TEXT OF PROPOSED REGULATIONS
FOR PROPOSED AMENDMENTS TO THE SECURING OF CRIMINAL OFFENDER RECORD INFORMATION REGULATIONS

TEXT OF PROPOSED REGULATIONS

CCR, Title 11, Division 1, Chapter 7, Article 1, Section 700.

Title and Scope.

(a) This article shall be known as the "Mandatory Securing of Criminal Offender Record Information (CORI) Regulations.

(b) This article describes the processes and procedures for securing, storing, disseminating, and destroying CORI furnished by the Department of Justice to any entity or agency.

(c) If any part of this article is held to be unconstitutional, contrary to statute, exceeding the authority of the Attorney General, or otherwise inoperative, such decision shall not affect the validity of the remaining portion of the article.

Note: Authority cited: Section 11077, Penal Code. Reference: Sections 11075-11081, 11105, and 13202, Penal Code.

CCR, Title 11, Division 1, Chapter 7, Article 1, Section 701.

Definitions of Key Terms.

For the purposes of this article, the following definitions shall apply whenever the terms are used.

~~(a) "Criminal Justice Agency" means a public agency or component thereof which performs a criminal justice activity as its principal function.~~

~~(b) "Authorized Person or Agency" means any person or agency authorized by court order, statute, or decisional law to receive criminal offender record information.~~

~~(c) (Reserved)~~

~~(d) (Reserved)~~

~~(e) (Reserved)~~

~~(f) "Record Check" means obtaining the most recent rap sheet from the California Department of Justice.~~

(a) "DOJ" is the California Department of Justice or any employee, volunteer, or contractor of the Department of Justice acting under the authority of the Department of Justice.

(b) “Criminal offender record information” or “CORI” is the California master record of information compiled and maintained by the DOJ pertaining to the identification and criminal history of any person which may include name(s), state identification number or criminal identification and index number, date of birth, physical description, biometric data, photographs, date(s) of arrest(s), arresting agency or agencies, booking number(s), charge(s), disposition(s), sentencing, incarceration, rehabilitation, release, and similar data.

(c) “Entity” is any person or agency within California authorized by court order, statute, regulation, or decisional law to receive CORI, or any person or agency outside of California authorized by court order, statute, regulation, or decisional law to receive CORI.

(d) “Law enforcement agency” is any public official, agency, or subunit thereof that performs law enforcement functions pursuant to a statute, regulation, or ordinance.

(e) “Criminal justice agency” is any public official, agency, or subunit thereof that performs criminal justice functions pursuant to a statute, regulation, or ordinance.

(f) “Custodian of Records” is the person designated by an entity as responsible for securing, storing, disseminating, and destroying CORI furnished to or accessed by the entity.

(g) “Background check” is the process of obtaining from the DOJ the most recent state and, if applicable, federal level CORI of a person for law enforcement or criminal justice official duties or to determine a person’s suitability for employment, licensing, certification, or adoption purposes.

(h) “Regulatory or other entity” is any public official, agency, authority, body, or subunit thereof that is not a law enforcement agency or a criminal justice agency.

(i) “System misuse” is an unauthorized query or access into a DOJ, federal, or national database or system or via a DOJ telecommunication connection.

Note: Authority cited: Section 11077, Penal Code. Reference: Sections 11075-11081, 11102.2, 11105, and 13202, Penal Code.

CCR, Title 11, Division 1, Chapter 7, Article 1, Section 702.

~~Compliance with State Regulations~~**Accessing Criminal Offender Record Information.**

~~(a) (Reserved)~~

~~(b) (Reserved)~~

~~(c) The California Department of Justice shall conduct audits of authorized persons or agencies using criminal offender record information to insure compliance with the State regulations.~~

~~(d) (Reserved)~~

~~(e) Authorized persons or agencies violating these regulations may lose direct access to criminal offender record information maintained by the California Department of Justice.~~

(a) Every law enforcement or criminal justice agency or entity that receives CORI from the DOJ shall have a written policy that adheres to this article for securing, storing, disseminating, and destroying CORI. This policy shall include measures in place to prevent unauthorized access to CORI and to train persons authorized to access CORI.

(b) Law Enforcement and Criminal Justice Agencies

(1) Agency personnel who have access to CORI from the DOJ must pass a state and federal criminal record background check prior to being permitted access to CORI.

(2) Every agency not exempt from the provisions of Penal Code Section 11102.2(a) and 11102.2(b) that receives CORI from the DOJ shall submit to the DOJ, on the Custodian of Records Notification (Form BCIA 8375, November 2014, incorporated by reference herein), the name of an agency employee who has undergone a state and federal criminal record background check, to be the agency's Custodian of Records.

(c) Regulatory or Other Entities

(1) The Custodian of Records policy for regulatory or other entities is delineated in Section 11102.2, Penal Code.

