CRIMINAL HISTORY RECORD CHECKS FOR NON-CRIMINAL JUSTICE PURPOSES POLICY AND MANUAL

Version 2.1

August 2019

Hawaii Criminal Justice Data Center

CHANGE GUIDE

Revision	Change Description	Sections	Date
2.0	Policy and Manual Rewrite	All	October 2017
2.1	Revised FBI Name Check Policy and Procedures Added Civil Rap Back Service Policy Removed Appendix E	8.7.3 10 Appendix E	August 2019

Table of Contents

1 INTRODUCTION AND BACKGROUND

This section describes the purpose of this manual, background information of the Hawaii Criminal Justice Data Center (HCJDC), the Federal Bureau of Investigation (FBI), and the CJIS Advisory Policy Board and National Crime Prevention and Compact Council, which is where national polices and regulations regarding access to and security of criminal history record information derive.

1.1 PURPOSE OF THIS MANUAL

The purpose of this manual is to provide users who access criminal history record information for non-criminal justice purposes, such as employment and licensure with clearly defined policies pertaining to the use, retention, security, destruction, and dissemination of both state and national criminal history record information (CHRI) obtained from fingerprint-based criminal history record checks.

This manual supplements the FBI Criminal Justice Information Services (CJIS) Security Policy. Both documents are considered living documents and will be updated as changes in policy, technology, and law occur.

The policies in this manual and the FBI CJIS Security Policy apply to every individual with access to confidential CHRI.

1.2 HAWAII CRIMINAL JUSTICE DATA CENTER

The HCJDC is a division of the Department of the Attorney General and is responsible for the maintenance of the CJIS-Hawaii system, which is the statewide central repository of adult CHRI, the Automated Biometric Identification System (ABIS), the Sex Offender and Other Covered Offender Registration Program, and the Hawaii Integrated Justice Information Sharing Program (HIJIS). Furthermore, the HCJDC serves as the state point of contact for the FBI's National Crime Information Center (NCIC) System and has been designated as the state's CJIS Systems Agency (CSA) by the FBI. The HCJDC also serves as the State Identification Bureau (SIB).

As the central repository, the HCJDC is responsible for the collection, storage, and dissemination of CHRI in such a manner as to balance the right of the public to be informed, the right of privacy of individual citizens, and the necessity for law enforcement agencies to utilize the tools needed to prevent crimes and detect criminals in support of the right of the public to be free from crime and the fear of crime.

Laws governing the dissemination of state CHRI are regulated by Chapter 846, Hawaii Revised Statutes.

1.3 CRIMINAL JUSTICE INFORMATION SERVICES DIVISION, FBI

The CJIS Division is the largest division in the FBI and serves as the national central repository of criminal justice information. The CJIS Division is responsible for an array of criminal justice information systems such as the Next Generation Identification (NGI) System, the NCIC, the National Instant Background Check System (NICS), the Law Enforcement National Data Exchange (N-DEx), and the Uniform Crime Reporting (UCR) program/National Incident-Based Reporting System (NIBRS).

1.3.1 CJIS Advisory Policy Board

The FBI established the CJIS Advisory Process to obtain the user community's advice and guidance on the development and operation of all the CJIS Division systems. The CJIS Advisory Policy Board (APB), which is comprised of 35 representatives from criminal justice agencies, national security agencies and organizations throughout the United States, is responsible for reviewing appropriate policy, technical, and operational issues related to FBI CJIS Division programs and makes recommendations to the FBI Director.

1.3.2 CJIS Systems Agency

The CSA is responsible for planning and providing necessary hardware, software, funding, quality assurance, and training for complete access to all FBI CJIS Division data services by all authorized agencies within the state. The HCJDC has been designated as the CSA for Hawaii.

As the CSA, the HCJDC is responsible for:

- Maintaining and monitoring the systems needed to assure 24x7 availability and access to state and national CHRI;
- Making the necessary upgrades and changes to all systems and software needed for access to state and national CHRI;
- Supporting all agencies and their users with any questions or concerns they may have about the FBI CJIS Systems and CJIS-Hawaii via the HCJDC Help Desk;
- Conducting training for agencies upon request;
- Enforcing all system security regulations as determined by state and FBI policies with regard to all user agencies; and
- Conducting triennial agency audits of all agencies authorized to access state and national CHRI in the State.

1.3.3 CJIS Systems Officer

The CJIS Systems Officer (CSO) is responsible for monitoring system use, enforcing system discipline, and assuring that operating procedures are followed by all users as well as other related duties. The CSO has operational and technical expertise in FBI CJIS Division systems and sufficient authority to represent the state's interest when voting on issues. Ms. Brenda Abaya of the HCJDC currently serves as Hawaii's CSO.

1.4 National Crime Prevention and Privacy Compact Council

National Crime Prevention and Privacy Compact Act (Compact) establishes an infrastructure by which states can exchange criminal records for non-criminal justice purposes according to the laws of the requesting state and provide reciprocity among the states to share records without charging each other for information. The Compact established a Council to promulgate rules and procedures for the effective use of the Interstate Identification Index (III), which contains automated CHRI, for non-criminal justice purposes such as employment and licensing. The Council consists of 15 members who are appointed by the U.S. Attorney General and empowered by Congress.

Hawaii ratified the Compact with the passage of Act 83, Session Laws of Hawaii 2006.

1.4.1 State Compact Officer

Once the Compact is ratified by a state, a person from the state is designated to serve as the State Compact Officer (SCO). The SCO is responsible for administering the Compact within the state, ensuring Compact provisions and rules, procedures and standards set by the Council are complied with in the state, regulating the in-state use of CHRI, and establishing procedures to protect the accuracy and privacy of CHRI. By state statute, the HCJDC Administrator or the HCJDC Administrator's designee serves as the SCO.

1.5 Non-Criminal Justice Agency

Initially, Non-Criminal Justice Agencies (NCJAs) were primarily governmental entities or 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.

For the purpose of this document, NCJAs also include criminal justice agencies accessing criminal history record information for non-criminal justice purposes such as employment, licensing and permitting.

2 CRIMINAL JUSTICE INFORMATION SYSTEMS

This section describes the criminal justice systems used or accessed when processing fingerprint-based state and national criminal history record checks.

2.1 CJIS-HAWAII

CJIS-Hawaii is a statewide criminal justice information system maintained by the HCJDC with data contributed by state and county criminal justice agencies. Criminal history maintained in CJIS-Hawaii is offender-based and verified by fingerprints. Other criminal justice information maintained in CJIS-Hawaii includes the Sex Offender and Other Covered Offender Registry, Temporary Restraining and Protection Orders, DNA Tracking, and Custody and Supervision information.

CJIS-Hawaii also serves as a communication tool to provide criminal justice information to various FBI CJIS Systems.

2.2 AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM

The Automated Biometric Identification System (ABIS) uses digital image technology to obtain, store, and analyze fingerprint and mug photo data for identification and investigative purposes. The system also integrates national latent fingerprint search capabilities, a statewide mug photo database, and facial recognition capability.

2.3 LIGHTS OUT TRANSACTION CONTROLLER

Hawaii has an automated identification process, which uses the Lights Out Transaction Controller (LOTC) to manage a fingerprint search of the state's ABIS and a demographic search of CJIS-Hawaii, in order to make a real-time identification of the subject. Roughly 85% of the time, this process allows positive identification to be made without the need for human intervention.

Through the LOTC, fingerprints are also sent to the FBI for a national search.

2.4 APPLICANT RAP BACK APPLICATION, HIJIS PORTAL

The Applicant Rap Back Application (ARBA), housed within the HIJIS Portal, is the application used by authorized agencies to obtain the identification results of their fingerprint submissions for non-criminal justice purposes. Authorized agencies will also use the ARBA to maintain and manage their non-criminal justice Rap Back subscriptions.

2.4.1 EHAWAII.GOV HIJIS USER ACCOUNT SYSTEM

The eHawaii.gov HIJIS User Account System is the system used to maintain user account information for access to the HIJIS Portal for non-governmental agencies and government agencies that have not established an active directory or another type of agency identity provider system.

2.5 NEXT GENERATION IDENTIFICATION, FBI

The FBI's NGI System provides the criminal justice community with a large and efficient electronic repository of biometric and criminal history information. Fingerprints sent by the state are searched against this system.

2.6 National Crime Information Center System, FBI

The NCIC database consists of the following 21 files: Supervised Release, National Sex Offender Registry, Foreign Fugitive, Immigration Violator, Missing Person, Protection Order, Unidentified Person, Protective Interest, Gang, Known or Suspected Terrorist, Wanted Person, Identity Theft, Violent Person, NICS Denied Transaction, and Stolen Articles, Boats, Guns, License Plates, Parts, Securities, and Vehicles.

When a Universal Control Number of an applicant matches that of someone in the National Sex Offender Registry or Wanted Person file, the national criminal history record check response will include a Caution Alert indicating that the subject is a registered sex offender or may be wanted by law enforcement.

2.7 Interstate Identification Index & National Fingerprint File Program

Often mistaken for an NCIC file, the III System is an index pointer system that ties computerized criminal history record files of the FBI and the centralized files maintained by each participating state into a national system.

The National Fingerprint File (NFF) program calls for the State to become the sole maintainer and provider of its criminal history records. Whereas for non-NFF States, the FBI maintains a duplicate record to meet the needs of federal, state, and local agencies and private entities that use III information for authorized non-criminal justice purposes.

During a national criminal history record check, when an identification is made on a non-NFF State record, the FBI provides a copy of the State record kept on file in the III. The III record may not contain all the CHRI residing at the state repository, such as final dispositions of the charges. On the contrary, when an identification is made on an NFF State record, the FBI reaches out directly to the state repository (i.e., HCJDC/CJIS-Hawaii) for the record, thus providing the most complete CHRI available.

