individual, and then contact the arresting agency to determine the result of the arrest. The research is labor-intensive for these contacted agencies, and they may limit the number of information requests DOJ can submit each day, which can add to the delay of a response sent to the agency. Once the effort is fulfilled, a DOJ employee reviews any information obtained, updates the Record of Arrest and Prosecution (RAP) sheet, and prepares the background check and response according to the statutory dissemination criteria.

Preparing Responses for Federal-Level of Service

If federal-level of service is requested, the fingerprint images are forwarded to the FBI to perform a fingerprint-based search of records in the national criminal history database. If the applicant's fingerprint images match fingerprint images in the national criminal history database, the FBI sends DOJ a cumulative RAP sheet that contains criminal history information from any states or federal agencies that have reported the information to the FBI.

A DOJ employee then reviews the criminal history record information from the FBI to determine if there is a corresponding disposition for each arrest. If there is, a DOJ employee applies the dissemination criteria statutorily mandated for the applicant type. The background check response is then prepared and sent electronically to the AAJC Portal. For nongovernmental agencies, please reference the *Federal-Level of Service* subsection under section *Dissemination of CORI* for more information about why federal CORI is not disseminated.

If there is not a matching disposition for every out-of-state or federal arrest, DOJ is again mandated by statute to perform the "genuine effort" to obtain the missing disposition information. Once the effort is fulfilled, a DOJ employee reviews any information obtained and prepares the background check response according to the statutory dissemination criteria.

Incorrect Data Entries

Incorrect data entries can be caused by information entered incorrectly by the Live Scan operator or by incomplete or improper information entered on the BCIA 8016 supplied by the agency. The applicant agency must accurately and completely populate the specified fields designated for the applicant agency's information on the BCIA 8016.

If the description of the "type of license, certification, or permit" was assigned by DOJ, it must be included in the submission exactly as it was assigned. If the "level of service" indicated on the form is "FBI," the FBI may use the description to verify the agency is authorized to receive a background check response from them. If the FBI cannot verify the type of employment, license, certification, permit, or working title transmitted to them, they will reject the transaction for confirmation and/or clarification. If this happens, the applicant must be fingerprinted a second time so the transaction can be resubmitted to the FBI by DOJ.

A delay can also occur if the agency's designated ORI or mail code is incorrect and the results are sent to the incorrect agency rather than the requesting applicant agency. The background check results will be sent via U.S. Mail to the applicant agency if the mail code is omitted.

Unfortunately, DOJ cannot correct most errors. In most cases, the applicant agency will have to send the applicant to be fingerprinted again as if it were the initial transaction. All fees will be charged again. If a

mistake is made by the Live Scan operator, then the agency should work with the Live Scan facility to have the second fingerprint rolling fee waived.

Poor Fingerprint Quality or Rejected Fingerprints

If an agency receives an "App Reject" or "FBI Reject" response due to an applicant's poor fingerprint quality, or rejected fingerprints, it means the fingerprint images taken were not as clear as they should have been. Poor fingerprint quality impacts the system's ability to confirm or deny a potential fingerprint match. Please be aware that an applicant's fingerprints may be accepted by the DOJ system, but rejected by the FBI. The FBI uses a higher threshold when comparing fingerprint images to define a match.

Pursuant to California Penal Code section 11105.7, if an applicant's fingerprints are rejected, the applicant must submit a second set of fingerprints. The applicant should return to the original Live Scan site with their copy of the BCIA 8016 and request a resubmission. All the information on the BCIA 8016 must be the same as the initial transaction. The applicant's ATI number, from the rejected transaction, must be entered in the "Original ATI Number" field on the BCIA 8016 for the second transaction, to link the two transactions and avoid additional costs. There is generally no charge for a resubmission due to rejected fingerprints.

To help decrease the chances of an applicant's fingerprints being rejected, have the applicant try these tips a few days before their appointment:

- Find a fingerprinting location that uses Live Scan (digital) technology rather than ink. Ink prints are acceptable, however, digital equipment produces better images.
- Avoid frequently washing or disinfecting hands on the day of your Live Scan appointment.
- Avoid activities that require the use of fingertips. This may include sports such as weight lifting or rock climbing, or playing musical instruments such as piano or guitar.
- Avoid regular handling of paper or typing.
- Avoid exposure to chemicals, such as bleach, chlorine, acetone, and antibacterial products.
- Moisturize for 2-3 days leading up to an appointment, but not on the day of the appointment.

