Department of Justice

Research Request Packet for Access to Criminal Offender Record Information

Pursuant Penal Code 13202

January 2017

Research Request Packet for Access to Criminal Offender Record Information

Contents

Introduction..... i

Conditions for Release of Criminal Offender Record Information..... 1

Research Project Outline - Curriculum Vitae..... 3

Criminal Offender Record Information Data Security Checklist.....5

Introduction

Pursuant to Penal Code section 13202, every public agency or bona fide research body concerned with the prevention or control of crime, the quality of criminal justice, or the custody of correction of offenders may access Criminal Offender Record Information (CORI). This packet contains important information about CORI and the mandatory forms that must be completed before your team can begin receiving CORI data. You must adhere to the Conditions for Release of Criminal Offender Information form. This form has detailed instructions regarding the use of CORI.

Once the packet has been completed in its entirety, please mail all documentation to:

Department of Justice
Criminal Offender Record Program
P.O. Box 903417, Room H100
Sacramento, CA 94203-3870

For questions at any time during this process, you may call the Criminal Offender Record Program at (916) 210-4025 or email coriresearch@doj.ca.gov.

Department of Justice
California Justice Information Services Division

Conditions for Release of Criminal Offender Record Information

Criminal offender record information (CORI) may be released to public agencies or bona fide research bodies provided that the data is used only for research and statistical purposes pursuant to California Penal Code (PC) section 13202 and subject to the conditions listed below. CORI is defined in PC section 11077 as records and data compiled by criminal justice agencies for the purpose of identifying criminal offenders and for maintaining a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release. The California Department of Justice (DOJ) database which contains CORI is the Automated Criminal History System.

1. Requests must be in writing and must specify the intended use for the data. All research requests must be accompanied by a written request to produce copies of any records as specified in condition #5, and by a security plan as specified in condition #6.

2. When CORI is to be obtained by a law enforcement or criminal justice agency via the California Law Enforcement Telecommunications System for a research project, access shall be by authorized agency staff during low traffic hours.

3. The public agency or bona fide research body receiving CORI is responsible for the care and security of the records. The public agency or bona fide research body receiving CORI will not receive personal identifiers such as name of subject, Federal Bureau of Investigation (FBI) number, State Identification (SID) number, social security number, driver's license number and California Department of Corrections (CDC) number unless there is a demonstrated compelling need for this information. The need for personal identifying information shall be in writing and will be reviewed on a case by case basis.

4. All staff members from any public agency or bona fide research body who have direct or indirect access to CORI provided by the DOJ for research must complete a fingerprint background check and are required to sign the Researcher Security and Disclosure Form provided by the DOJ; including but not limited to research staff, IT staff, and system administrators.

5. The public agency or bona fide research body receiving CORI is strictly prohibited from using the data for any purpose other than the purpose for which the data was provided. The public agency or bona fide research body shall not produce copies of CORI provided by the DOJ unless specified in the data security plan. CORI obtained from the DOJ is confidential and, under penalty of law (PC section 11142), may not be disseminated to a third party.

6. The public agency or bona fide research body must take reasonable precautions to protect CORI from unauthorized access. The public agency or bona fide research body is required to submit to the DOJ a detailed plan of the security measures in place to guard against unauthorized access of hard copies or electronic files containing CORI. Please refer to the attached Criminal Offender Record Information Data Security Checklist document for additional information and guidelines regarding the security of CORI.

7. It is incumbent upon the public agency or bona fide research body to prevent disclosure of CORI from unauthorized users throughout the duration of the research project and to immediately report any security breach to the DOJ.

8. The public agency or bona fide research body receiving CORI must destroy the CORI in accordance with California Code of Regulations (CCR) section 708 (a) of Chapter 7 of Division 1 of Title 11 after

the research project is completed. When the CORI is furnished in an electronic format, the CORI must be deleted from any electronic storage medium in which it was stored after the research project is completed. The medium, by which the information was furnished, such as a disc or tape, must be destroyed or disabled so that any access to the information is not possible. Any hard copies made from electronic records must be destroyed in accordance with section 708 (a) of Chapter 7 of Division 1 of Title 11 of the CCR. The DOJ must be notified in writing (for address, see condition #10) of the destruction of electronic or hard copy records, including the deletion of electronic records.

9. Periodic unannounced site inspections and scheduled audits may be performed by the DOJ to ensure compliance with the DOJ's policies and regulations.

