INITIAL STATEMENT OF REASONS
FOR PROPOSED AMENDMENTS TO THE CRIMINAL OFFENDER RECORD INFORMATION SECURITY REGULATIONS

PROBLEM

The current regulations governing access to criminal offender record information (CORI) are incomplete, as sections have been redacted and repealed over the years. They provide incomplete direction to agencies on the processes and procedures regarding access to and storage, handling, dissemination, and destruction of CORI.

BENEFITS

Amending, repealing, and adopting regulations that govern CORI Security (California Code of Regulations, Title 11, Chapter 7, Article 1, sections 700 through 708) would provide clarification to the procedures for accessing, storing, handling, disseminating, and destroying CORI. Doing so would also standardize these processes and procedures, as well as penalties for non-compliance. Lastly, the new regulations would consolidate information from various documents regarding CORI into a central location, and give those processes and procedures the force of law.

PURPOSE

Section 700: To establish the title, scope, and purpose of the regulations.

Section 701: To define key terms used throughout the regulations.

Section 702: To define the conditions that must be met for an agency to receive access to CORI, personnel who may have access to CORI, and requirements for the physical and virtual storage of terminals that transmit biometric data or receive CORI, as well as to indicate the forms necessary to meet these requirements, Custodian of Records Notification (Form BCIA 8375, November 2014) and Custodian of Records Application for Confirmation (Form BCIA 8374, November 2014), by incorporating them by reference.

Section 703: To specify that each authorized agency must acknowledge compliance with the regulations outlined in this article and to incorporate the required compliance agreement documents, California Law Enforcement Telecommunications System Subscriber Agreement (Form HDC 0001 Revised 03/20/2010) and Applicant Fingerprint Response Subscriber Agreement (Form BCII 9005 Revised 01/2009), by reference in the regulations.

Section 704: To define to whom CORI may and may not be disseminated and for what purposes it may be used.

Section 705: To define the conditions under which CORI can be retained and requirements for storage of CORI and tracking when and by whom CORI is accessed.

Section 706: To define how the Department of Justice (DOJ) may ensure that non-law enforcement authorized agencies maintain compliance with the regulations and the investigation and consequences of non-compliance.

Section 707: To define how the DOJ may ensure that law-enforcement authorized agencies maintain compliance with the regulations and the investigations and consequences for non-compliance.

Section 708: To define when and to what extent CORI should be destroyed by an authorized agency and to indicate the National Institute of Standards and Technology (NIST) documents incorporated by reference in the regulation.

NECESSITY

Section 700: This section is necessary to explain that the DOJ maintains and furnishes CORI under specific cited provisions of the Penal Code (PC), as well as the scope of CORI dissemination to various law enforcement agencies, criminal justice agencies, and other authorized entities. This section is also necessary to describe the mandated uses, storage and destruction of CORI under current law.

Section 701: This section is necessary to define the key terms used in the regulations and in the explanations of the regulations. Subsections (c) – (e) are stricken because they were repealed in 1985 pursuant to Government Code (GC) section 11349.7. The new definitions are being added to reflect new provisions that are being added to the regulations. The definition of "DOJ" is being added to clarify that this term encompasses all individuals acting under the authority of the Department of Justice. The definition of "criminal offender record information" or "CORI" is being added to explain exactly what information is classified as CORI and to provide necessary examples to the public so that it is clearly understood what is included within this protected information. The definition of "entity" is being added to explain that this term will represent any person or agency authorized to receive CORI and specifies how such persons or agencies may become authorized. The definition of "law enforcement agency" is being added to clearly identity which individuals or groups fall within the scope this type of organization and the definition of "criminal justice agency" was expanded to more precisely describe this type of organization in the context of "law enforcement agency" and "entity." These types of organizations have different standards dedicated to their oversight in the proposed regulations. The definition of "custodian of records" is being added to specify that this title represents the designation of an individual who has been deemed to be responsible for the handling of CORI. Such individuals are subject to the standards dedicated to their oversight in the proposed regulations. The definition of "background check" is being added to explain what the information prohibited from dissemination under the proposed regulations contains and to provide a description of the process that non-exempt individuals must undergo before being authorized to receive CORI. The definition of "regulatory or other entity" is being added to provide a clearly defined separation between law enforcement or criminal justice agencies and entities that fall outside of that category and are thus subject to separate and specific oversight standards in the proposed regulations. The definition of "system misuse" is being added to clarify what actions constitute this violation of CORI handling procedures. The definition of

"authorized person or agency" no longer needs to be defined because the pertinent part of section 702 that included the term has been stricken.

Section 702: This section is necessary to ensure that law enforcement agencies or criminal justice agencies or entities receiving CORI understand the responsibilities they must meet when accessing and securely storing CORI. The changes to the existing section reflect the repeal of subsections (a), (b) and (d) in 1985 pursuant to GC section 11349.7, and the additional requirement by the DOJ that a Custodian of Record be identified by each agency and properly pass a state and federal background check. This section is also necessary to identify the forms that must be used to meet these requirements, Custodian of Records Notification (Form BCIA 8375, November 2014) and Custodian of Records Application for Confirmation (Form BCIA 8374, November 2014), by incorporating them by reference. The additional requirements added to the section give guidance to CORI recipients as to the necessary measures to be taken to safeguard CORI when it is in their possession. The previous language explaining the audit procedure has been moved to section 706 of the Regulations.