Name Check Due to Fingerprint Rejects

Even if an applicant's second submission of fingerprints is illegible, the applicant shall be deemed to have complied with the statutory requirement to submit fingerprints. In this situation, a background check based on a name check will be performed for the applicant instead.

Applicants whose fingerprints are rejected twice by DOJ due to poor fingerprint quality will be processed by DOJ via a search of the applicant's name and personal descriptors in DOJ's criminal history database.

For applicants whose fingerprints are rejected twice by the FBI, one of the rejection responses must be the L0008 error message stating, "The quality of the characteristics is too low to be used" to prompt a name check. Any other reason code is considered correctable by the fingerprint roller and is not rejected due to poor fingerprint quality. DOJ's FBI Response Unit will submit a request to the FBI, on behalf of the applicant agency, to request a name check from the FBI through the national criminal history database. The applicant agency should not contact the FBI to request a name check.

Remitting Fees

If an agency has a billing number, DOJ processing fees should be remitted monthly upon receipt of the invoice from DOJ. The monthly billing detail report will consist of the applicant's name, fingerprint date, and total fingerprint fees billed. If an agency finds a discrepancy within its billing details, the agency may

request a credit using the *Credit Request – Applicant Live Scan Fingerprint Billing* (BCII 9006), and DOJ will research the request. All credit requests should be emailed to DOJ.AppBill@doj.ca.gov. Regardless of any potential discrepancy, the applicant agency must pay their monthly invoice in full upon receipt.

No Longer Interested

Pursuant to California Penal Code section 11105.2, every applicant agency must immediately notify DOJ and submit a No Longer Interested (NLI) request when:

- Employment is terminated
- A license or certificate is revoked
- An applicant did not renew or cannot reinstate the license or certificate
- An applicant is not chosen for employment or is denied licensing, certification, or approval

A notification must be submitted within five days via an NLI request in the AAJC Portal. The NLI requirement includes reconciling and updating a list with whom an agency does or does not have an existing relationship in the Active Applicants feature in the AAJC Portal. Please reference the *AAJC External User Guide* for a step-by-step guide on how to submit an NLI request. For video tutorials and FAQs on NLI requests and the Active Applicants feature, navigate to the Resources widget on the AAJC home page.

California Penal Code section 11102.2 requires applicant agencies to immediately notify DOJ when a designated COR no longer serves in that capacity. Since applicant agencies cannot submit an NLI request for a COR in the AAJC Portal, notifying DOJ should be done by emailing the NCJAOS at COR@doj.ca.gov.

Security and Access to CORI

Definition of CORI

The records and data compiled by criminal justice agencies for purposes of identifying criminal offenders are referred to as CORI. It may also include: a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges; information pertaining to sentencing, incarceration, rehabilitation, and release; or information depicting employment, licensing, and certification history. Criminal justice agencies throughout the state provide this information to DOJ, and it is maintained in a statewide repository.

Proper Use of CORI

The CORI that an agency receives as a result of a fingerprint-based background check may only be used for official purposes, and only for the specific purpose for which it was requested and provided. Agencies must not subsequently re-use CORI for a different purpose or subsequent application even if a statute authorizes access to CORI. No agency or individual shall confirm the existence or nonexistence of CORI to any person or agency that does not have the authority to receive the information. CORI may only be disclosed as specifically authorized by law.

Proper Use of Assigned ORI Number and Applicant Types

Once an ORI is assigned, it may only be used for the purpose for which it was assigned according to state and federal law. Agencies may only submit requests for CORI using applicant types covered by the statutory authority leveraged for the request. In addition, agencies may only submit requests for

purposes that are known to exist at the time of submission. Agencies must not submit requests for a future anticipated need, even if the need is authorized by statute.