NFF is the final stage of the complete decentralization of criminal history records. Hawaii is a participating NFF State.

3 AUTHORITY TO CONDUCT STATE & NATIONAL CRIMINAL HISTORY RECORD CHECKS

In order to submit fingerprints and receive state and national CHRI for non-criminal justice purposes, the recipient must be authorized by law. Below are some of the most common authorities used in Hawaii.

3.1 PUBLIC LAW 92-544

The FBI is authorized to exchange identification records with officials of state and local governments for the purposes of licensing and employment if authorized by a state statute which has been approved by the U.S. Attorney General. The standards require that the authorization must:

- Exist as the result of legislative enactment;
- Require fingerprinting of the applicant;
- Expressly or by implication authorize use of FBI records for screening the applicant;
- Not be against public policy; and
- Not be overly broad in its scope and must identify the specific category of applicants/licensees.

Fingerprints submitted to the FBI under Public Law 92-544 must be forwarded through the SIB (i.e., HCJDC).

3.1.1 SECTION 846-2.7(b), HAWAII REVISED STATUTES

Section 846-2.7(b), Hawaii Revised Statutes (HRS) serves as Hawaii's umbrella statute for criminal history record checks conducted pursuant to Public Law 92-544. Established in 2003, Section 846-2.7, HRS, addressed inconsistencies and duplicative statutory language authorizing criminal history record checks for employment and licensing purposes.

New subsections added to section 846-2.7(b), HRS, must be approved by the FBI prior to being considered an authorized statute. Upon enactment into law, the HCJDC will request review and approval of the amended 846-2.7(b) from the FBI.

3.2 NATIONAL CHILD PROTECTION ACT, AMENDED BY THE VOLUNTEERS FOR CHILDREN ACT, PUBLIC LAW 105-251

The National Child Protection Act/Volunteers for Children Act (NCPA/VCA) allows qualified entities to contact authorized agencies to request national criminal history record checks on providers who provide care to the vulnerable population. A "qualified entity" means a business or organization, whether public, private, for-profit, not-for-profit, or voluntary, that provides care or care placement services.

NCPA/VCA requires the resulting CHRI be received by an authorized agency. An "authorized agency" means a division or office of a State. The authorized agency is responsible for accessing and reviewing of the state and national CHRI, making the determination on whether the provider has been convicted of a crime bearing upon the provider's fitness to have responsibility for the safety and well-being of the

children, the elderly, or individuals with disabilities, and for conveying the fitness determination results to the qualified entity.

3.2.1 Volunteer & Employee Criminal History Service (VECHS)

Section 846-2.7(c), HRS, establishes Hawaii's VECHS program, which leverages the fingerprint-based national criminal history record check authorized by NCPA/VCA by requiring the applicants to sign a consent and waiver form, which in turn, allows the CHRI to be received directly by the qualified entity, which may be a private business or organization.

3.3 Adam Walsh Child Protection and Safety Act, Public Law 111-13

The Adam Walsh Child Protection and Safety Act (Adam Walsh Act) authorizes child welfare agencies to conduct national fingerprint-based criminal history record checks and receive CHRI for individuals under consideration as prospective foster or adoptive parents.

The Adam Walsh Act also allows private or public elementary or secondary schools or a local or state educational agency to conduct national fingerprint-based criminal history record checks and receive CHRI on individuals employed, under consideration for employment, or otherwise in a position in which the individual would work with or around children in the school or agency.

3.4 Edward M. Kennedy SERVE America Act, Public Law 111-13

The Edward M. Kennedy Serve America Act (Serve America Act) expands national service programs administered by the Corporation for National and Community Service (Corporation) by requiring national criminal history record checks for individuals who serve in positions that receive living allowances, stipends, national service educational awards, or salaries from the Corporation. Requirements of the Serve America Act differ based on whether the individual has recurring access to vulnerable populations.

3.5 REAL ID Act, Public Law 109-13

The REAL ID Act requires States to conduct state and national fingerprint-based criminal history record checks on covered employees. Covered employees include individuals involved in the manufacture or production of REAL ID driver's licenses and identification cards, or current employees who will be assigned to such positions.

4 CRIMINAL HISTORY RECORD CHECK START-UP PROCESS

This section details the steps required for an agency to start up and maintain a criminal history record check process.

4.1 NEW AGENCY APPLICATION

Request for access to confidential CHRI must be made to the HCJDC. A letter of request should include the purpose of the request and type of individuals for which criminal history record checks will be conducted (e.g. employees, providers, licensees). If known, reference to the State or Federal law authorizing fingerprint-based state and national criminal history record checks should be included. Once approved, the HCJDC will send your program's information to the FBI for approval and issuance of an Originating Agency Identifier (ORI).

Entities that wish to participate in the VECHS program may view information and obtain the VECHS application form and related documents online at: http://ag.hawaii.gov/hcjdc/vechs.

4.2 ORI ASSIGNMENT

An ORI is a nine-character identifier, assigned by the FBI, and is used to identify authorized agencies and control access to the systems. To qualify for an ORI assignment for non-criminal justice purposes, an agency must be authorized under Public Law 92-544 with an approved state statute or authorized by other federal legislation.

The HCJDC will send a request for an ORI assignment to the FBI on the behalf of the requesting agency. The FBI's typical review time is 60 days.

Every assigned ORI is unique to that agency and the agency's authorized purpose for access to CHRI. For Hawaii, all ORIs begin with the letters "HI". Usually, an ORI used for non-criminal justice purposes will end with the letter "Z".

VECHS qualified entities will not receive an FBI-assigned ORI. Instead, VECHS qualified entities are issued a State-assigned ORI starting with "VECHS". Like the FBI-assigned ORI, all VECHS ORIs are unique to that agency and used for identification and access purposes.

The agency's ORI will be associated with every fingerprint submission and all results from the state and national criminal history record check.

4.2.1 PROPER ORI USAGE

ORIs are approved according to state and federal law, and must only be used for approved authorized purposes. This means a local government agency that has an ORI approved for criminal history record checks on applicants for liquor licenses may not use the ORI to conduct criminal history record checks on its employees. Similarly, an agency with an ORI approved to conduct criminal history record checks on its volunteers and employees that provide care for Hawaii's vulnerable population may not use the ORI to conduct criminal history record checks on volunteers and employees that do not provide care to the vulnerable population.

Prior to submitting requests for criminal history record checks for an additional population, the agency must contact HCJDC. If the criminal history record checks on

the additional population is authorized by state or federal law, the HCJDC will request approval from the FBI on the agency's behalf. The FBI must approve the additional statute prior to the submission of fingerprints.

4.3 User Agreement

The FBI CJIS Security Policy requires that each agency with access to criminal justice information have a current user agreement signed by the agency representative and the HCJDC. The purpose of the user agreement is to provide CHRI to authorized agencies.

The user agreement states that the HCJDC will:

- Act as an intermediary between the agency and the FBI and provide state and national CHRI available to the agency under state and federal law;
- Provide security awareness training;
- Conduct audits to assure compliance with the User Agreement; and
- Cease providing CHRI if the User Agreement is violated or suspected of being violated.

The agency agrees to the following:

- Abide by terms and conditions of the User Agreement;
- Promptly advise the HCJDC of any violations;
- Comply with state and federal laws, rules, regulations, procedures, and policies regarding the use and dissemination of CHRI;
- Use CHRI only for the purpose authorized;
- Provide for the security of the CHRI;
- Obtain and provide the required consent and notifications to each individual fingerprinted;
- Allow the individual an opportunity to challenge and correct the CHRI prior to being adversely affected;
- Keep all records necessary to facilitate a security audit by the HCJDC and/or FBI;
- Allow the HCJDC and/or FBI to conduct audits to assure compliance with the User Agreement; and
- Pay for all applicable fees.

The user agreement is executed on the date the last signature is obtained on the document and continues to be in effect until terminated by either party. The User Agreement may be terminated by one or both parties upon 30-days written notice or immediately upon violation of the terms of the User Agreement.

4.3.1 VECHS User Agreement

The same user agreement requirements stated above are applicable to VECHS agencies with the additional requirement that VECHS agencies must have a completed VECHS Consent & Waiver Form (Form HCJDC-VECHS-02) on file prior to the applicant being fingerprinted. The VECHS User Agreement includes additional wording for the VECHS Consent & Waiver Form requirement.

4.4 Points of Contact

Each agency with direct access to any HCJDC or FBI maintained criminal justice information system and any agency with access to confidential CHRI is required to designate appropriate points of contact.

4.4.1 Terminal Agency Coordinator

The Terminal Agency Coordinator (TAC) should be the person that knows and understands the purpose of conducting the criminal history record check, and who should have access to the resulting CHRI. The TAC acts as a liaison between the agency and the HCJDC and CSO. The TAC is responsible for monitoring system use, enforcing system discipline, and ensuring proper procedures are followed within their agency. The major responsibilities of the TAC include, but are not limited to:

- Being the agency expert in criminal history record check policy and procedures by familiarizing him/herself with all state and federal policies, rules and regulations;
- Liaising with the State, SCO, and other local TACs;
- Ensuring compliance with state and federal policies, rules and regulations;
- Ensuring access to criminal justice systems and CHRI cease when the user's authority is terminated;
- Serves as the point of contact for audits conducted by HCJDC or the FBI;
- Ensuring all authorized users:
    - Comply with all state and federal policies, rules, and regulations;
    - Complete security awareness training as required;
    - Obey all security rules and regulations as defined by the FBI CJIS Security Policy;
    - Secure their terminals as appropriate to prevent unauthorized access;
    - Ensure all printed or copied CHRI, in any form, is properly stored and destroyed when no longer needed;
    - Use properly formulated robust passwords to secure and protect their access;
    - Conduct correct, legal, efficient, and protected dissemination of CHRI obtained; and
    - Maintain dissemination logs.