(2) Only the designated Custodian of Records of a regulatory or other entity shall receive CORI from the DOJ. The Custodian of Records must be confirmed by the DOJ, through the Custodian of Records Application for Confirmation (Form BCIA 8374, November 2014, incorporated by reference herein), prior to being permitted to access CORI.

(d) Measures shall be taken to place terminals and equipment that transmit or receive CORI in an area with physical security to provide protection from theft, damage, vandalism, or sabotage, and to preclude access to CORI by unauthorized personnel. This includes protection from unauthorized viewing of CORI displayed on the actual terminals/devices or manually stored/printed data at all times.

Note: Authority cited: Section 11077, Penal Code. Reference: Sections 11075-11081, 11102.2, 11105, and 13202, Penal Code.

CCR, Title 11, Division 1, Chapter 7, Article 1, Section 703.

~~Release~~Handling of Criminal Offender Record Information.

~~(a) (Reserved)~~

~~(b) Criminal offender record information may be released, on a need-to-know basis, only to persons or agencies authorized by court order, statute, or decisional law to receive criminal offender record information.~~

~~(c) (Reserved)~~

~~(d) Record checks shall be conducted on all personnel hired after July 1, 1975, who have access to criminal offender record information.~~

(a) Any law enforcement or criminal justice agency authorized to receive CORI shall acknowledge compliance with the requirements of this article for maintaining the security of CORI and criminal penalties for failing to comply with these regulations by signing and submitting to the DOJ the California Law Enforcement Telecommunications System Subscriber Agreement (Form HDC 0001 Revised 03/20/2010, incorporated by reference herein).

(b) Any regulatory or other entity authorized to receive CORI shall acknowledge compliance with the requirements of this article for maintaining the security of CORI and criminal penalties for failing to comply with these regulations by signing and submitting to the DOJ the Applicant Fingerprint Response Subscriber Agreement (Form BCII 9005 Revised 01/2009, incorporated by reference herein).

Note: Authority cited: Section 11077, Penal Code. Reference: Section 15165, Government Code. Sections 11075-11081, 11102.2, 11105, and 13202, Penal Code.

CCR, Title 11, Division 1, Chapter 7, Article 1, Section 704.

~~Juvenile Records~~Dissemination of Criminal Offender Record Information.

(a) CORI received by a law enforcement or criminal justice agency for law enforcement purposes shall be used by the agency solely for the purpose for which it was requested, and not for any other purpose including employment, licensing, certification, or adoption purposes or to respond to inquiries by the subject of the CORI.

(b) Inquiries regarding the CORI, made by the subject of the CORI, should be referred to the DOJ.

(c) Any background check performed by an entity for employment, licensing, certification, or adoption purposes that incorporates CORI shall not be reproduced for secondary dissemination to any other entity.

(d) No entity shall solicit or receive CORI from any other entity in response to a background check requested by the other entity.

Note: Authority cited: Section 11077, Penal Code. Reference: Sections 11075-11081, 11105, and 13202, Penal Code.

CCR, Title 11, Division 1, Chapter 7, Article 1, Section 705.

~~Review~~Storage of Criminal Offender Record Information.

(a) CORI received by an entity for employment, licensing, certification, or adoption purposes shall not be retained by the entity beyond the time necessary to satisfy the purpose for which it was requested unless otherwise provided by law.

(b) CORI received by an entity for employment, licensing, certification, or adoption purposes shall be maintained in a secure area with adequate physical security to preclude access by any unauthorized entity personnel. CORI obtained for employment, licensing, certification, or adoption purposes must be stored separately from an applicant or employee personnel file.

(c) Any entity authorized to receive CORI shall keep a record identifying persons who may access CORI and each date that CORI is accessed by an authorized person. The record shall be retained and available for inspection by the DOJ for a period of not less than three years from the date the CORI is received by the entity.

Note: Authority cited: Section 11077, Penal Code. Reference: Sections 11075-11081, 11105, and 13202, Penal Code.

CCR, Title 11, Division 1, Chapter 7, Article 1, Section 706.

~~Protection of Criminal Offender Record Information~~Regulatory or Other Entity Compliance.

(a) The DOJ may conduct unannounced site inspections and/or scheduled audits of any regulatory or other entity that maintains or receives CORI to ensure compliance with these regulations.

(b) The DOJ shall have full access to the terminals, equipment, statistical data, reports, lists of agencies, files, and record(s) related to the access, handling, dissemination, storage, or destruction of CORI of any regulatory or other entity that maintains or receives CORI during a site inspection and/or scheduled audit.

(c) The DOJ may investigate any violation of this article including investigation of system misuse of CORI. The DOJ may provide the results of any investigation in writing to the entity. The entity shall return a written assessment of the investigation and a statement of corrective action to the DOJ when requested. If the written assessment and statement of corrective action does not comply with this article, the DOJ may take appropriate action as set forth in subdivision (d). The DOJ shall notify the entity of its action in writing.