Section 703: This section is necessary to clarify changes in the laws governing the handling of CORI by law enforcement agencies, criminal justice agencies, or other entities that receive CORI from the DOJ. The sections stricken out have been removed because the applicable law was repealed in 1985 pursuant to GC section 11349.7 or because the DOJ has clarified and updated the procedures used to ensure that all persons who are authorized to maintain, receive, and access CORI are subject to state and federal level background checks. The addition of the requirement to sign and return the Telecommunications System Subscriber Agreement (Form HDC 0001) and Applicant Fingerprint Response Subscriber Agreement (Form BCII 9005) ensures that CORI recipients have acknowledged the responsibilities and the consequences for improperly storing or misusing CORI.

Section 704: This section is necessary to provide guidance to law enforcement or criminal justice agencies to ensure that CORI is used for the purpose for which it was requested. This section clearly explains prohibitions placed on sharing the CORI between agencies under the applicable PC sections, and makes clear the disclosure rules for disseminating the information to the subject of the CORI.

Section 705: This section is necessary to clarify how long law enforcement or criminal justice agencies or entities can keep CORI and how it is to be safely stored. A record of authorized persons at an agency or entity who may access CORI and each date that the CORI is accessed is required to be maintained to allow the DOJ to fulfill the auditing function outlined in section 706. The DOJ chose the three year retention period after considering the standards of other interstate systems that exchange CORI, including the FBI, as required by section 11077 of the PC.

Section 706: This section moves the auditing function of the DOJ from section 702 and gives to non-law enforcement authorized agencies that are maintaining or receiving CORI specific instructions on what the DOJ will need to access while conducting an audit. Having the ability to comprehensively audit an agency ensures the public trust is met and allows the DOJ to fulfill the statutory requirement given in section 11077 of the PC to control CORI. This section also makes

clear that the consequences of misusing CORI can include revoking and suspending an agency's access to CORI.

Section 707: This section is necessary to ensure law enforcement authorized agencies are in compliance with laws regulating the accessing, handling, storing, dissemination, and destruction of CORI and the consequences if these regulations are not followed. The section was given updated language and previous subsections were struck out to provide a clear separation of compliance for law enforcement or criminal justice agencies from the other entities described in section 706. The updated language also changes this section into an area providing guidance to agencies as to what the DOJ considers to be full access in order to perform audits necessary to fulfill the statutory requirements given in section 11077 of the PC to control CORI. This section prescribes the necessary steps to be taken in the event of a violation of the regulations. This section also makes clear that the consequences of misusing CORI can include revoking and suspending an agency's access to CORI.

Section 708: This section is necessary to reflect the repeal of subsection (b) in 1985 pursuant to GC section 11349.7 and to reflect new technical standards that ensure CORI is destroyed in compliance with the law. The NIST "Guidelines for Media Sanitization" were adopted as the approved destruction method as this represents the current national standard for the destruction of digital media. The three year requirement for the maintenance of written documentation of steps taken to destroy digital media is imposed to reflect the same period of time given in section 705 to allow for auditing by the DOJ.

ECONOMIC IMPACT ASSESSMENT

Creation/Elimination of California Jobs:

The DOJ has determined that the amendments will not create or eliminate jobs in California. The amendments affect only the accessing, storing, handling, dissemination, and destruction of CORI.

Creation/Elimination/Expansion of California Businesses:

The DOJ has determined that the amendments are not expected to create, eliminate, or expand business with the State of California. The regulations are being requested to assist authorized agencies within California by making clear the procedures for the accessing, storing, handling, dissemination, and destruction of CORI.

Benefits to the Public:

The DOJ has determined that the amendments will facilitate the protection of public safety and welfare. Centralizing and consolidating CORI regulations and documents will reduce the time and resources needed by DOJ staff, as well as protect the privacy of the personal CORI of each California resident. The changes will also make the process of using the regulations more open and transparent to the public.

REASONABLE ALTERNATIVES CONSIDERED BY THE DOJ

No reasonable alternatives to the regulations were proposed or identified. The DOJ is required to establish regulations to assure the security of CORI from unauthorized access and disclosures. No reasonable alternative to the regulatory proposal would be less burdensome and equally effective in achieving the purposes of the regulations in a manner that ensures full compliance with PC section 11077. The DOJ determined the proposed regulations will not have a statewide adverse impact on small business, and therefore no alternatives that would lessen the impact were considered.

EVIDENCE SUPPORTING FINDING OF NO SIGNIFICANT STATEWIDE ADVERSE ECONOMIC IMPACT DIRECTLY AFFECTING BUSINESS

The proposed regulatory action will not have a significant adverse economic impact on businesses because the proposed changes establish standards which ensure the security of CORI from unauthorized access and disclosures. These standards apply to a select number of individuals and entities, who are already statutorily mandated to protect CORI, and serve to provide consolidated and centralized guidelines. There are no new requirements in this proposed regulatory action that would be imposed on a business, thus there would be no adverse economic impact directly affecting business.