4.4.2 Local Agency Security Officer

The Local Agency Security Officer (LASO) is the technical contact and acts as a liaison between the agency and the CSA Information Security Officer (ISO) to provide assistance in ensuring the confidentiality and security of criminal justice information on the agency's network. The LASO and the TAC may be the same person. The LASO's responsibilities include, but are not limited to:

- Identifying who is using the CSA approved hardware, software, and firmware, and ensuring no unauthorized individuals or processes have access to the same;
- Identifying and maintaining documents on how the equipment is connected to the State system;

- Ensuring that personnel security screening procedures are being followed as stated in this policy;
- Ensuing that approved and appropriate security measures are in place and working as expected;
- Supporting policy compliance and keeping the CSA ISO informed of security incidents. The LASO shall notify the CSA ISO of incidents and compromises at their agency. See Appendix B for the NCJA Security Incident Reporting Form; and
- Performing installation and troubleshooting for software needed to access criminal justice information systems.

4.5 Security Awareness Training

Security awareness in an integral part of protecting criminal justice information systems and the CHRI obtained from security infractions and improper dissemination and use. Users are expected to be informed of security issues involved with these systems and to fulfill the requirements set forth in the FBI CJIS Security Policy. CHRI shall be accessed and used only for the purpose for which authorized.

Security awareness training is required to be completed prior to receiving access to CHRI and biennially thereafter. The HCJDC will provide security awareness training via on-line sessions.

Each agency and person with access to criminal justice information, including CHRI, is to know and understand that the information is confidential. Improper access, use, and dissemination of any criminal justice information, including CHRI, is serious and may result in administrative sanctions, termination of services, as well as state and/or federal criminal and civil penalties. Each person with access to criminal justice information, including CHRI, has a responsibility to protect the information and report security incidents.

4.6 Application Privacy Rights

The National Crime Prevention and Privacy Compact Council created "Guiding Principles: Agency Privacy Requirements for Non-Criminal Justice Applicants" to advise agencies receiving federal CHRI of their obligation to notify applicants of their rights in accordance with Title 28 Code of Federal Regulations (CFR) 50.12 regarding the exchange of FBI identification records. Agencies are obligated to ensure the applicant is provided certain notice and other information and that the results of the check are handled in a manner that protects the applicant's privacy. CHRI may be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities.

Officials making the fitness determination shall provide the applicant the opportunity to complete or challenge the accuracy of the CHRI. These officials must also advise the applicant that the procedures for obtaining a change, correction, or updating an FBI identification record are set forth in Title 28 CFR 16.30-34. A license or employment should not be denied until the applicant has been afforded reasonable time to correct or complete the record, or has declined to do so.

This policy is intended to ensure that all relevant CHRI is made available to provide for public safety and to protect the interests of the prospective employee or licensee who may be affected by the information, or lack of information in an identification record.

4.6.1 Agency requirements for Applicant Privacy Rights

For each applicant subject to a criminal history record check, prior to obtaining the applicant's fingerprints, the agency must obtain the applicant's:

- Consent to obtain fingerprints and conduct state and FBI criminal history record checks;
- Identifying information required to conduct the criminal history record check such as name, date of birth, height, weight, eye color, hair color, gender, race, and place of birth;
- Statement indicating whether the applicant has ever been convicted of a crime, and if so, the particulars of the conviction; and
- Acknowledgement of receipt of notification of:
    - Retention of the fingerprints by the HCJDC and FBI for all purposes and uses authorized for fingerprint submissions, including participation in the Rap Back program;
    - Right to challenge the accuracy and completeness of any information obtained from the criminal history record check and obtain a determination as to the validity of such challenge before a final determination is made;
    - Procedures for obtaining a change, correction, or updating the CHRI; and
    - FBI Privacy Act Statement.

Each agency should establish and document the process and procedure it utilizes for how and when it gives the applicant notice, what constitutes "reasonable time" for the applicant to correct or complete the record, and any appeal process that is afforded to the applicant. Such documentation will assist State and FBI auditors.

5 Security of and Access to CHRI

Information obtained from the criminal history record check process is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28 Part 20, CFR and Chapter 846, Hawaii Revised Statutes.

5.1 Definition of CHRI

CHRI means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrest, detention, indictment, information, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification such as fingerprint records if such information does not indicate the individuals involvement with the criminal justice system.

Information is considered CHRI if it is transferred or reproduced directly from CHRI and associated with the subject of record. This includes information such as conviction/disposition data as well as identifiers used to index a record regardless of format. Examples of formal and informal products or verbalizations include: correspondence of letters and emails, forms, hand-written notes, and conversations.

Information is considered CHRI if it confirms the existence or nonexistence of CHRI.

5.1.1 Limitations of CHRI

CHRI is compiled from information submitted to the central repository from law enforcement agencies, prosecutors, and courts (contributing agencies). Although the central repository makes reasonable efforts to ensure all information is submitted as required by law, it is not responsible for omissions from the contributing agencies. CHRI may be incomplete or inaccurate.

CHRI is constantly being updated as new arrests and other information are entered into the systems by the contributing agencies.

The arrest warrant file, sex offender registration file, or other databases maintained by the state are not part of the state criminal history record check.

Certain statutes allow for the expungement, suppression, or deletion of records; such information will not be provided in response to a criminal history record check.

The HCJDC maintains records for the state of Hawaii only. Most fingerprinting authorizations include a check through the FBI, which the HCJDC will request on behalf of the agency as a normal part of the criminal history record check, if authorized by law.

5.2 Proper Use of CHRI

CHRI disseminated for non-criminal justice purposes shall be used only for the purposes for which it was given. No agency or individual shall confirm the existence or nonexistence of CHRI to any person or agency that would not be authorized to receive the information itself.

Users shall not perform background checks to access criminal history record information on themselves for training purposes; this is considered misuse of CHRI and is a sanctionable offense.

5.3 Dissemination of CHRI

Dissemination of CHRI includes all forms such as, but not limited to verbal, hard-copy, electronic, email, and facsimile. It is recommended that agencies have a specific policy in place for dissemination to ensure that any and all dissemination is in accordance with state and federal laws.

5.3.1 Subject or Record

The FBI and the state do not object to officials providing a copy of the applicant's criminal history record to the applicant for review and possible challenge when the record was obtained based on positive fingerprint identification. If the agency's policy permits, this courtesy will save the applicant the time and additional State and FBI fees to obtain their record directly. It will also allow for a more timely determination of the applicant's suitability. See Appendix A for Dissemination of CHRI to the Subject of Record procedures.

5.3.2 Related Agency

Agencies that have a commonality of purpose and congruent responsibility authorized by state or federal law can receive CHRI and exchange CHRI with each other for the authorized purpose originally requested. The agency must have unity of purpose and typically a concurrent regulatory responsibility.

If a board or association for the State has approved statutory authority to receive CHRI for licensing/employment and an additional entity is part of the licensing/employment process, that entity is allowed access to CHRI for adjudication and/or final decision. For example, if the Department of Education is authorized to receive CHRI on a prospective teacher for employment purposes, and the final suitability determination decision is made by the Department of Human Resources Development, the Department of Education may disseminate CHRI to the Department of Human Resources Development for final decision of suitability.

Just as with the primary receiving agency, any related secondary recipient must also be authorized to obtain CHRI. For example, a private employer, such as a day care center, may be perceived as having a commonality of purpose; however, since the private day care center is not an authorized agency, the regulating governmental agency authorized to receive CHRI may NOT disseminate CHRI to them.

Agencies may not share CHRI across state lines. There is no related agency or commonality of purpose across state lines.

Agencies are required to contact the HCJDC prior to disseminating CHRI to a related agency.

5.3.3 Dissemination Logs

Authorized agencies are required to maintain dissemination logs for whenever CHRI is secondarily disseminated. Secondary dissemination occurs whenever CHRI is released to another agency or person outside of the agency, including the subject of record.

At a minimum, the following must be included in the log:

- Name and SID and/or UCN of subject of record;

- Name of person releasing the CHRI;
- Name and agency of person receiving the CHRI;
- Reason for releasing the CHRI; and
- Date and method used to release the CHRI.

Dissemination logs may be maintained in either electronic or hard-copy format and must be maintained for a minimum of 12 months. The logs must be made available to the HCJDC or the FBI Audit Unit upon request.

Additionally, users are encouraged to keep their own personal logs with as much detail as needed to accurately recall the reasons why the fingerprint-based state and national criminal history record check was performed. Such optional internal logs may assist the user during agency audits, as he/she will be required to provide the reason and purpose of the fingerprint-based criminal history record check.

5.3.4 Public Hearings/Public Access Requests

CHRI must not be disseminated to the general public. This includes maintaining CHRI in formats that are accessible by the public or within records that are subject to release through public record requests. However, CHRI may be disclosed as part of the adjudication process during a hearing that is open to the public if the agency demonstrates:

- The hearing is based on a formally established requirement;
- The applicant is aware prior to the hearing that CHRI may be disclosed;
- The applicant is not prohibited from being present at the hearing; and
- CHRI is not disclosed during the hearing if the applicant withdraws from the application process.