(d) In the event of any violation of this article, the DOJ, in addition to any other remedies authorized by law, may take any or all of the following actions:

(1) Revocation of the entity's Custodian of Records certification;

(2) Suspension of the entity's access to CORI for a specified period of time and/or for a specified purpose;

(3) Revocation of access to CORI.

Note: Authority cited: Section 11077, Penal Code. Reference: Sections 11075-11081, 11105, and 13202, Penal Code.

CCR, Title 11, Division 1, Chapter 7, Article 1, Section 707.

~~Automated Systems~~Law Enforcement and Criminal Justice Agency Compliance.

~~(a) Automated systems handling criminal offender record information and the information derived therefrom shall be secure from unauthorized access, alteration, deletion, or release. The computer system and terminals shall be located in secure premises. Non-criminal justice agencies shall not receive criminal offender record information directly from an automated criminal justice system.~~

~~(b) Record checks shall be conducted on all personnel hired after July 1, 1975, who have access to the computer system, its terminals, or the stored criminal offender record information.~~

~~(c) Each authorized agency shall keep a record of each release of criminal offender record information from the automated system. The record shall be retained and available for inspection for a period of not less than three years from the date of release. This record shall contain the date of release, the requesting terminal identifier, the receiving terminal identifier, and the information given.~~

(a) The DOJ may conduct unannounced site inspections and/or scheduled audits of any law enforcement or criminal justice agency that maintains or receives CORI to ensure compliance with these regulations.

(b) The DOJ shall have full access to the terminals, equipment, statistical data, reports, lists of agencies, files, and record(s) related to the access, handling, dissemination, storage, or destruction of CORI of any law enforcement or criminal justice agency during a site inspection and/or scheduled audit, except that a law enforcement or criminal justice agency shall not be required to produce files or records concerning an active law enforcement or criminal justice investigation.

(c) Any violation of this article shall be reported to the DOJ and investigated internally by the law enforcement or criminal justice agency that reported the violation. Any violation involving system misuse shall include a review of the agency's internal processes for securing CORI. The agency shall return a written assessment of the investigation and a statement of corrective action to the DOJ. If the assessment and statement of corrective action does not comply with this article, the DOJ may take appropriate action as set forth in subdivision (d). The DOJ shall notify the law enforcement or criminal justice agency of its action in writing.

(d) In the event of any violation of this article by a law enforcement or criminal justice agency, the DOJ, in addition to any other remedies authorized by law, may take any or all of the following actions:

(1) Issuance of a Letter of Censure;

(2) Suspension of access to CORI for a specified period of time and/or for a specified purpose;

(3) Revocation of access to CORI.

Note: Authority cited: Section 11077, Penal Code. Reference: Sections 11075-11081, 11105, and 13202, Penal Code.

CCR, Title 11, Division 1, Chapter 7, Article 1, Section 708.

Destruction of Criminal Offender Record Information.

~~(a) When criminal offender record information is destroyed, the destruction shall be carried out to the extent that the identity of the subject can no longer reasonably be ascertained. When criminal offender record information is destroyed outside of the authorized agency, a person designated by the agency shall witness the destruction.~~

~~(b) (Reserved)~~

~~(c) Printouts of criminal offender record information obtained through system development, test, or maintenance shall be destroyed at the completion of the function or purpose for which the printout was obtained.~~

(a) When an entity determines that there is no need to retain CORI, CORI maintained in hard copy format shall be destroyed by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means, in a manner compliant with the Destroy method in Appendix A of the United State's Department of Commerce National Institute of Standards and Technology (NIST) Special Publication 800-88 Revision 1, "Guidelines for Media Sanitization" (publication date, December 2014), which is incorporated by reference herein. The entity shall maintain written documentation of the steps taken to destroy digital media. The documentation shall be retained and available for inspection by the DOJ for a period of not less than three years. When CORI maintained in hard copy format is to be destroyed by an agency or entity other than the agency or entity authorized to receive CORI, the Custodian of Records, or a person designated by the Custodian of Records, of the agency or entity authorized to receive CORI shall be present to witness destruction of CORI.

(b) When an entity determines that there is no need to retain CORI, CORI maintained on digital media shall be destroyed in a manner that makes it unreadable or undecipherable by any means, compliant with the Destroy method in Appendix A of the United State's Department of Commerce National Institute of Standards and Technology (NIST) Special Publication 800-88 Revision 1, "Guidelines for Media Sanitization" (publication date, December 2014), such that there is reasonable assurance that the information cannot be retrieved or reconstructed prior to

disposal or release for reuse. The entity shall maintain written documentation of the steps taken to destroy digital media. The documentation shall be retained and available for inspection by the DOJ for a period of not less than three years. When CORI maintained in digital media is to be destroyed by an agency or entity other than the agency or entity authorized to receive CORI, the Custodian of Records, or a person designated by the Custodian of Records, of the agency or entity authorized to receive CORI shall be present to witness the destruction of CORI.

Note: Authority cited: Section 11077, Penal Code. Reference: Sections 11075-11081, 11102.2, 11105, and 13202, Penal Code.