Guide to AB 506 & DOJ Background Checks

Church & Casualty™
INSURANCE AGENCY

MESA NETWORK

OVERVIEW

Below are simple, actionable steps to take to ensure compliance and be prepared should the DOJ audit your organization:

What is AB 506?

AB506, now known as Business and Professions Code Section 18975, took effect on January 1, 2022. It requires all youth-serving organizations in California to meet oversight standards to protect vulnerable populations. Here's what is required for your organization:

KEY REQUIREMENTS:

Training

Administrators, employees, and regular volunteers must complete training in child abuse and neglect identification and reporting. AB506 allows organizations to use the mandated reporter training provided by the California Office of Child Abuse Prevention. However, this training:

- Does not specify required topics, length, frequency, or record-keeping requirements.
- Does not include an online record-keeping option–organizations must track completion manually.

Recommendation:

If you don't have a current training program, we highly recommend MinistrySafe's training, which provides:

- More comprehensive education on spotting groomers.
- Stronger safeguards tailored for youth-serving organizations.
- Better tracking and documentation options.

By implementing MinistrySafe's training, your organization can take an extra step toward preventing abuse and protecting children.

An alternative training that we recommend is Kingdom One's Above Reproach course, which provides all the requirements of AB 506, taught from a Christian perspective.

Reach out to CCIA for information about customer discount codes for these programs.

Background Checks

These individuals must undergo a background check under Penal Code Section 11105.3 to screen for a history of child abuse. DOJ Background Checks: Live Scan fingerprinting is mandatory for all employees and volunteers working with youth. Volunteers are included if they work more than 16 hours a month or 32 hours a year.

Child Abuse Prevention Policies

- Organizations must develop reporting policies to ensure suspected child abuse is reported to external entities, including mandatory reporting under Penal Code Section 11165.9.
- Policies should require at least two mandated reporters to be present when supervising children whenever possible.
- Exception: One-on-one mentoring programs are exempt if they implement screening, training, and regular contact policies for volunteers and parents.

Liability Insurance Compliance

Insurers may request proof of compliance with these requirements before providing liability insurance.

Definitions

- Regular volunteer: An 18+ volunteer with direct contact or supervision of children for 16+ hours per month or 32+ hours per year.
- Youth service organization: Any organization with employees or volunteers who are mandated reporters under Penal Code Section 11165.7(a)(7).

Why Compliance Matters

Compliance with DOJ regulations isn't just about checking boxes—it's about building a safer, more accountable organization. Whether you're running a church, youth group, or nonprofit, understanding and adhering to these rules protects everyone involved and ensures your organization remains operational and trusted.

Specialized Training

- Specialized Training: Everyone—from administrators to volunteers—must complete training on child abuse prevention and safe practices.

- The presence of two or more mandated reporters when supervising or in contact with youth under 18 years of age

Terms To Know

ICJIS
Criminal Justice Information Services.
A division of the FBI. CJIS provides services and tools to law enforcement, intelligence agencies, and the public.

COR
Custodian of Records
The agency Custodian of Records will be responsible for the security, storage, dissemination and destruction of the criminal records furnished to the agency and will serve as the primary contact for the DOJ.

1. Be at least 18 years old
2. Complete and submit the Custodian of Records Application Form (BCIA 8374)

CORI
Criminal Offender Record Information
CORI means records and data compiled by criminal justice agencies for purposes of identifying criminal offenders.

For each offender, CORI may include a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, and information pertaining to sentencing, incarceration, rehabilitation, and release.
Criminal justice agencies throughout the state provide this information to the DOJ, which in turn is required to maintain it in a statewide repository.

DOJ
Department of Justice
The California Department of Justice (DOJ) is mandated to maintain the statewide criminal record repository for the State of California. In this capacity, sheriff, police and probation departments, district attorney offices, and courts submit arrest and corresponding disposition information.

The DOJ uses this information to compile records of arrest and prosecution, known as "RAP sheets," for individuals and disseminates the information for law enforcement and regulatory (employment and licensing) purposes.
RAP sheets are based upon fingerprint submissions, and therefore positively identified biometrically; a process by which a person's unique identity is confirmed.

