Fingerprint-Based Background Check Responsibilities for Non-Criminal Justice Agencies and Users

Version 1.2

Hawaii Criminal Justice Data Center

March 20, 2014

Table of Contents

I. Introduction and Background

On October 9, 1998, President Clinton signed into law the National Crime Prevention and Privacy Compact Act of 1998 (Compact) United States Code, (U.S.C.) Title 42, Chapter 140, Subchapter II, Sections 14611-14616. The Compact facilitates electronic information sharing among the Federal Government and the states and permits the exchange of criminal history records by non-criminal justice agencies (NCJAs) for noncriminal justice purposes when authorized by federal or state law.

In the beginning, NCJAs were primarily governmental entities or any subunits that provided services for purposes other than for the administration of criminal justice. Increasingly, NCJAs are also nongovernmental entities that are authorized by federal and state law to conduct national and state criminal history record checks.

The Compact established the Compact Council in 1998 and authorized it to set the rules, procedures and standards for the use of Interstate Identification Index (III), which is the national criminal history record information system, for noncriminal justice purposes. The Compact Council has the authority to establish rules, procedures, and standards for the interstate and Federal/State exchange of criminal history records. The Compact's standards include, but are not limited to, assessing participation requirements and monitoring the continual maintenance and security of criminal history information.

There are a number of responsibilities associated with access to III. Agencies need to ensure they are compliant with FBI Criminal Justice Information System (CJIS) policies and procedures. Access to the system requires agencies to be in compliance with the CJIS Security Policy.

As the CJIS Systems Agency (CSA) for the State of Hawaii, The Hawaii Criminal Justice Data Center (HCJDC) is here to help you if you have any questions or concerns. Please do not hesitate to contact the Help Desk at (808) 586-2547 for assistance.

II. Agency Responsibilities

A. TAC Designation

Each user agency is required to designate a Terminal Agency Coordinator (TAC). The TAC acts as a liaison between the agency and the State CJIS Systems Officer (CSO). The TAC is appointed by the local agency head for monitoring system use, enforcing system discipline, and ensuring proper procedures are followed within their agency. Please refer Appendix A for more detailed information about TAC responsibilities. The TAC will also serve as the audit contact person to coordinate audit related activities.

B. LASO Designation

Each user agency is required to designate a Local Agency Security Officer (LASO). The LASO acts as a liaison between the agency and the CSA Information Security Officer (ISO) to provide assistance in ensuring the confidentiality, integrity and availability of criminal justice information on the network. The LASO can also be designated as the assigned TAC. The LASO will be responsible for the following:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.

2. Identify and document how the equipment is connected to the state system.

3. Ensure that personnel security screening procedures are being followed as stated in this policy.

4. Ensure that approved and appropriate security measures are in place and working as expected.

5. Support policy compliance and keep the CSA ISO informed of security incidents. LASOs shall notify the CSA ISO of incidents and compromises at their agency.

6. Perform installation and troubleshooting for software needed to access criminal history record information systems.

7. Notify CSA of any incidents and compromises at the local level. See Appendix B for guidance of the information that should be collected and reported.

C. Billing

NCJAs are billed monthly by the HCJDC based on the number of fingerprint cards submitted for national and state criminal history record checks. The cost is $16.50 for each national criminal history record check and $30 for each state criminal history record check. There is also a $5.00 fee for each inked fingerprint card that is scanned by the HCJDC staff for electronic submission to the FBI.

D. Audits

Periodic audits will be conducted for every user agency to ensure compliance with State and FBI CJIS policies and regulations. Such compliance audits shall cover the following areas:

1. Security: This portion of the audit is a security compliance assessment. It includes areas such as ensuring that the agency/organization protects its information against

unauthorized access, ensuring confidentiality of the information in accordance with applicable laws and FBI CJIS policy, regulations, and standards.

2. Compliance Review: This portion of the audit is a user compliance assessment. It includes areas such as ensuring that all information obtained and/or released is in accordance with applicable laws and regulations, a record of dissemination of criminal history records is maintained, and other user related reviews.

E. Outsourcing

If any administrative functions related to the access and usage of III information is contracted to an outside non-governmental agency, a contract must be executed between the user agency and the contractor that meets the Security and Management Control Outsourcing Standard. The contract must be approved by the State or FBI compact officer prior to allowing the contractor access to III information.

III. User Responsibilities

A. Criminal History Record Information (CHRI)

The data stored in III is documented criminal justice information and must be protected to ensure correct, legal, and efficient dissemination and use.