For example, a board or commission is authorized to access CHRI, and as part of regularly scheduled meetings, applicant appeals are discussed as standard agenda items. Even when the specific conditions are met to allow disclosure during a public hearing, the most preferable method for introducing CHRI is to enter into a closed session which limits participation by the public at large. States and local agencies should be able to reasonably demonstrate how the prerequisite criteria are being met for audit purposes.

5.3.5 Unauthorized Dissemination

CHRI shall NOT be disseminated to:

- Unauthorized agencies or individuals. Unauthorized individuals include family members or friends of the subject of record. Unauthorized agencies include agencies that do not have legislative authority, do not have an ORI, and do not have a current User Agreement with the HCJDC.
- Independent or third-party auditors, such as a corporate auditor, national program or grant auditor, etc. Authorized auditors are employees of the HCJDC or the FBI.
- Other authorized agencies that do NOT have a commonality of purpose and congruent responsibility authorized by state or federal law.

5.3.6 Misuse of CHRI

Pursuant to section 846-9, HRS, criminal history record information disseminated to non-criminal justice agencies shall be used only for the purpose for which it was given. No agency or individual shall confirm the existence or nonexistence of criminal history record information to any person that would not be eligible to receive the information itself.

Pursuant to section 846-16, HRS, any person who knowingly permits unauthorized access to criminal history record information, or who knowingly disseminates criminal history record information in violations of the provisions of Chapter 846, HRS, or any person violating any agreement authorized by section 846-9, HRS, or any person who gains unauthorized access to criminal history record information shall be guilty of misdemeanor.

5.4 Physical and System Security

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

Physical security measures include:

- Face monitors away from windows, doors and hallways;
- Have computers in a controlled area;
- Limit access to controlled area during CHRI processing times to only those personnel authorized by agency to access and view CHRI;
- Escort all visitors and monitor activity at all times in computer areas and areas where CHRI is being processed;
- CHRI stored in electronic media must be encrypted or password protected; and
- Store hard copies in a secure or locked area.

System security measures include:

- Protect passwords to the computer and to the applications;
- Lock computers when stepping away for any length of time;
- Watch for shoulder surfing;
- Beware of persons trying to get information over the phone that would allow them access to the system, computer or confidential information.

5.5 CHRI In Transit

All CHRI transmitted or transported outside a 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 CHRI in an email unless the proper technical controls are in place to protect it, such as encryption and access control.

5.6 Retention and Storage of CHRI

When CHRI is stored, agencies shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the information. Retention of CHRI is not required and it is not needed for compliance reviews/audit purposes.

Should the agency choose to retain CHRI, the agency must ensure the following:

- CHRI must be kept in a secure environment, free from public or unauthorized access;
- The area where the CHRI is stored must be secured by lock with limited access;
- When retained in electronic format, the data must be protected with a password and/or encryption.

Procedures for handling and storage of CHRI should be established and documented to ensure that access to the CHRI in all forms is restricted to authorized individuals and to protect the CHRI from unauthorized disclosure, alteration or misuse.

5.6.1 Electronic Media Standards

Electronic storage media includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

The agency shall store electronic media within secure locations or controlled areas. The agency shall restrict access to electronic media to authorized individuals.

If the agency is not able to restrict access to electronic CHRI, the electronic CHRI shall be encrypted with a minimum of 128-bit encryption that is certified to meet Federal Information Processing Standards Publication (FIPS)140-2.

A passphrase must be used for encryption. Passphrases must be a minimum of ten characters that include at least one uppercase letter, one lowercase letter, one number, and one special character. Passphrases should not be a dictionary word or a proper name and cannot be the same as the user ID. The passphrase should be set to expire every 90 days and should not be identical to any previous 10 passphrases. Each person with access should be advised to not share their passphrase with anyone, including agency IT staff. Passphrases should not be written down, and must be changed when previously authorized personnel no longer require access.

Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files.

5.6.2 Off-Site Storage

Prior to storing CHRI off-site and under the control of a third party, the agency is required to obtain approval from the SCO to enter into an agreement that includes the Security and Management Control Outsourcing Standards with the third-party that would have access to the CHRI in its storage responsibilities. Approval from the SCO and the compliance with the Security and Management Control Outsourcing Standards is required even if the CHRI will be stored in locked portable containers. See Section 6 of this manual for more information about Outsourcing.

5.7 Destruction of CHRI

Physical media, including hard-copies of CHRI, shall be disposed of when no longer required, using formal procedures that minimize the risk of sensitive information being compromised by unauthorized individuals.

Electronic media shall be sanitized, that is, overwritten with random 0s and 1s at least three times or degaussed prior to disposal or released for reuse by unauthorized individuals. Inoperable media shall be destroyed. The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media.

All destruction of CHRI shall be witnessed or carried out by authorized personnel.

If a private destruction company is contracted, the destruction must take place under direct supervision of authorized agency personnel. If the destruction of CHRI takes place off-site, the agency's agreement with the private vendor must include the Security and Management Control Outsourcing Standards. Approval from the SCO and the compliance with the Security and Management Control Outsourcing Standards is required whenever any administrative functions of handling CHRI is contracted to a third party. See Section 6 of this manual for more information about Outsourcing.

5.8 Incident Response

The security risk of both accidental and malicious attacks against government and private agencies remain persistent in both physical and logical environments. To ensure the protection of criminal justice information and CHRI, agencies shall establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities, and track, document, and report incidents to the state CSO.

5.8.1 Identifying Incidents

A security incident is any act or circumstance that involves CHRI that deviates from the requirements of the FBI CJIS Security Policy and state or federal laws and regulations. Compromises, possible compromises, inadvertent disclosures, and deviations are considered security incidents.

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:

- The system unexpectedly crashes without clear reason;
- New user accounts are mysteriously created which bypass standard procedures;
- Sudden high activity on an account that has had little or no activity for months;
- New files with novel or strange names appear;
- Accounting discrepancies;
- Change in file lengths or modification dates;
- Attempts to write to system files;
- Data modification or deletion;
- Denial of service;
- Unexplained poor system performance;
- Anomalies;
- Suspicious probes; or

- 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.

5.8.2 Reporting Incidents

The agency shall promptly report incident information to the appropriate authorities, including the CSO. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Where ever feasible, the agency shall employ automated mechanisms to assist in reporting security incidents. All employees, contractors, and third party users shall be made aware of the procedures for reporting the different types of event and weaknesses that might have an impact on security and are required to report any security events and weaknesses as soon as possible to the designated point of contact.

The Agency LASO is required to complete the "NCJA Security Incident Reporting Form" and submit it to the CSO for all security incidents. See Appendix B for a copy of the NCJA Security Incident Reporting Form.

6 SECURITY & MANAGEMENT CONTROL OUTSOURCING STANDARDS

Outsourcing incorporates the process of a third party contractor performing administrative functions related to the processing of criminal history record checks. Outsourcing of administrative functions from the authorized agency to a contractor includes, but is not limited to:

- Accessing and/or reviewing CHRI;
- Making fitness determinations and/or recommendations;
- Obtaining missing dispositions;
- Disseminating CHRI as authorized by federal statute, federal executive order, or state statute as approved by the U.S. Attorney General; and
- Other authorized activities relating to the general handling, use, and storage of CHRI.

Prior to allowing a third-party contractor access to CHRI, written approval from the SCO must be received.

6.1 OUTSOURCING STANDARDS

The National Crime Prevention and Privacy Compact Council adopted a Final Rule and published the Outsourcing Standard in the Federal Register in 2005. The Outsourcing Standard establishes minimum requirements to ensure that security and privacy controls are in place for CHRI while under control or management of an outsourced third-party, the contractor. It also requires the contractor to have a security program in place that will ensure the integrity of CHRI is not compromised and meets all requirements of state and federal laws and the FBI CJIS Security Policy.

The Security and Management Control Outsourcing Standards for Non-Channelers can be found online at https://www.fbi.gov/file-repository/security-and-management-control-outsourcing-standard-for-non-channelers-2.pdf/view

6.2 SAMPLE DOCUMENTATION

See Appendix C for the following sample documentation:

- Authorized Recipient Sample Request Letter
- Sample Language between the Authorized Recipient and Contractor regarding Non-Criminal Justice Outsourcing Functions
- Sample 90-Day Audit Checklist for an Authorized Recipient

7 Compliance Audits

7.1 Background

Formal audits were established to ensure compliance with security requirements of access to CHRI. Audits are defined quite simply as methodical examinations and reviews.

FBI CJIS Security Policy requires that each CSA periodically audit all non-criminal justice agencies with access to criminal justice information in order to ensure compliance with applicable statutes, regulations and policies. Additionally, the FBI CJIS Division shall triennially conduct audits of a sampling of non-criminal justice agencies.

7.2 Methodology

The compliance audits consist of both interviews (in-person and/or teleconference) and a survey questionnaire.

7.3 Areas of Review

Compliance audits shall cover both security compliance assessments (ensuring that agencies protect the CHRI against unauthorized access and remains confidential) and compliance reviews (ensuring all CHRI is obtained and released in accordance with applicable laws and regulation, dissemination logs are maintained, and other user related reviews).

7.3.1 Applicant Notification and Record Challenge

The assessment of requirements for applicant notification and record challenge will focus on the following primary areas and include a review of an agency's application process:

- Written notification to the individual fingerprinted that the fingerprints will be used to check the criminal history records of the HCJDC and the FBI, retained by the HCJDC and the FBI and used for all purposes and uses authorized for fingerprint submissions;
- Opportunity to complete or challenge the accuracy of the information contained in the FBI Identification record;
- Providing procedures to obtain a change, correction, or update to an FBI Identification record;
- Reasonable time to correct or complete the record.