Human resource agency
Defined as a public or private entity responsible for determining the character and fitness of a person applying for a license, employment, or as a volunteer within the human services field that involves the care and security of children, the elderly, the handicapped, or the mentally impaired.

ORI - Organization Record Identifier
The California Department of Justice requires any agency that needs to conduct fingerprint (Live Scan) of employees and volunteers to have an ORI number. If you are a church or youth service organization, this is now a legal requirement for you as of January 1, 2022

OBTAINING DOJ CREDENTIALS & LIVESCAN FINGERPRINTING

Step 1: Application for credentials

- Fill out the Complete the Youth Organizations – Human Resource Agencies Application
- Fill out **REQUEST FOR AUTHORIZATION TO RECEIVE STATE SUMMARY CRIMINAL HISTORY** (page 4 and 5) This is organization specific.
- Fill out **REQUEST FOR CONTRIBUTING AGENCY ORI AND/OR RESPONSE MAIL CODE** (BCII 9001) (BCII 9001 page 6) This is organization specific and gives your organization an Organization Record Identifier. This is for first time organization applicants. If your organization has never signed up for this, you must fill this out.
- Fill out **NOTIFICATION OF ORI, MAIL CODE AND/OR BILLING NUMBER ASSIGNMENT** (BCIA 9003 page 8). This is organization specific. This is a request for an ORI and mail code.
- Fill out **BILLING ACCOUNT INFORMATION** (CJIS 9000 page 11). This is an application to be filled out if your organization will pay for Livescans for your employees and volunteers.
- The Custodian of Records (COR) needs to read and fill out the **APPLICANT FINGERPRINT RESPONSE SUBSCRIBER AGREEMENT** (BCIA 9005 pages 13-16). This person is the one who will have access to the DOJ portal and will be the one that must protect and maintain employee and volunteer records.
- The Custodian of Records (COR) must fill out and sign **USE OF APPLICANT CRIMINAL OFFENDER RECORD INFORMATION** (p. 17)
- The Custodian of Records (COR) must fill out and sign **USE OF APPLICANT CRIMINAL OFFENDER RECORD INFORMATION** (CORI) (p. 18).
- The Custodian of Records (COR) must fill out and sign the **COR CUSTODIAN OF RECORDS APPLICATION FOR CONFIRMATION** (BCIA 8374 p. 19).

Step 2: COR Livescan

The COR must schedule an appointment (online) to get fingerprinted as a COR (even though he/she was fingerprinted in the past). They must fill out the **REQUEST FOR LIVE SCAN SERVICE** (Custodian of Records) (BCIA 8016CUS p. 21) Apply ONLY AFTER receiving DOJ authorization confirmation.

- *Your application may be returned with additional information needed.*
- *Once your application has been accepted, you will receive a COR request for LiveScan*
- *Have the Custodian of Records complete the Live Scan*

Step 3: Approval

Once the COR Live Scan is approved, you will receive a notification via mail or email notifying you of the COR approval.

After COR Life Scan is approved, you will need to wait for a Welcome Packet from the DOJ – this notifies your final approval and that you are able to start Live Scan fingerprinting.

OBTAINING DOJ CREDENTIALS & LIVESCAN FINGERPRINTING

Step 4: Fingerprinting

Complete the Employer/Agency portions of the LIVESCAN form.

The organization fills in:

- ORI code
- Type of application (employee, volunteer, etc.)
- Your organization's information (Agency Information)
- Mail code - This is an electronic method for delivering the results.
- Additional Agency Information - Fill out Level of Service (DOJ and FBI)

Livescan locations can be found at: https://oag.ca.gov/fingerprints/locations
Access information about your application. https://applicantstatus.doj.ca.gov/

Fingerprinting Fees:

There are rolling fees that will vary from location to location and cover only the operator's cost of rolling the fingerprint images. The applicant will need to pay this when getting their fingerprinting and can be reimbursed by the employer/agency.

The Employer/Agency will be charged a fee separate from that paid at the location. You can see the breakdown of fees here and these will be invoiced monthly from DOJ.