CHRI obtained under the authority of the Compact, may be used solely for the purpose requested and cannot be disseminated outside of the receiving departments, related agencies, or other authorized agencies. All non-criminal justice agencies accessing CHRI shall be subject to all FBI operational policies, rules, and regulations. The NCJA must abide by all other policies and procedures established by the FBI with regard to the access, use, and dissemination of CHRI for non-criminal justice purposes.

B. Security Awareness

Security awareness is an integral part of protecting the systems and information obtained from III from security infractions and improper dissemination. Users are expected to be informed of security issues involved with these systems and to fulfill the requirements set forth in Section 4.3 of the CJIS Security Policy. Authorized users shall access the FBI CJIS Systems and disseminate III data only for the purposes for which they are authorized.

Security Awareness training is required every 2 years and will be provided by the CSA via in-person or on-line sessions.

C. Physical and System Security

Users are responsible for ensuring that access to the systems and storage of the III data is secure.

1. Physical security includes:
   a. Face monitors away from windows, doors and hallways.
   b. Have computers in a controlled area.
   c. Escort all visitors in computer areas.
   d. Criminal history information is stored on a flash drive or CD, or is sent in an email, the data must be encrypted or protected by password.
   e. Store hard copies in a secure or locked area.

2. System security includes:
   a. Protect passwords to the computer and to the applications.
   b. Lock computers when stepping away for any length of time.
   c. Watch for shoulder surfing.
   d. Beware of persons who try to get information over the phone that would allow them access to the system, computer or confidential information.

D. Chain of Custody

The NCJA should ensure that they and their Contractors employ processes to protect the integrity of the applicant's fingerprints when taken.

1. Establish provisions to manage both manually and electronically captured fingerprints.

2. Establish a tracking system (applicant log) using the name or some other means to identify the person taking the fingerprints and verifying the applicant's identity.

3. Establish a procedure that documents the type of identification used by the applicant.

4. Implement the use of forms which may include:
   a. Date of fingerprinting
   b. Reason for fingerprinting
   c. Printed name, signature and/or identification number of the fingerprints
   d. Name of employee's supervisor
   e. Supervisor's signature
   f. Address of agency to receive fingerprints
   g. Name of agency and address where fingerprinting was performed
   h. Type of fingerprint capture

i. Applicant's disclosure information
j. Applicant's consent to the procedure

E. Dissemination Logging (Internal-optional & External-required)

Any information obtained from III for someone outside of the user's agency/program, must be maintained in a secondary dissemination log to document this dissemination. The secondary dissemination log should contain at least the name and agency of the person receiving the information, record being disseminated, reason and purpose of dissemination, and the date. The secondary dissemination log must be maintained for at least 12 months and be available upon request by HCJDC or the FBI Audit Unit.

Dissemination to another agency is authorized if the other agency/program is:

1. An authorized recipient of such information (i.e., a law enforcement agency) and is being serviced by the accessing agency, or

2. Consistent with the Related Agency Doctrine. See Appendix C. (Contact the CSA prior to disseminating CHRC using this doctrine.)

It is essentially the user's responsibility to ensure that the person/agency is authorized to receive the information.

Users are also encouraged to keep their own personal log with as much detail as needed for them to accurately recall the reasons why the fingerprint-based background check was performed. During agency audits, they will be required, upon request, to provide the reason and purpose of inquiries that were made; an internal log would assist them greatly during the triennial audit process.

F. Destruction of Criminal History Record Check Copies

If copies (paper or electronic) are maintained they must:

1. Have secure storage;

2. Be key elements for the integrity/utility of the case file; and

3. Be shredded, incinerated or degaussed, whichever is appropriate, when the copy is no longer needed.

G. Compliance Review Audit

Users must ensure the systems are accessed for purposes consistent with their job responsibilities and that if a request is received for criminal justice information, the user ensures that the person requesting the information is authorized to receive the data.

Every three (3) years, the HCJDC is required to conduct an audit of NCJAs. The compliance review audit is conducted on fingerprint-based background check requests that are performed. For this review, a random list of fingerprint transactions is generated from the system logs, and users are required to verify that they did initiate the transaction. The review also involves verifying the reason and purpose for the fingerprint-based check, and ensuring the correct Reason Fingerprinted is being used.

Users should not perform background checks to access criminal history information on themselves; this is considered misuse and is a sanctionable offense.