7.3.2 Use of CHRI

The assessment of requirements for use of CHRI will focus on the following primary areas:

- All applicant types are covered by approved statutory authorities;
- Changes to approved statutory authorities were submitted for review as applicable;
- Procedural requirements for use of specific authorities;
- Submission of fingerprints and use of name-based III checks;
- Re-use of criminal history records;

- Obtain and review documentation associated with processes;
- Review a sampling of fingerprint transactions and compare with supporting information; and
- As applicable, review a sampling of name-based III inquiries and compare with supporting information from the agency to validate the appropriate use of criminal history records.

7.3.3 Reason Fingerprinted and Purpose Code Usage

The assessment of requirements for the reason fingerprinted field and purpose code usage, fingerprint collection and submission, identity verification, and chain of custody will consider the following:

- Accurate representation of the purpose code and/or authority in the reason fingerprinted field;
- Correct purpose code for name-based III inquires, if applicable;
- Specific reasons/justifications for all requests for CHRI;
- Sampling of fingerprint transactions and comparison with supporting information to validate appropriate use of Reason Fingerprinted Field; and
- As applicable, a sampling of name-based III inquiries and comparison with supporting information from the agency to validate the appropriate use of Purpose Codes.

7.3.4 Dissemination of CHRI

The assessment requirements for dissemination of criminal history record information will consider dissemination to:

- Entities not authorized relative to the statutory authority used;
- Entities for separate, unrelated use subsequent to the original request;
- Private and governmental entities that perform administrative functions;
- Entities outside allowable jurisdictional boundaries;
- The public; and
- The subject of record.

7.3.5 Security of CHRI

The assessment of requirements for security of criminal history record information will consider the following areas:

- Physical security;
- Technical security
- Personnel security;
- Documentation associated with processes; and
- Access controls.

7.3.6 Outsourcing of Administrative Functions

The assessment of requirements and best practices for outsourcing of non-criminal justice administrative functions will consider the following areas associated with the Security and Management Control Outsourcing Standard for Non-Channelers:

- Responsibilities of the authorized recipient;
- Responsibilities of the contractor;

- Adherence to the FBI CJIS Security Policy;
- Site security;
- Dissemination;
- Personnel security;
- System security;
- Security violations;
- Exemptions;
- Review of applicable documentation.

7.4 Agency Requirements for Non-Compliance Findings

For all areas of concern or those deemed non-compliant, the TAC is required to provide a written response to the HCJDC within 30 days of receiving notice of audit completion by the HCJDC. The written response should include a plan of action, along with target dates to address the non-compliance areas.

Upon completion of the corrective measures, the agency must notify the HCJDC in writing that the agency has accomplished its planned objective and is now in full compliance with policy and regulations.

Agencies which refuse to cooperate in the audit process or fail to provide HCJDC with a plan of action will be considered non-compliant and may be subject to suspension of access to CHRI.

8 FINGERPRINT SUBMISSION

Electronic fingerprint capture and submission is the preferred method for submitting fingerprints to the HCJDC and the FBI; however, the HCJDC will accept and process hard-copy fingerprint cards.

8.1 CONSENT AND NOTIFICATION REQUIREMENTS

Each applicant must provide the required consent and be provided the required notifications prior to being fingerprinted. See Section 4.6.1 Agency Requirements for Applicant Privacy Rights for the required elements. Also see Appendix D for Sample Consent and Notification Form.

8.2 VERIFICATION OF IDENTIFICATION

As the demand for fingerprint-based criminal history record checks for non-criminal justice purposes continues to rise, so do the concerns regarding an applicant with a criminal record having someone else pose as the applicant for fingerprinting purposes.

Personnel or contractors obtaining the fingerprints must request some type of photo identification card as one method for verifying an individual's identity and be trained to recognize and properly utilize the security features of various forms of identification. Personnel or contractors should:

- Physically examine the applicant's photo on the identification card and visually compare the photo with the applicant in person;
- Compare the physical descriptors of the applicant to the document provided by the applicant (height, weight, age, etc.);
- Request the applicant verbally provide date of birth, address, etc., and check this against the identification forms used;
- Check the applicant's signature in person with that on the identification form;
- Ensure that the identification form has not been altered in any manner;
- If available, verify that the machine readable data matches the date on the card when it is scanned.

If an agency has reason to believe an applicant has presented fraudulent information, agency personnel should contact local law enforcement. No attempt should be made to detain or pursue the person.

8.2.1 PRIMARY AND SECONDARY FORMS OF IDENTIFICATION

As a primary form of identification only a current, valid, and unexpired photo identification document should be accepted. The following documents may be presented by an applicant when being fingerprinted:

- State-issued driver's licenses or identification card;
- U.S. Passport or U.S. Passport Card;
- Federal Government Personal Identity Verification Card (PIV);
- Uniformed Services Identification Card;
- Department of Defense Common Access Card;
- Foreign Passport with Appropriate Immigration Documents;
- USCIS – Permanent Resident Card (I-551);

- USCIS – Employment Authorization Card (I-766);
- Federal, state, or local government agency ID card with photograph;
- U.S. Coast Guard Merchant Mariner Card; or
- Canadian Driver's License.

In the absence of a primary identification, applicants may provide at least two (2) secondary identification documents including:

- State Government Issued Certificate of Birth;
- U.S. Tribal or Bureau of Indian Affairs Identification Card;
- Native American tribal document;
- Social Security Card;
- Court Order for Name Change/Gender Change/Adoption/Divorce;
- Government Issued Certificate of Marriage;
- U.S. Government Issued Consular Report of Birth Abroad;
- Draft Record;
- School ID with Photograph;
- Certificate of Citizenship (N-560);
- Replacement Certificate of Citizenship (N-561);
- Certification of Naturalization (N-550); or
- Replacement of Certificate of Naturalization (N-570).

When validating the authenticity of secondary identification documents and forms, the data and information may be supported by at least two (2) of the following current documents:

- Utility Bill with Address;
- Jurisdictional Voter Registration Card;
- Vehicle Registration Card/Title
- Paycheck Stub with Name and Address (financial information may be redacted);
- Jurisdictional Public Assistance Card; or
- Spouse/Parent Affidavit.

8.3 Capturing Quality Fingerprints

If the quality of the fingerprint images submitted for a criminal history record check is too low, it may result in:

- Failure to be correctly identified with a criminal record;
- Being rejected by the HCJDC or the FBI for both identification and retention purposes;
- Inability to participate in the Rap Back Program; and/or
- Delay in hiring/filling positions.

8.4 Chain of Custody

When possible, electronic fingerprint submission should be used, thus eliminating the return of the fingerprint card to the applicant. However, in those instances when the fingerprints are not able to be submitted to the HCJDC electronically, the agency should establish procedures to protect the integrity of the applicant's fingerprints when captured. At a minimum, agencies and their contractors should:

- 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.
- Establish procedures that document the type(s) of identification used by the applicant.
- Implement the use of form(s), which may include:
    - Date of fingerprinting;
    - Reason for fingerprinting;
    - Printed name, signature, and/or identification number of the employee taking the fingerprints;
    - Address of agency to receive the fingerprints;
    - Name of agency and physical address of where the fingerprinting was performed;
    - Type of fingerprint capture (ink, livescan);
    - Applicant's consent for fingerprinting;
    - Type of ID verified (Driver's License #/State/Expiration Date)

Agencies should use specially sealed envelopes, agency specific stamps, etc., when forwarding the applicant's manually captured fingerprints to HCJDC. A statement indicating how the personnel or contractor capturing the fingerprints verified the applicant's identity, along with contact information, or a copy of the aforementioned form must also be included.

8.5 Fingerprint Fraud Scenarios

The following scenarios illustrate how an applicant attempted and successfully circumvented the fingerprinting process in order to obtain a position of trust, and the importance of verifying the individual's identity, as well as maintaining the chain of custody. These scenarios did not take place in Hawaii.

An individual applied for, and successfully obtained, a position of trust as a teacher within a school district, after having another individual go to the sheriff's office and provide his fingerprints. The prospective teacher also utilized his father's name, which was the same as his. The fingerprints were subsequently submitted to the State Identification Bureau for a background check. Two years later, the falsified fingerprints were discovered when the teacher was arrested for criminal trespass and window peeping. It was also discovered the teacher had a prior arrest and conviction for simple assault and a sexual battery arrest which resulted in a misdemeanor assault conviction. As a result, the individual's employment was terminated. Subsequently, the individual who had submitted the falsified fingerprints was also arrested for fraudulent activity.

An applicant with a disqualifying out-of-state arrest applied for a teacher certificate and persuaded a student to provide the applicant her fingerprints. The fingerprints were submitted, and the applicant was able to obtain a teaching certificate. The student subsequently was arrested, and the fingerprints hit on her own fingerprints that were in the state rap back system. When the Board of Education received the rap back notification, they discovered that the identifying information did not match the teacher enrolled in rap back. An investigation revealed identity fraud and the case was turned over for criminal prosecution of

both the teacher applicant and the student. In this instance, rap back prevented a disqualified individual from having continued access to a vulnerable population.

The following scenario illustrates how an applicant attempted to circumvent the fingerprinting process in order to obtain a position of trust, but due to the vigilance of the fingerprinting vendor, the hiring agency was able to successfully prevent the individual from obtaining the position.

An individual applied for a health care worker position. Due to the fact that she had a criminal history record, she requested her roommate be fingerprinted on her behalf. However, the fingerprinting agency verified the applicant's identification and determined that the photo/biographic identification did not match the applicant's identity. The fingerprint vendor notified the Department of Health (DOH) that the applicant did not match the identification submitted. Subsequently, both the applicant and the individual that agreed to submit the false fingerprints were arrested and charged. Due to verification of the identification, the DOH was able to detect fingerprint fraud and prevent a prohibited person from obtaining a position of trust as a health care worker.