Additional Information:

- Incomplete forms will be returned unprocessed.
- Please do not submit your fingerprint(s) until approval has been granted.
- Mail the completed form into the DOJ (address listed on application)
- You must provide proof of nonprofit status
- Photocopy and keep a set of documents in case you need to discuss with a government employee or in case the originals get lost in the mail

Employee or Volunteer - How to fill out the BCIA 8016

Instructions for completing the REQUEST FOR LIVE SCAN SERVICE APPLICANT SUBMISSION FORM

Be sure to take identification to the live scan site. You must show ID prior to having your fingerprints taken.

The following information must be printed or typed on the form. All other spaces on the form should remain **blank.**

- Name of Applicant: Enter your full name.
- Alias: Enter any other names you have used.
- Date of Birth: You must provide your date of birth in order for the Secretary of State's Office to process your background check.
- Sex: Gender (male or female)
- Height
- Weight
- Eye Color
- Hair Color
- Place of Birth
- SOC: Social Security Number.
- Driver's License No.: California driver's license number. If you do not have a California driver's license, enter other identifying numbers such as another state driver's license number or California ID card number.
- Agency/OCA No.: Enter your driver's license number or birth date.

IMPORTANT: Retain two copies of the **Request for Live Scan Service form:** one copy will be submitted to the Secretary of State; the second copy is for your records in case you need to have your prints retaken.

This copy will serve as your proof that you or your organization has paid the fingerprint processing fee so you will not be required to pay again. You may, however, be required to pay for the rolling fee. Website with details: https://oag.ca.gov/fingerprints/agencies // For questions email: applicantinfoservices@doj.ca.gov OR AuthorizationQuestions@doj.ca.gov

CUSTODIAN OF RECORDS (COR)

An organization employs a COR (Custodian of Records) who must meet Essential Compliance Requirements for CORs (Custodian of Records)

Custodian of Records (COR) Responsibilities

To meet AB506 and DOJ standards a COR assumes the following responsibilities:

Expertise & Compliance

- Serve as the agency's expert on **Criminal Offender Record Information (CORI)** security policies.
- Stay informed on all relevant state and federal regulations.

Training & Access Management

- Complete CJIS Security Awareness Training within six months and biennially thereafter.
- Manage CJIS administrative account privileges and training assignments for agency personnel.

Secure Handling of CORI

- Maintain CORI in a locked and secure location, separate from personnel files.
- Ensure proper dissemination, storage, and destruction of CORI, including:
  - Preventing unauthorized access to terminals.
  - Using strong passwords for system security.
  - Keeping dissemination logs up to date.

Security Measures & Incident Reporting

- Establish handling procedures to protect against unauthorized access.
- Track, document, and report security incidents to the CA DOJ.

Destruction of Digital & Physical Media

- Use formal procedures for secure disposal of sensitive data.
- Destroy digital media via overwriting (3x), degaussing, or physical destruction.
- Shred or incinerate physical records to prevent compromise.

Providing Criminal History Records

- Provide an individual with their criminal history if it was used in an adverse hiring, licensing, or certification decision, as required by California Penal Code § 11105(t).

Notification of Changes

- Notify CA DOJ when an applicant's authorized relationship ends (e.g., not hired, employment terminated, license revoked) via an NLI request in the AAJC portal within five days.
- Report changes to Custodian of Records status, agency name, address, or phone number in a timely manner.

Statutory Authority & Compliance

- Maintain a **list of statutory authority** for conducting criminal background checks to support agency audits and use CORI only for its intended purpose.

Live Scan & Privacy Notices

- Keep an up-to-date Request for Live Scan Service form (BCIA 8016).
- Ensure all applicants acknowledge receipt of Privacy Notices before fingerprinting.

Point of Contact for CA DOJ

- Act as the primary liaison for DOJ or FBI audits to ensure compliance.
- Provide information on Live Scan transactions when requested.

DOJ AUDITS

From a DOJ representative when asked about the audits: "[The DOJ] prefer[s] to steer agencies toward better CORI management practices and, if serious issues persist, will temporarily restrict an agency's access to CORI. If persistent issues require long-term restrictions, that could potentially affect an agency's ability to maintain their insurance coverage."