IV. CSA Responsibilities

The Hawaii Criminal Justice Data Center is the CSA for the State of Hawaii. The CSA responsibilities include:

1. Maintaining and monitoring the systems needed to assure 24x7 availability and access to national and State CHRI.

2. Making the necessary upgrades and changes to all systems and software needed for access to national and state CHRI.

3. Supporting all agencies and their users with any questions or concerns they may have about III and CJIS-Hawaii via the HCJDC Help Desk.

4. Conducting training for the various agencies upon request.

5. Enforcing all system security regulations as determined by State and FBI policies with regard to all agencies we serve.

6. Conducting triennial agency audits of all authorized NCJAs in the State of Hawaii.

Appendix A

Terminal Agency Coordinator (TAC) Responsibilities for Agencies Conducting Fingerprint-Based Criminal History Record Checks

Major Responsibilities:

1. Ensure compliance with FBI and state policies, rules and regulations. The Terminal Agency Coordinator (TAC) is responsible for familiarizing him/herself with FBI and state policies, rules and regulations in order to ensure that all of the agency's users that have access to criminal history record information are in compliance. This information can be found in the CJIS Security Policy, each agency's agreement and Hawaii Revised Statutes.

2. On-scene expert in policy and procedures.

3. Liaison with the State/Federal CSO and other local TACs.

4. Provide input into state and national systems.

5. Be responsible for ensuring that all authorized users:

    a. Obey all security rules and regulations as defined in the CJIS Security Policy.

    b. Secure their terminals as appropriate in order to prevent unauthorized access.

    c. Make sure that printed or copied criminal history record information, in any form, is properly stored and destroyed when no longer needed.

    d. Use properly formulated robust passwords to secure and protect their access.

    e. Conduct correct, legal, efficient and protected dissemination of criminal history record information obtained.

    f. Maintain required dissemination logs.

Appendix B

Identifying Security Incidents

A security incident is any act or circumstance that involves FBI CJIS Data that deviates from the requirements of the FBI CJIS Policy or state and Federal governing statutes. For example: compromise, possible compromise, inadvertent disclosure, and deviation.

DO NOT POWER DOWN THE SYSTEM.

The following is a partial list of incident indicators that deserve special attention from users and/or system administrators:

1. The system unexpectedly crashes without clear reason.
2. New user accounts are mysteriously created which bypass standard procedure.
3. Sudden high activity on an account that has had little or no activity for months.
4. New files with novel or strange names appear.
5. Accounting discrepancies.
6. Changes in file lengths or modification dates.
7. Attempts to write to system files.
8. Data modification or deletion.
9. Denial of service.
10. Unexplained poor system performance.
11. Anomalies.
12. Suspicious probes.
13. Suspicious browsing.

These indicators are not proof that an incident has or is occurring. However, it is important to suspect that an incident might be occurring and act accordingly.

Incident Report Information

The following is information that must be reported to the HCJDC through the Agency LASO regarding any security incident:

1. Description of the incident and activities.
2. How was the incident discovered?
3. Who does the incident affect?
4. When did the incident occur?
5. Why did the incident happen?
6. Where did the incident occur?
7. Describe resolutions which have been identified.
8. What are the vulnerabilities and impacts associated with this incident?
9. What is being done to see this does not happen again?

Appendix C

Related Agency Doctrine

The CJIS Security Policy defines "Related Agency Doctrine" as "a legal principal providing for the re-dissemination of CHRI by an authorized recipient. Agencies that have a commonality of purpose and (typically) congruent responsibility authorized by federal statute or executive order, or approved state statute pursuant to Pub. L. 92-544, can receive CHRI and exchange that information with each other for the authorized purpose originally requested." The agencies must have a unity of purpose and typically, concurrent regulatory responsibility.

If a board or association for the state has approved statutory authority to receive information for licensing/employment and an additional entity is part of the licensing/employment process, that entity is allowed access to the CHRI for adjudication and/or final decision. For example, if the Board of Education is authorized to receive CHRI for teacher employment purposes, and the final suitability decision is made by the Department of Education Personnel Office, the Board may disseminate the CHRI to the Personnel Office.

Authorized recipients (state and local governmental agencies and their governmental subunits that review FBI identification records to make employment and licensing suitability determinations) cannot share CHRI across state lines. There is no related agency or commonality of purpose across state lines. The term "related agencies" does not apply to out-of-state governmental agencies.

Important: Please contact the CSA prior to disseminating CHRI under this doctrine.