8.6 Fees

Agencies are billed on a monthly basis for fingerprint transactions submitted during the previous month. If the agency is not on a billing account, payments are due at the time of fingerprint submission. Applicable fees may include the State Criminal History Record Check fee, the FBI Criminal History Record Check Fee, Fingerprinting Fees, and/or Hard-Copy Card Scanning Fees. All fees for HCJDC and FBI services are in accordance with Chapter 5-24, Hawaii Administrative Rules and Title 28 Code of Federal Regulations 20.31(e)(3).

8.7 Rejection Procedures

There are several reasons that cause fingerprints to be rejected by the HCJDC or the FBI. Some of the reasons include:

- Quality of the characteristics are too low;
- Fingerprint images are incomplete or out of sequence;
- Fingerprint patterns are not discernable; and/or
- Reason fingerprinted is incorrect or other quality assurance errors.

In any of these instances, a second fingerprint submission is required to complete the criminal history record check. As long as the second submission is submitted correctly and within 90 days of the original submission, there is no charge for the second submission.

8.7.1 Rejection by the HCJDC

If a fingerprint is rejected by HCJDC, an email or letter will be sent back to the agency with instructions on how to submit a second set of fingerprints.

8.7.2 First Rejection by the FBI

The agency will receive notification of the FBI rejecting an applicant's fingerprint via the Applicant Rap Back Application in the HIJIS Portal. Instead of the applicant's

FBI results indicating Match or No Match, the search results will indicate Unknown and list the reason for the rejection.

Agencies must capture a new set of fingerprints with a new tracking number (OTN), include the original submission's Transaction Control Number (TCN) in the appropriate field on the livescan or card scan device, and insert an R as a prefix in the OCA field. Failure to insert the TCN in the appropriate field and/or failure to prefix the OCA with an R may result in additional fees. The TCN is needed to avoid second charge by the FBI and the R prefix in the OCA is needed to avoid a second charge by the HCJDC.

8.7.3 Second Rejection by the FBI – FBI Name Check Procedure

When fingerprint images are rejected a second time due to low quality prints by the FBI (Error L0008) and one of the rejection notices indicates "The quality of characteristics is too low to be used. Candidate(s) were found." an agency has the option to request a name check through the FBI. Please note: One of the rejections notices must indicate that candidate(s) were found. If neither rejection notice indicates that candidate(s) were found, an FBI name check may not be requested.

To request an FBI name check, the agency must email the request to the FBI at AP_Team@leo.gov with the subject of "Name Check Required". The email shall include the full name of the applicant and the two Transaction Control Numbers (TCNs) found on the rejection notices. The TCN is 20 digits and starts with an "E".

The name check result will be sent directly from the FBI to the authorized recipient, with the exception of VECHS agencies.

For VECHS agencies, the HCJDC is the authorized recipient and thus the FBI will only respond to the HCJDC. VECHS agencies must notify the HCJDC via email at ag.hcjdc.chrc@hawaii.gov when an applicant's fingerprints have been twice rejected due to low quality (L0008) and at least of the rejection notices indicated that candidate(s) were found. The HCJDC, in turn, will request the name-based FBI check and send the results to the VECHS agency. The email to the HCJDC shall have the subject of "Name Check Required" and include the full name of the applicant and the two Transaction Control Numbers (TCNs) found on the rejection notices. The TCN is 20 digits and starts with an "E".

The Name Check must be requested within 90 days of the last rejection date. The first rejection must be within one-year prior to the second rejection.

As a reminder, since the name-based search is not fingerprint-based, the results are NOT backed by positive identification.

9 Criminal History Records

9.1 Hawaii Criminal History Records

Hawaii CHRI is compiled from information submitted to the HCJDC from arresting agencies, prosecutors, and the courts. Although the HCJDC makes reasonable efforts to ensure all the information is submitted by law, it is not responsible for omission, inaccuracies, or incompleteness of the CHRI received from the contributing agencies.

9.2 Final Dispositions

Final dispositions include information disclosing that criminal proceedings have been concluded, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to continue with criminal proceedings.

Final dispositions include, but are not limited to:

- Acquitted;
- Acquitted Due to Mental Incapacity;
- Civil Commitment in Lieu of Prosecution;
- Declined to Prosecute;
- Dismissed;
- Dismissed Due to Mental Incapacity;
- Dismissed without Prejudice;
- Guilty;
- Informational No Charge;
- No Bill;
- Moot;
- No Action by Prosecutor;
- Not Addressed;
- Not Guilty;
- No Action by the Court;
- Nolle Prosequi;
- Released/Discharged - No Charge;
- Released/Discharged Pending Further Investigation;
- Released - Prosecution Declined; and
- Stricken.

9.3 Missing Dispositions

For Hawaii charges missing a final disposition, requests for disposition research may be sent to the HCJDC Help Desk at ag.hcjdc.helpdesk@hawaii.gov.

9.4 Expungement of Arrest Records

Section 831-3.2, Hawaii Revised Statutes allows for certain arrests to be expunged from an individual's arrest record. Expunged arrest and conviction information is not included on criminal history record checks for non-criminal justice purposes. It is important to note that an Expungement of Arrest Records does not remove or seal court records or traffic abstracts. Refer to http://ag.hawaii.gov/hcjdc/expungements for more information.

9.5 Challenging, Correcting Records

The applicant may contact the Criminal History Record Checks Unit of the HCJDC at (808) 587-3279 for obtaining information on how to challenge, correct, or update a Hawaii criminal history record.

If the applicant is challenging the accuracy or completeness of the FBI criminal history record, they should send the challenge to the agency that contributed the questioned information, or they may send a challenge directly to the FBI. The FBI will then forward their challenge to the agency that contributed the questioned information and request the agency to verify or correct the challenged entry.

10 Civil Rap Back Service

10.1 Purpose of the Rap Back Service

The Rap Back Service is an extension of a fingerprint-based criminal history record check that allows agencies to subscribe to the submitted fingerprints to receive notification of certain subsequent criminal justice events to allow for timely suitability decisions on an individual's continued volunteer service, employment, license or permit.

10.2 Authority to Participate in the Rap Back Service

§846-2.7, Hawaii Revised Statutes provides the authority for the Rap Back Service. Rap Back subscriptions may only be created if the agency has a continuing authority to receive criminal history record information on the individual. The individual must actively volunteering with or employed, licensed or permitted by the agency. The subscription may only be created after the individual has successfully passed the initial suitability clearance.

Participation in the Rap Back Service is optional.

10.3 Triggering Events

Certain events reported to the HCJDC or the FBI will trigger an email notification to the authorized agency.

10.3.1 Arrest Trigger

Hawaii arrests supported by verified fingerprints will result in a notification. Additionally, arrests supported by verified fingerprints that have been reported to the FBI will also result in a notification; these include arrests from other states and U.S. territories. It is important to recognize that if fingerprints are not taken at the time of the arrest or if the arrest fingerprints have been rejected due to low-quality or other submission errors, the arrest will not trigger a notification.

10.3.2 Dispositions Reported to the FBI Trigger

If the FBI receives updated information on an existing criminal arrest and the FBI/UCN, which is the FBI's Universal Control Number, is matched against a subscribed individual, the authorized agency will receive a notification. It is important to note that 20 states, including Hawaii, participate in the National Fingerprint File (NFF) program, and do not submit disposition information to the FBI; therefore, a disposition notification will not be triggered.

10.3.3 NCIC Want/Immigration Violator Trigger

Want/Immigration Violator notifications are triggered from agencies entering information within the National Crime Information Center (NCIC) System in which a matching FBI/UCN is entered. Agencies will be notified if a NCIC Want/Immigration Violator record is added, modified, or deleted within the NCIC system. These types of notifications may not be biometrically matched to the subscribed individual.

10.3.4 NCIC National Sex Offender Registry (NSOR) Trigger

NSOR notifications are triggered from agencies entering information into the NCIC System in which a matching FBI/UCN is entered. Agencies will be notified if a NCIC NSOR record is added, modified, or deleted within the NCIC system. These types of notifications may not be biometrically matched to the subscribed individual.

10.3.5 Death Trigger

This trigger will activate when the FBI receives a death notice and associates it with a subscribed individual. The notice will trigger from both fingerprint-based and non-fingerprint-based death notice submissions.

10.4 Participation Requirements

While there are no fees to participate in the Rap Back Service, there are considerable operational resources required. At the time of initial implementation, there will be no bulk services available. Agencies will have to manage each subscription individually.

10.4.1 Applicant Consent and Notification

Prior to being fingerprinted for the initial criminal history record check, each applicant must provide the appropriate consent and be given the appropriate nonfictions, as required by §846-2.7, HRS and federal regulations. This includes written or electronic acknowledgement that the applicant has been provided with the current version of the FBI Privacy Act Statement.

10.4.2 Applicant Rap Back Application (ARBA)

All Rap Back subscription activities will be completed through the ARBA within the Hawaii Integrated Justice Information Sharing (HIJIS) Portal. This same application is currently used by all authorized agencies to receive the initial results of their fingerprint-based state and national criminal history record checks. The ARBA will provide authorized agencies a means to subscribe, validate, and cancel their subscriptions, as well as receive updated rap sheets and Rap Back information.

10.4.3 Subscribing to an Individual

Rap Back subscriptions may only be created if the agency has a continuing authority to receive criminal history record information on the individual. In other words, the individual must be actively volunteering with or employed, licensed, or permitted by the agency. The subscription may only be created after the individual has successfully passed initial fitness determination. If the applicant's fingerprints were rejected by the FBI due to low quality or other submission errors, the agency will not be able to create an FBI Rap Back subscription.

