


<p>California Department of Justice CALIFORNIA JUSTICE INFORMATION SERVICES DIVISION Joe Dominic, Chief</p> 	<h1>INFORMATION BULLETIN</h1>	
<p><i>Subject:</i> Applicant Agency CJIS Security Awareness Policy and Training</p>	<p><i>No.</i> 20-05-CJIS</p> <p><i>Date:</i> 04-28-2020</p>	<p><i>Contact for information:</i> Applicant Agency Justice Connection (AAJC) Support Desk (916) 210-3272 AAJCSupport@doj.ca.gov</p>

TO: ALL APPLICANT AGENCIES

Background

On May 30, 2019, Information Bulletin (IB) 19-04-CJIS: *Purpose, Use, and Security of Criminal Offender Record Information (CORI)* was distributed to the community of applicant agencies to provide instruction on the security requirements related to the use, sharing, and maintenance of CORI.

The purpose of this bulletin is to reiterate CORI security requirements and advise all applicant agencies of the California Justice Information Services (CJIS) Division's Security Policy, Security Awareness Training requirement, and forthcoming Security Policy Assessment.

IB 19-04-CJIS is incorporated by reference herein.

CORI Security Requirements

IB 19-04-CJIS outlined four (4) security requirements imperative to the proper use and maintenance of CORI: *Limited Access to CORI, Dissemination/Use of CORI, Data Security, and Adequate Destruction Required*. To ensure continued compliance, all CORI recipients should routinely observe these security requirements and adjust work processes accordingly.

The following is an excerpt from IB 19-04-CJIS:

Limited Access to CORI

- Agency access to CORI is restricted to its custodian of records and/or hiring authority charged with determining the suitability for employment, licensing, or certification of an applicant. The custodian of records is the individual designated by an agency as responsible for the security, storage, dissemination, and destruction of CORI furnished to the agency, and serves as the primary contact for the California Department of Justice (CA DOJ). The CA DOJ must be notified when the designated custodian of records no longer serves in that capacity for the agency/entity.
- CORI is privileged, confidential, and may not be disclosed, except as specifically authorized by law.
- CORI is exempt from disclosure under the California Public Records Act.

Dissemination/Use of CORI

- CORI may only be used for official purposes, and only for the specific purpose for which it was requested and provided.
- CORI may only be disclosed as specifically authorized by law. It may not be reproduced for secondary dissemination, transferred to, or shared with any other employing, licensing, or regulatory entity, or in response to a Public Records Act request. Unauthorized access, disclosure, and/or misuse of CORI is a criminal offense.

Data Security

CORI must be stored in a secure and confidential place (e.g., a locked area, room, file cabinet, or other storage container), with both physical and personnel security controls necessary to prevent unauthorized access and viewing. CORI kept in electronic format must be protected at the same level as physical media. Agency data-security responsibilities also include visitor control and physical access to workspaces, etc.

Adequate Destruction Required

- If the purpose for CORI access no longer applies, the agency must notify the CA DOJ as soon as possible that it is no longer interested in receiving subsequent arrest and disposition notifications, and, consistent with regulations, destroy any CORI in such a manner that the identity of the subject can no longer be ascertained. Secure disposal or destruction of physical media, including shredding or incineration, minimizes the risk of unauthorized access or use of CORI.
- All agencies and organizations must ensure the disposal or destruction is witnessed or carried out by authorized personnel. If hard copy document maintenance services, or other noncriminal justice administrative functions, are performed on behalf of the agency, the authorized agency/entity must ensure that the contractor does not have uncontrolled access to the CORI.

For a complete list of policy, statutory and regulatory references please refer to the citations in IB 19-04-CJIS.

CJIS Security Awareness Training

As an agency or organization that receives CORI to determine the suitability of an applicant for employment, licensing, or certification purposes, all personnel with access to CORI are required to successfully complete a certification exam before CORI may be accessed and take a re-certification exam every two years.

To facilitate compliance with this policy, the CA DOJ utilizes an online testing system called 'CJIS Online.' The training is self-paced and is not timed. Access and instructions are available on the AAJC portal.

CJIS Security Policy Assessment

To enhance and standardize the protection of CORI, the CA DOJ will begin to collect, from each agency or organization authorized to receive CORI, pertinent information about current policies, practices, and procedures in use by CORI recipients. This information will be collected through a CJIS Security Policy Assessment Survey and will be facilitated by the AAJC Support Desk 90 days from the date of this bulletin.

If you have any questions about the information contained within this bulletin, contact the AAJC Support Desk at (916) 210-3272 or AAJCSupport@doj.ca.gov.

Sincerely,



JOE DOMINIC, Chief
California Justice Information Services Division

For XAVIER BECERRA
Attorney General