> ***Example 1:*** *A local government agency that has an ORI approved to conduct fingerprint-based background checks for applicants seeking the issuance of a license, cannot use the ORI to conduct fingerprint-based background checks for their employees.*
>
> ***Example 2:*** *A non-profit agency with an ORI approved to conduct fingerprint-based background checks for volunteers and employees that provide direct supervision of minors, cannot use the ORI to conduct fingerprint-based background checks on employees that provide care for the elderly.*

If an agency would like to submit fingerprint-based background checks for an additional applicant population other than the one they were originally authorized for, they must contact the NCJAOS at ORIQuestions@doj.ca.gov for assistance.

Misuse of CORI

CORI and related data are sensitive and have the potential for great harm if misused. The unauthorized access and misuse of it may result in the suspension or loss of employment and prosecution for state and federal crimes. Additionally, any person intentionally disclosing information obtained from personal or confidential records maintained by DOJ, or from records within a system of records maintained by a governmental agency, violates various California privacy and confidentiality laws. Several statutory provisions impose penalties for misuse or unauthorized use of CORI.

> California Penal Code sections 11142 and 13300 state: "Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person not authorized by law to receive a record or information is guilty of a misdemeanor."
>
> California Civil Code section 1798.53 states: "Any person who intentionally discloses information, not otherwise public, which they know or should reasonably know was obtained from personal or confidential information maintained by a state agency or from records within a system of records maintained by a federal government agency, shall be subject to a civil action, for invasion of privacy, by the individual."

Dissemination of CORI

CORI is disseminated to applicant agencies based on California and federal statutory authority. California and federal statutory authority controls the dissemination of CORI received from DOJ. Other state or local laws, ordinances, administrative rules, or procedures, do not govern the dissemination of CORI.

State-Level of Service

CORI is disseminated for state-level of service pursuant to California Penal Code section 11105. The complete California Penal Code section with/containing dissemination criteria can be found on the California Legislative Information website.

- Subdivision (k) applies to requests from an authorized agency or organization where the information is to be used for peace officer employment or certification purposes.
- Subdivision (l) applies to requests from a criminal justice agency or organization where the information is to be used for criminal justice employment, licensing, or certification purposes.
- Subdivision (m) applies to requests from an authorized agency or organization pursuant to California Health and Safety Code sections 1522, 1568.09, 1569.17, or 1596.871, or a statute

that incorporates the criteria of any of those sections or this subdivision by reference, where the information is to be used for employment, licensing, or certification purposes.

- Subdivision (n) applies to requests from an authorized agency, organization, or individual, where the information is to be used for employment, licensing, or certification purposes pursuant to any of the following:
    - Subdivision (c)(10) of California Penal Code section 11105, and the information is used by a cable corporation
    - California Penal Code sections 11105.3 or 11105.4
    - California Welfare and Institutions Code section 15660
    - Any statute that incorporates the criteria of any of the statutory provisions listed in the points above
- Subdivision (o) applies to requests from an authorized agency or organization under California Financial Code section 379 or 1300, or a statute that incorporates the criteria of either of those sections or this subdivision by reference, where the information is to be used for employment, licensing, or certification purposes.
- Subdivision (p) applies to requests from an agency, organization, or individual not described in subdivision (k), (l), (m), (n), or (o), or by a transportation company authorized under California Penal Code section 11105.3, or a statute that incorporates the criteria of that section or this subdivision by reference, where the information is to be used for employment, licensing, or certification purposes.

Federal-Level of Service

Federal-level of service dissemination criteria is determined by statute and by agency type. The dissemination criteria mirrors that of state-level of service, except for nongovernmental agencies. Federal Public Law 92-544 prohibits nongovernmental agencies, otherwise known as private entities, from receiving federal CORI. Instead, when a nongovernmental agency has requested a fingerprint-based background check for an applicant, the agency will receive a response that DOJ is unable to make a determination. The response will not contain federal CORI or allude to the presence of federal CORI. An example of the response is:

> *The Department of Justice (DOJ) has reviewed the results of the fingerprint search and is unable to make a determination for this applicant.*
>
> *The DOJ is prohibited from releasing any further information to a non-governmental entity.*
>
> *If the applicant wishes to obtain a copy of his/her FBI criminal history record, he/she should go to www.fbi.gov/about-us/cjis/background-checks or write to:*
>
> *FBI/CJIS DIVISION*
>
> *Attn: SCU MOD2*
>
> *1000 Custer Hollow Rd*
>
> *Clarksburg, WV 26306*
>
> *If you have any questions regarding this matter, please contact the Department of Justice, Applicant Services Program, FBI Response Unit at FBIResponseUnit@doj.ca.gov.*

Most governmental agencies are statutorily designated, funded, and organized as part of a state's executive, legislative, and judicial branches. However, governmental entities such as commissions and

boards that may be comprised of political appointees, elected officials, and/or officials from private industry, may also qualify as authorized recipients of CORI (e.g., school boards and lottery commissions).

A Fitness Determination to a Nongovernmental Agency

A nongovernmental agency may work with a governmental agency (i.e. a city or county board) to assist with providing a fitness determination for their applicants. The nongovernmental agency would designate a governmental agency as the responsible entity for conducting the background check and receiving the federal CORI. In this relationship, the nongovernmental agency would not be delegated access to the AAJC Portal or be given any copies of responses containing federal CORI. The governmental agency would provide a determination to the nongovernmental agency without alluding to the presence of CORI.

Subject of Record

Under California Penal Code section 11105(t), whenever state or federal CORI is provided by DOJ, the authorized agency shall expeditiously furnish a copy of the information to the subject of the record if the information is a basis for an adverse employment, licensing, or certification decision.

To limit potential risks associated with a subject's subsequent use of a criminal history record, it is recommended that the original background check response remain with the applicant agency and that a copy be provided to the subject of the record. The copy should be marked as "copy." Agencies that provide a copy of the CORI to the subject of the record should verify the subject's identity before giving them the copy and should document each occurrence. When furnished other than in person, the copy shall be delivered to the last known address provided by the applicant.

To review and challenge the information in an applicant's criminal history record, the applicant must request a copy of their criminal history record from DOJ. For more information about the Record Review process, please visit the DOJ website at: https://oag.ca.gov/fingerprints/security.

Public Access

CORI is exempt from disclosure under the California Public Records Act. CORI must not be disseminated to the general public. The prohibition includes maintaining CORI in formats that are accessible by the public or within records that are subject to release through public record requests. However, CORI may be disclosed as part of the adjudication process during a hearing that is open to the public if the agency demonstrates:

- The hearing is based on a formally established requirement
- The applicant is aware before the hearing that CORI may be disclosed
- The applicant is not prohibited from being present at the hearing

Even when the specific conditions are met to allow disclosure during a public hearing, the most preferable method for introducing CORI is during closed session, if authorized, which limits participation by the public at large.

Personnel Security

Background Check Requirements for Personnel with Access to CORI

Before permitting access to CORI, agencies must ensure all personnel with access to CORI undergo a state and federal fingerprint-based background check. For this section, "access to CORI" means the physical or electronic ability to view, modify, or make use of CORI.

Personnel designated as CORs for their agency shall undergo the COR confirmation process, which includes a state and federal fingerprint-based background check. For more information on the COR confirmation process, please refer back to the Custodian of Records Confirmation section within this document.

Personnel that are not designated as CORs, and may have access to CORI, must undergo an employment fingerprint-based background check. An agency's employment fingerprint-based background check must include state and federal levels of service to satisfy this requirement.

Agencies must submit a notification within five days via an NLI request in the AAJC Portal whenever an employment relationship no longer exists with any personnel. Please reference the No Longer Interested Section for further details.

Agencies and CORs should familiarize themselves with the requirements specified in the FBI *CJIS Security Policy* and implement a formal sanctions process for personnel failing to comply with established CORI security policies and procedures.