10.4.4 Receiving a Notification (Pre-Notification)

When a triggering event occurs on a subscribed individual, the HCJDC will email the agency to login to the ARBA within the HIJIS Portal. Because arrest information is confidential and may only be used for authorized purposes, prior to viewing the resulting (new) criminal history record information, the ARBA will require the agency to verify that the individual is still volunteering with or, employed, licensed or permitted by the agency. If the agency responds in the negative, the new criminal

history record information will not be made available and the subscription will be cancelled. If the agency responds in the affirmative, the agency will be able to access the new criminal history record information.

10.4.5 Validating a Subscription

All subscriptions must be validated every five years to ensure the agency is still authorized to receive criminal history record information on the subscribed individual. Subscriptions are automatically set to expire on the fifth anniversary of the subscription creation date. Every month, the agency will receive a listing of subscriptions set to expire within the next 45-75 days. In order to extend the subscription, agencies will be required to verify that each individual is still volunteering with or employed, licensed or permitted by the agency. Failure to validate a subscription by the expiration date will result in the automatic cancellation of the subscription.

10.4.6 Cancelling a Subscription

FBI policy dictates that subscriptions must be cancelled within five business days from the final determination of the agency's ineligibly to subscribe to the individual. This means that within five business days of the agency knowing that the individual is no longer volunteering with or employed, licensed, or permitted by the agency, the subscription must be cancelled.

10.4.7 State and FBI Audits

Like the information received from the initial criminal history record check, information received from the Rap Back Service is considered confidential criminal history record information and held to the same security standards and policies. Rap Back subscriptions and resulting information are subject to state and FBI audits and sanctions. Agencies must maintain all necessary documents and written policies to comply with State and FBI audits.

10.5 Rap Back Service Start-Up Checklist

If interested in participating in the Rap Back Service, please contact the HCJDC Help Desk at ag.hcjdc.helpdesk@hawaii.gov to receive a copy of the Hawaii Civil Rap Back Service Startup Checklist.

APPENDICES

Dissemination of State and/or National Criminal History Record Information (CHRI) to Applicant

Authorized recipients of criminal history record information (CHRI) may provide a copy of the CHRI to the subject of the record when the CHRI was obtained as a result of positive fingerprint identification. The CHRI may only be released to the applicant to allow the subject to complete, or challenge the accuracy of, the record.

For the protection of both the authorized recipient and the subject of the record, the following steps must be taken.

If the CHRI is to be released by any other method than in-person, at the time of fingerprinting, the subject of record must provide the following written or electronic consent:

> "If the resulting criminal history record information (CHRI) impacts my fitness determination, I authorize *<insert authorized recipient name>* to release the CHRI directly to me via certified mail with restricted delivery at the physical address below or a passphrase protected, encrypted portable document format (pdf) attachment to the email sent to the email address below so that I may have the opportunity to complete, or challenge the accuracy of, my criminal history record.
>
> Physical address: _____
>
> Email address: _____
>
> Signed:_____ Dated: _____"

To release CHRI by mail:

1. All correspondence containing CHRI must be sent certified directly to the subject of the record.
2. Maintain a dissemination log with the subject's name, SID # and/or UCN #, and where the criminal history record information was mailed. The criminal history record information may not be sent to a third-party.
3. Keep a copy of the certified receipt and the return receipt with the subject's signature on file with the dissemination log.

To release CHRI by e-mail:

1. All correspondence containing CHRI must be sent as passphrase protected or encrypted portable document format (pdf) directly to the subject of the record.
2. Encryption shall be a minimum of 128-bit. The passphrase to unlock the encryption shall meet the following requirements:
   a. Be at least 10 characters;
   b. Not be a dictionary word; and
   c. Include at least one (1) uppercase letter, one (1) lower case letter, one (1) number, and one (1) special character.
3. The passphrase shall not be transmitted to the subject of record in the same email as the CHRI.
4. Maintain a dissemination log with the subject's name, SID # and/or UCN #, and when and where the criminal history record information was emailed. The criminal history record information may not be sent to a third-party.

To release CHRI in-person:

1. The subject must present a government issued photo identification card.
2. Maintain a dissemination log with the subject's name, SID # and/or UCN #. The subject must sign and date the dissemination log indicating when the copy of the record was reviewed or picked up. The criminal history record information may not be released to a third-party.

	Hawaii Criminal Justice Data Center	**Non-Criminal Justice Agency Security Incident Reporting Form**

Immediately upon discovery of a security incident, this form is to be completed by the Local Agency Security Officer (LASO) and submitted to the CJIS Systems Officer (CSO) via email at ag.hcjdc.helpdesk@hawaii.gov.

Name of Person Completing this Form:

Contact Information
(Include phone, extension, email):

Date of Report:

Date & Time of Incident:

Location of Incident(s):

Description of Incident(s):

System(s) Affected:

Record(s) Affected:

Method of Detection:

Action Taken/Resolution:

How future incidents of this nature will be prevented:

Sample Authorized Recipient Request Letter for Non-Channeler Outsourcing

REQUEST LETTER
FOR [*insert Authorized Recipient's name*] TO USE
[*insert Contractor's name*] AS A CONTRACTOR
FOR NON-CRIMINAL JUSTICE ADMINSTRATIVE FUNCTIONS

[*Insert date*]

[I*nsert State Compact Officer's name*]
Hawaii Criminal Justice Data Center
465 South King Street, Room 102
Honolulu, HI 96813

Dear [*insert State Compact Officer's name*]:

[*Insert Authorized Recipient's name*], the Authorized Recipient, requests permission to use [*insert Contractor's name*] as a contractor to outsource non-criminal justice administrative functions relating to the processing of criminal history record information (CHRI) on our behalf. This would include [*insert all functions that apply. For example, obtaining missing dispositions, making determinations and recommendations, off-storage of CHRI and its corresponding fingerprint submissions, etc.].*

If approved, [*Insert Authorized Recipient's name*] and [*insert Contractor's name*] will enter into an agreement in which [*insert Contractor's name*] will act on our behalf in accordance with the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Non-Channelers.

[I*nsert Authorized Recipient's name*] is authorized to perform criminal history record checks pursuant to the [*insert the legal citation of the statute or public law that requires or authorizes the Authorized Recipient to have access to CHRI*.].

Upon execution of the Contract, [*insert Authorized Recipient's name*] will take responsibility for [*insert Contractor's name*]'s compliance with the terms of the Contract, to include the Outsourcing Standard for Non-Channelers, and will notify you of any violations.

Sincerely,

[Insert name]
[*Insert title*]
[*Insert address*]
[*Insert phone number*]
[*Insert email address*]
[*Insert fax number*]

Sample Language for Contract between Authorized Recipient and Contractor regarding Non-Channeler Outsourcing

CONTRACT BETWEEN
[insert Authorized Recipient's name]
AND
[*insert Contractor's name*]
REGARDING OUTSOURCING OF
NON-CRIMINAL JUSTICE FUNCTIONS

This contract is entered into between [*insert Authorized Recipient's name and address*], the Authorized Recipient, and [*insert Contractor's name and address*], the Contractor, under the terms of which the Authorized Recipient is outsourcing the performance of non-criminal justice administrative functions involving the handling of criminal history record information (CHRI) pursuant to Title 28, Code of Federal Regulations, Part 906 and the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Non-Channelers. The most current version of the outsourcing standard is incorporated by reference into this contract and appended hereto as Attachment "[insert]".

The Authorized Recipient's authority to submit fingerprints for non-criminal justice purposes and obtain the results of the fingerprint search, which may contain CHRI, is [*insert the legal citation of the statute or public law that requires or authorizes the Authorized Recipient to have access to CHRI*.]. This authority requires or authorizes fingerprint-based criminal history record checks of [*insert all categories of current and prospective employees, licensees, or applicants for other benefits covered by statute or public law*.].

The specific non-criminal justice administrative function(s) to be formed by the Contractor that involve access to CHRI on behalf of the Authorized Recipient is to [*insert specific non-criminal justice administrative functions to be performed; i.e., obtain missing dispositions, make determinations and recommendations, off-storage of CHRI, etc.].*

[*insert Contractor's name*] will comply with the Outsourcing Standards for Non-Channelers requirements, to include the *FBI CJIS Security Policy*, and other legal authorities to ensure adequate privacy and security of personally identifiable information (PII) and criminal history record results related to this contract, and will ensure that all such data is returned to the Authorized Recipient as soon as no longer needed for the performance of contractual duties.

NOTE: The signature page with dates should be included in the contract.

Sample 90-Day Checklist for an Authorized Recipient's Audit of Contractor

The Outsourcing Standard for Non-Channelers requires ARs who have been approved to outsource non-criminal justice administrative functions conduct an audit of the Contractor within 90 days of the date the Contractor first receives CHRI. The following chart has been designed as a tool to assist ARs who are developing an audit process to comply with this requirement. Depending on the function(s) outsourced and the specifics of the process, all of the requirements may not be applicable.