10. When data derived from criminal offender record information records is used or referenced in any publication, a copy of that publication must be furnished to:

California Department of Justice
Bureau of Criminal Information and Analysis
Criminal Offender Record Program
P.O. Box 903417, Room H100
Sacramento, CA 94203-4170
coriresearch@doj.ca.gov

11. A public agency or bona fide research body is required to notify the DOJ when a team member is added or removed from the research project.

12. The public agency or bona fide research body is required to notify the DOJ once the project has been completed.

I have read and understand the preceding Conditions for Release of Criminal Offender Record Information. I understand that failure to comply with these conditions may result in the loss of access to criminal offender record information for this and/or future research projects, and that the DOJ reserves the right to revise these conditions, or impose additional conditions, at any time it deems necessary to protect the confidentiality and security of information maintained by the DOJ.

SIGNATURE	DATE
PRINTED NAME	POSITION

NAME OF PUBLIC AGENCY/RESEARCH ORGANIZATION

RESEARCH PROJECT OUTLINE
CURRICULUM VITAE

Please answer the following questions in the space provided. All information must be typed. You may attach a more detailed project description if you choose.

Agency Name:

Contact Person:

Address:

Project Title:

Anticipated Completion of Project or Report:

Nature and Purpose of Project or Report:

Analysis plan or methodology, including proposed use of criminal history records:

Expected benefits and procedures of the projects:

RESEARCH PROJECT OUTLINE
CURRICULUM VITAE

Justification for requesting personal identifying information (name of subject, Federal Bureau of Investigation number, State Identification number, social security number, driver's license number or California Department of Corrections number):

Please detail the security measures your organization has in place to guard against unauthorized access of hard copies or electronic files containing CORI:

Criminal Offender Record Information Data Security Checklist

The public agency or bona fide research body planning to store Criminal Offender Record Information (CORI) in a computer system is responsible for the integrity and security of the information. Systems or networks containing CORI must be segmented from other applications, with controlled and limited access. It is incumbent upon the public agency or bona fide research body to ensure that their system or network remains secure throughout the duration of the research project.

1. Architecture of Criminal Justice Information System (CJIS)

Actively manage (inventory, track, restrict, and correct) all hardware and software so that only authorized assets have access to and can execute on the network.

1.1 Criminal Justice Information Technology (CJIT) associated with processing CORI shall be isolated in a protected network zone (firewalled network segment), access to CORI shall be restricted to authorized users only, and the zone controls shall be implemented in a manner to prevent secondary dissemination. ☐

1.2 Procedures shall be implemented and followed to control the installation of hardware and software within the protected zone, and an inventory of the zone CJIT shall be maintained. ☐

1.3 Development, testing, and operational zones shall be separated to reduce the risks of unauthorized access or changes to the operational environment. ☐

2. Secure Configurations of Hardware and Software

Establish, implement, and actively manage the security configuration of laptops, servers, and workstations using a rigorous configuration management and change-control process.

2.1 Organizations shall establish and appropriately protect and validate source code within a secure development environment. ☐

2.2 Testing of security functionality shall be carried out during software development and network architecture and implementation. ☐

2.3 Information systems shall be regularly reviewed and tested for compliance with the organization's information security policies and standards. ☐

3. Continuous Security Evaluations and Malware Defenses

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and control the installation and spread of malicious code.

3.1 Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. ☐

3.2 Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness. ☐

3.3 All employees of the organization and relevant contractors shall receive appropriate awareness education, training, and regular updates in organizational policies and procedures. ☐

4. Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

4.1 User provisioning and the allocation and use of privileged access rights shall be restricted and controlled. Asset owners shall review users' access rights at regular intervals and adjust as required. ☐

4.2 The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled. ☐

Criminal Offender Record Information Data Security Checklist *(continued)*

5. Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

5.1 Event logs recording user activities, exceptions, faults, and information security events shall be produced and kept, protected from alteration, and regularly reviewed. ☐

6. Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

6.1 A policy on the use of cryptographic controls and key management shall be developed and implemented. ☐

6.2 Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization. ☐

7. Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure to quickly discover an attack and to effectively contain the damage.

7.1 Information security events shall be reported through appropriate management channels as quickly as possible, assessed, and decided if they are to be classified as information security incidents. ☐

7.2 The organization shall define and apply procedures for the identification, collection, acquisition, and preservation of information that can serve as evidence. ☐