Physical Protection of CORI

When an agency retains CORI for an authorized purpose, it must establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the information. In addition to security awareness training, personnel security controls, and technical security controls, each authorized agency must implement the following physical controls:

- Separate and post the perimeter away from non-secure locations
- Keep a current list of personnel with authorized access
- Control all physical access by verifying individual access authorizations before granting access
- Control physical access to information system distribution and transmission lines within the location
- Control physical access to devices that display CORI and position the devices to prevent unauthorized individuals from accessing and viewing CORI
- Monitor physical access to the information system to detect and respond to physical security incidents
- Control physical access by authenticating visitors before authorizing escorted access to the location and escort visitors at all times and monitor visitor activity
- Authorize and control information system-related items entering and exiting the location

If an agency cannot meet all of the physical controls required for establishing a physically secure location but has an operational need to access or store CORI, the agency must designate a controlled area. A controlled area can be an area, room, or storage container, established for day-to-day CORI access or storage. The agency must, at a minimum:

- Limit access to the controlled area during CORI processing times to only those personnel authorized by the agency to access or view CORI.
- Lock the area, room, or storage container when unattended.
- Position information system devices and documents in such a way as to prevent unauthorized individuals from access and view.
- Follow the encryption standards found in the FBI *CJIS Security Policy*.

Agencies must implement and document policies and procedures to ensure CORI is physically protected through access control measures. For additional information, please reference the FBI *CJIS Security Policy*.

Media Protection of CORI

CORI may only be stored for an authorized purpose on two forms of media. The first is digital media. "Digital media" is electronic storage media such as memory devices in laptops and computers (e.g., hard drives). Digital media also includes any removable, transportable digital memory media such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

The second form is "physical media," referring to CORI in physical form (e.g., printed documents, printed imagery, etc.).

Transmitting or Transporting CORI

All CORI transmitted or transported outside a physically secure location must be encrypted according to FBI standards or carried in a locked container and protected in transit. Email is not a secure method of communication. Do not send CORI in an email unless the proper technical controls are in place to protect it, such as encryption and access control. Physical media shall be protected at the same level as the information would be protected in electronic form.

Destruction or Sanitization of CORI

Agencies must sanitize (electronically overwrite the data at least three times) or degauss (decrease or eliminate a remnant magnetic field) digital media containing CORI before disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed and carried out only by authorized personnel. Inoperable digital media must be destroyed by cutting up, shredding, etc.

Agencies must securely dispose of physical media containing CORI when no longer needed by shredding or incineration. This disposal or destruction needs to be witnessed and carried out only by authorized personnel.

Agencies must implement and document policies to ensure that access to digital and physical media in all forms containing CORI is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting, and storing media. For additional information, please reference the FBI *CJIS Security Policy*.

Outsourcing

Some applicant agencies may outsource CORI-related responsibilities to an outside agency or third-party contractor. This may include contracting with a third party to review the background check results and make the eligibility or hiring determinations, storage of personnel files containing criminal history records, and destruction of criminal history when it is no longer needed. Outsourcing may involve both physical and electronic access to CORI, as there is an increasing occurrence of information being maintained electronically and accessed by information technology vendors and contractors.

Governmental agencies are the only applicant agencies permitted to submit a request for outsourcing. Before allowing a third-party contractor access to CORI, the applicant agency must first submit the *Request for Outsourcing of Noncriminal Justice Functions* (BCIA 7000) to the Chief Administrator of DOJ.

Once the BCIA 7000 is received, the *Outsourcing Management Control Agreement* (BCIA 7001) will be sent out to the authorized applicant agency. This agreement is intended to set forth the terms and conditions under which the contractor may receive CORI, on behalf of the applicant agency, and the responsibilities of each participating party.

The authorized applicant agency will be required to submit a detailed description of its information system configurations, its system applications, processes, procedures, data structures, authorization

processes, data flow, and its system environment. Security controls must be in place to meet the outsourcing requirements needed to protect CORI.

If approved, DOJ will conduct an audit of the contractor and ensure applicant agency compliance in outsourcing. For further details, please reference the National Crime Prevention & Privacy Compact Council's *Security and Management Control Outsourcing Standard for Non-Channelers.*

Applicant Agency Audits

Formal audits ensure compliance with all CORI security requirements. The CSA must periodically audit all noncriminal justice agencies with access to CORI to ensure compliance with applicable statutes, regulations, and policies. The FBI *CJIS Security Policy* imposes the minimum security requirements that states must follow. The FBI CJIS Audit Unit will triennially conduct audits of a sampling of noncriminal justice agencies as well. For additional information, please reference the FBI *CJIS Security Policy* available on the FBI website.