Contractor Assessment	Reference OS- Outsourcing Standard for Non-Channelers CSP – FBI CJIS Security Policy	Yes	No	N/A
Policy References				
a) Copy of current Outsourcing Standard for Non-Channelers	OS – 2.02; 2.03; 2.05; 2.07; 3.02; 3.03; 5.03; 6.02; 7.01; 8.01a; 9.01; 9.04; 11.05; 11.06			
b) Copy of current *FBI CJIS Security Policy*	OS – 2.03b; 2.03c; 3.01; 3.02; 3.03; 7.01; 7.02; 9.02			
Security Program				
a) Authorized Recipient (AR) approved minimum requirements for content of Security Program	OS – 3.02			
b) Implementation of security requirements	OS – 3.02; 3.03a-d			
c) Reporting procedures for security violations	OS – 3.03c; 8.0			
Security Training Program				
a) AR approved	OS – 3.04			
b) Training prior to appointment or assignment	OS – 3.04			
c) Training upon receipt of changes	OS – 3.04			
d) Annual refresher training	OS – 3.04			
Site Security				
a) Available for announced/unannounced audits	OS – 3.05			
b) Physically secure location	OS – 4.01; 7.02a			
Use and Maintenance of CHRI				
a) Maintained in accordance with contract and does not exceed period of time AR is authorized to maintain	OS – 3.07			
b) Used only in accordance with contract and AR's authority	OS – 2.03; 3.01			
Dissemination				
a) AR approved in accordance with contract and AR's authority	OS – 5.01			
b) Compliant with laws, rules, and regulations[1]	OS – 5.01			
c) Log captures required information and retained for a minimum of 365 days	OS – 3.08; 5.02			
Personnel Security				
a) Confirmation of understanding by employee	OS – 6.02			
b) List of personnel with access to CHRI	OS – 6.03			
c) Updates to list of personnel changes within 24 hours of changes	OS – 6.03			
Security Violations				
a) Develop and maintain written security violation plan	OS – 8.01a; 2.07; 3.03			
b) Policy for disciplinary action	OS – 8.01a			
c) Immediate suspension pending investigation	OS – 8.01b			
d) Immediate report	OS – 8.01c			
e) Follow-up report	OS – 8.01c			
Security on Systems Processing CHRI				
a) Current topological drawing	OS – 2.04			
b) Firewalls	OS – 7.01a CSP – 5.10			
c) Encryption	OS – 7..01b CSP – 5.5.2.4; 5.10.1.2			
d) Virus protection on networks processing CHRI	CSP – 5.10.4.2			
e) User identification	CSP – 5.6			
f) Authentication of user identification	CSP – 5.6			
g) Advanced authentication when accessing via the internet	CSP – 5.6			
h) Audit trails	CSP – 5.4.6			
Media Destruction				
a) Hard copy	OS – 7.02c CSP – 5.8.4			
b) Electronic media	OS – 7.02 CSP – 5.8.3			

Based on OS for Non-Channelers dated 11/06/2014 and the FBI CJIS Security Policy 5.3 dated 08/04/2014.

[1] Applicable laws, rules, and regulations regarding the dissemination of national CHRI include Title 28, United States code , Section 534; Title 28, Code of Federal Regulations, Section 50.12(b) and Part 906.

State and National Criminal History Record Check
Consent & Notification

At a minimum, the below consent & notification must be obtained from each applicant for which fingerprints are submitted to the HCJDC and the FBI. Electronic consent & notification is acceptable. All of the information is REQUIRED.

Department: _____

Division: _____

Applicant Type: _____

Name: _____

Alias(es): _____

SSN: _____ Sex: _____ Race: _____

Height: _____ Weight: _____ Eye: _____ Hair Color: _____

Place of Birth: _____ Date of Birth: _____

Citizenship: _____

☐ I have not been convicted of a crime.
☐ I have been convicted of the following crime(s):

Describe the crime(s) and the particulars, such as dates, offense, and disposition (attach additional sheets as necessary):

I, the undersigned, hereby authorize the Department/Division listed above to submit a set of my fingerprints to the Hawaii Criminal Justice Data Center (HCJDC) and the Federal Bureau of Investigation (FBI) for the purposes of accessing and reviewing state and national criminal history records that may pertain to me. I understand that my fingerprints will be retained by the HCJDC and the FBI for all purposes and uses authorized for fingerprint submissions, which may include participation in the state and national rap back program.

I understand that I have the right to challenge the accuracy and completeness of the results of my fingerprint-based criminal history record check. Should the Department/Division policy not allow a copy of the results to be given to me, I may obtain a copy of my criminal history record by submitting fingerprints and fees directly to the HCJDC and/or FBI. I understand that the procedures for obtaining a change, correction, or updating of my criminal history record are set forth in Title 28, Code of Federal Regulations, Section 16.34.

I acknowledge that I have read, understand, and agree to the FBI Privacy Act Statement.

Signature: _____ Date:_____

FBI Privacy Act Statement

Authority: The FBI's acquisition, preservation, and exchange of fingerprints and associated information is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Pub. L. 92-544, Presidential Executive Orders, and federal regulations. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.

Social Security Account Number (SSAN). Your SSAN is needed to keep records accurate because other people may have the same name and birth date. Pursuant to the Federal Privacy Act of 1974 (5 USC 552a), the requesting agency is responsible for informing you whether disclosure is mandatory or voluntary, by what statutory or other authority your SSAN is solicited, and what uses will be made of it. Executive Order 9397 also asks Federal agencies to use this number to help identify individuals in agency records.

Principal Purpose: Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based background checks. Your fingerprints and associated information/biometrics may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems (including civil, criminal, and latent fingerprint repositories) or other available records of the employing, investigating, or otherwise responsible agency. The FBI may retain your fingerprints and associated information/biometrics in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI.

Routine Uses: During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. Routine uses include, but are not limited to, disclosures to: employing, governmental or authorized non-governmental agencies responsible for employment, contracting licensing, security clearances, and other suitability determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.

Additional Information: The requesting agency and/or the agency conducting the application-investigation will provide you additional information pertinent to the specific circumstances of this application, which may include identification of other authorities, purposes, uses, and consequences of not providing requested information. In addition, any such agency in the Federal Executive Branch has also published notice in the Federal Register describing any systems(s) of records in which that agency may also maintain your records, including the authorities, purposes, and routine uses for the system(s).

Non-Criminal Justice Applicant's Privacy Rights

As an applicant who is the subject of a national fingerprint-based criminal history record check for a noncriminal justice purpose (such as an application for a job or license, an immigration or naturalization matter, security clearance, or adoption), you have certain rights which are discussed below.

- You must be provided written notification[1] that your fingerprints will be used to check the criminal history records of the FBI.
- If you have a criminal history record, the officials making a determination of your suitability for the job, license, or other benefit must provide you the opportunity to complete or challenge the accuracy of the information in the record.
- The officials must advise you that the procedures for obtaining a change, correction, or updating of your criminal history record are set forth at Title 28, Code of Federal Regulations (CFR), Section 16.34.
- If you have a criminal history record, you should be afforded a reasonable amount of time to correct or complete the record (or decline to do so) before the officials deny you the job, license, or other benefit based on information in the criminal history record.[2]

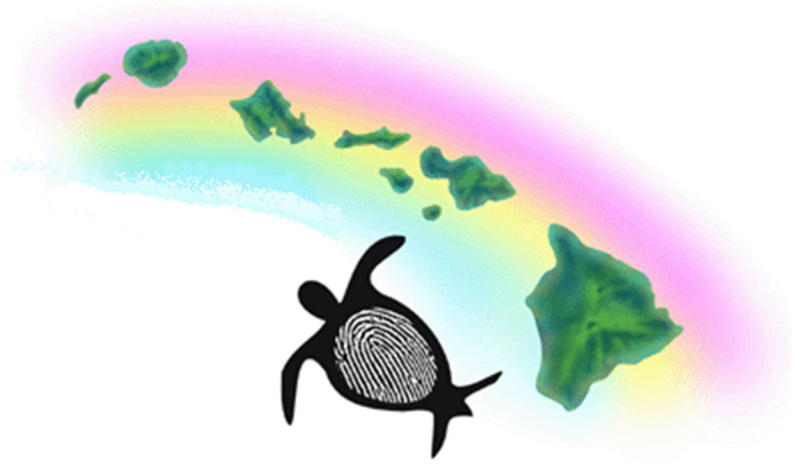
You have the right to expect that officials receiving the results of the criminal history record check will use it only for authorized purposes and will not retain or disseminate it in violation of federal statute, regulation or executive order, or rule, procedure or standard established by the National Crime Prevention and Privacy Compact Council.[3]

If agency policy permits, the officials may provide you with a copy of your FBI criminal history record for review and possible challenge. If agency policy does not permit it to provide you a copy of the record, you may obtain a copy of the record by submitting fingerprints and a fee to the FBI. Information regarding this process may be obtained at http://www.fbi.gov/aboutus/cjis/background-checks.

If you decide to challenge the accuracy or completeness of your FBI criminal history record, you should send your challenge to the agency that contributed the questioned information to the FBI. Alternatively, you may send your challenge directly to the FBI. The FBI will then forward your challenge to the agency that contributed the questioned information and request the agency to verify or correct the challenged entry. Upon receipt of an official communication from that agency, the FBI will make any necessary changes/corrections to your record in accordance with the information supplied by that agency. (See 28 CFR 16.30 through 16.34.)

Endnotes

[1] Written notification includes electronic notification, but excludes oral notification.
[2] See 28 CFR 50.12(b).
[3] See 5 U.S.C. 552a(b); 28 U.S.C. 534(b); 42 U.S.C. 14616, Article IV(c); 28 CFR 20.21(c), 20.33(d) and 906.2(d).



Hawaii Criminal Justice Data Center
Department of the Attorney General
465 South King Street, Room 102
Honolulu, HI 96813

Contact information for Authorized Recipients:
Phone: (808) 586-2547
Fax: (808) 587-3024
ag.hcjdc.helpdesk@hawaii.gov

Contact information for public:
Phone: (808) 587-3279
Fax: (808) 587-3024
ag.hcjdc@hawaii.gov