PREPARING FOR DOJ AUDITS

The DOJ plans to eventually audit every organization submitting fingerprints for criminal history checks. The FBI mandates that states review Livescan data for auditing at least once every three years. Churches and Houses of Worship are getting audited, but not at a very high rate. While there's no set timeline, audits will focus on these key areas:

Audit Focus Areas

- Up-to-Date Background Checks: Ensure all employees and volunteers have valid Live Scans on file.
- Accurate Participant Tracking: Remove inactive individuals promptly from monitoring systems.
- Data Security: Keep CORI secure and destroy outdated records properly.
- Training Records: Verify that all mandatory training is completed and documented.

What Happens During an Audit?

- Audit Assignment: You will be emailed about an assignment to an audit. No one is showing up at your door.
- Timeline: You have 30 days to respond to audit requests by completing the audit and submitting it back.
- Noncompliance: Upon review, if there are non-compliant findings, it is sent back to you, and you are given another 30 days to correct them.

HOW TO STAY COMPLIANT

Policy and Data Management

- Develop clear policies for managing CORI access, storage, and destruction.
- Limit CORI access to trained, authorized personnel only.
- Shred or delete outdated CORI records securely.

Training Requirements

- Train all employees and volunteers on child safety and DOJ compliance.
- Ensure Custodians of Records complete DOJ certification.
- Provide confidentiality training for anyone handling CORI.

Self-Audit Checklist

- Verify employment and volunteer statuses regularly.
- Update monitoring lists to reflect only active participants.

Avoiding Common Mistakes

Top Compliance Pitfalls

- Retaining outdated CORI longer than legally required.
- Allowing unauthorized personnel to access sensitive data.
- Failing to notify the DOJ about "No Longer Interested" (NLI) statuses.
- Lack of transparency. Be transparent with applicants and participants about background check procedures. Inform individuals of their rights to view and dispute criminal history reports.

Resources and Support

Key Tools for Success

- Policy Templates: Use DOJ-approved resources to create compliant policies.
- Training Programs: Attend workshops or webinars on child safety and DOJ audits.
- Guidance Forms: Employees who access critical documents like the BCIA 8016 Employee Statement Form, must fill out the Employee Statement Use of Applicant Criminal Offender Record Information (p. 22).

Need Help?

By following these steps, your organization will be well-positioned to navigate DOJ audits and maintain compliance with AB506.

Reach out to our HR partners, **MESA NETWORK** through CCIA's **AskHR service**, or directly to the DOJ for tailored advice or explore additional resources to ensure your team is prepared.

APPENDIX A

Employee Statement Use of Applicant CORI

Additional employees who have access to the CORI information must sign the EMPLOYEE STATEMENT USE OF APPLICANT CRIMINAL OFFENDER RECORD INFORMATION (p. 22 of the ORI/COR application).

This document is kept and monitored by the COR. DO NOT submit to the DOJ with other documents.

DEPARTMENT OF JUSTICE
DIVISION OF CALIFORNIA JUSTICE INFORMATION SERVICES

RESEARCHER SECURITY AND DISCLOSURE FORM

As a requestor of Criminal Offender Record Information, (CORI) you will have access to confidential criminal record information which is controlled by state and federal statutes. Misuse of such information may adversely affect an individual's civil rights and violate their constitutional rights of privacy. The penalties for the misuse of CORI information are covered under the following Penal Code and Government Code sections: Penal Code section 502 prescribes the penalties relating to computer crimes. Penal Code sections 11105 and 13300 identify who has access to criminal history information and under what circumstances it may be disseminated. Penal Code sections 11140-11144 and 13301-13305 prescribe penalties for misuse of criminal history information. Government Code section 6200 prescribes felony penalties for misuse of public records.

Penal code sections 11142 and 13303 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 the record of information, is guilty of a misdemeanor."

Invasion of Privacy 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."

CIVIL, CRIMINAL, AND ADMINISTRATIVE PENALTIES

-11141 PC: DOJ furnishing to unauthorized person (misdemeanor)
-11142 PC: Authorized person furnishing to other (misdemeanor)
-11143 PC: Unauthorized person in possession (misdemeanor)
-California constitution, Article I, Section I (Right of Privacy)
-1798.53 Civil Code
-Title 18, USC, Sections 641, 1030, 1343, 1951, and 1952

Violations of these laws may result in criminal and /or civil action.