In California, the process of periodically auditing all noncriminal justice agencies with access to CORI is the responsibility of DOJ. Audits will be conducted every three years; however, they may be conducted on a more frequent basis if an audit reveals an agency is not in compliance with state and/or federal laws.

For further information related to the audit methodology and specific areas of review, please see the *Applicant Agency Audit Procedure Guide* located in the AAJC Portal on the Resources page.

Appendix A: Acronyms

Acronym	Term
AAJC	Applicant Agency Justice Connection
ACP	Authorization and Certification Program
ARQSB	Applicant and Record Quality Services Branch
ASP	Applicant Services Program
ATI	Applicant Transaction Identifier
BCIA	Bureau of Criminal Information and Analysis
DOJ	California Department of Justice
CACI	Child Abuse Central Index
CAU	CJIS Audit Unit
CJILU	Criminal Justice Information Law Unit
CJIS	Criminal Justice Information Services
COR	Custodian of Records
CORI	Criminal Offender Record Information
CSA	CJIS System Agency
FBI	Federal Bureau of Investigation
LASO	Local Agency Security Officer
LSID	Live Scan Identification
MFA	Multi-Factor Authentication
NCJAOS	Noncriminal Justice Access Oversight Section
NLI	No Longer Interested
OCA	Originating Case Agency
ORI	Originating Agency Identifier
OTP	One-Time Password
RAP	Record of Arrest and Prosecution
RQSP	Record Quality Services Program
TASS	Training and Administrative Support Section

Forms Index

Form Name	Form # (if applicable)	Form Purpose
Billing Account Application [CJIS]	9000	For applicant agencies that wish to be billed for fingerprints submitted through Live Scan.
Request for Live Scan Service (Custodian of Records) [BCIA]	8016	Provided to the agency's designated COR to begin the confirmation process to complete a Live Scan.
Custodian of Record Application for Confirmation [BCIA]	8374-9007	Provided to the agency's desired COR applicant.
CORI Security Requirements [BCIA]	9007	To inform Agency Head(s) and COR(s) of the importance of maintaining the security of CORI, and the roles and responsibilities for accessing, securing, storing, disseminating, and destroying CORI.
Employee Statement [BCIA]	9006	To acknowledge knowledge and understanding of the laws prohibiting the misuse of CORI, which must be kept on file by the COR.
Authorized Recipient User Agreement [BCIA]	9005	Establishes the terms and conditions under which CORI will be provided to the authorized applicant agency.
Contract for California Subsequent Arrest and Disposition Notifications [BCIA]	8049	Sets forth the terms and conditions to be adhered to by the subscribing agency and COR(s) if they wish to utilize the service.
Background Check Requirement Verification	N/A	Agencies that apply to become a School Contractor must have the contracting school district or school complete this form. Confirms that a background check will be required from the applicant before beginning work on school grounds.
Request for Department of Justice Name Check [BCIA]	9010	To be completed and submitted in the instance the applicant is unable to submit legible fingerprints due to disability, illness, accident, or other

		circumstances beyond their control.
Credit Request Applicant Live Scan Fingerprint Billing [BCII]	9006	If there is a discrepancy with billing details, an agency may submit this form for DOJ to research said discrepancy.
Request for Outsourcing of Noncriminal Justice Functions [BCIA]	7000	To allow a third-party contractor access to information relating to CORI.
Outsourcing Management Control Agreement [BCIA]	7001	Sent to the agency once BCIA 7000 has been completed and received.
CORI Authorization [BCIA]	9001	To request authorization to receive CORI.
Applicant Transmittal Form – Billing [JUS]	204	For an agency that wishes to be billed for the process of submitting fingerprint hard cards to DOJ.
Applicant Transmittal Form – Prepaid (Cash)	203	For an agency that wishes to pay via check or money order for the process of submitting fingerprint hard cards to DOJ.