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.

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. 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.

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 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).

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.

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.