I HAVE READ THE ABOVE AND UNDERSTAND THE POLICY REGARDING MISUSE OF CORI INFORMATION.

SIGNATURE_____ **DATE**_____

PRINTED NAME_____

APPENDIX B

Child Abuse Prevention Policy For [Organization Name]

Purpose

[Organization Name] is committed to providing a safe, nurturing, and Christ-centered environment for all children and youth under our care. In alignment with biblical teachings, we uphold the sanctity of every individual and seek to protect the vulnerable from harm. This policy outlines our commitment to preventing child abuse and ensuring the safety of minors involved in our programs and ministries.

Scope

This policy applies to all staff members, volunteers, and representatives of [Organization Name] who interact with children and youth in any capacity.

Definitions

- Child Abuse: Any action or lack of action that results in physical, emotional, or sexual harm to a minor.
- Neglect: Failure to provide for a child's basic needs, including food, shelter, medical care, and emotional well-being.
- Physical Abuse: Any non-accidental physical harm inflicted upon a child.
- Sexual Abuse: Any form of sexual contact or behavior with a minor, including but not limited to inappropriate touching, exploitation, and exposure to explicit materials.
- Emotional Abuse: Verbal or non-verbal actions that harm a child's sense of self-worth, including constant criticism, threats, or rejection.

Screening and Training

1. Screening Procedures:
    - All staff and volunteers working with minors must undergo a thorough background check, including criminal records and reference verification.
    - Applicants must complete an interview and provide personal and professional references.
    - A probationary period may be required before full participation in ministry roles.

Training:

- All staff and volunteers must complete child abuse prevention training before serving.
- Regular refresher courses will be conducted annually.
- Training will include recognizing signs of abuse, appropriate interaction guidelines, and reporting procedures.

Safe Interaction Guidelines

- Two-Adult Rule: At least two approved adults must be present during all interactions with minors.
- No Private Meetings: Private one-on-one meetings between an adult and a child must take place in an open or easily observable setting.
- Appropriate Physical Contact: Physical contact should be appropriate, non-threatening, and should avoid areas of vulnerability.
- Digital Communication: Any communication between adults and minors must be transparent and include parents or guardians whenever possible.

Reporting Procedures

1. Mandatory Reporting: Any suspicion or knowledge of abuse must be reported immediately to the designated Child Protection Officer (CPO) or church leadership.
2. Confidentiality: Reports must be handled with the utmost sensitivity and confidentiality.
3. Reporting to Authorities: When required by law, [Organization Name] will report allegations to the appropriate legal authorities.
4. Response Plan:
    - Immediate action will be taken to ensure the safety of the child.
    - The accused individual may be suspended from duties pending an investigation.
    - Cooperation with authorities and appropriate pastoral care for all parties involved will be provided.

Monitoring and Accountability

- Regular Policy Review: This policy will be reviewed and updated annually or as needed.
- Accountability Team: A designated team will oversee compliance and address any concerns regarding child safety.
- Feedback Mechanism: Parents, staff, and volunteers are encouraged to report concerns or suggestions for improving child protection efforts.

Commitment Statement

By implementing this policy, [Organization Name] reaffirms its commitment to honoring God by protecting children and fostering a safe, Christ-centered environment for all.

Approved by: [Leadership Name]Date: [Approval Date]

Church & Casualty™
INSURANCE AGENCY

ABOUT US

We are specialists in property & casualty insurance and risk management solutions for California and Nevada houses of worship and nonprofit organizations.

Church & Casualty customers get free email access to our robust team of industry leaders, including HR & Employment Law professionals, Legal Information & Guidance, Finance & Accounting, and Security Consulting – all specializing in religious and nonprofit organizations.

Customers also get free and discounted value-added services to help manage risk further including child abuse awareness training, the Mineral online HR platform, safety response plans, safety resources and recommendations, background check services, and more.

We host several webinars and quarterly podcast episodes throughout the year to help educate and inform customers about relevant topics including changes to state and federal laws, HR compliance, various religious risk management topics, maintaining your property, and safety and security.

Call Us: (949) 852-8558

Email Us: hello@ccia.com