



***THE GEORGIA CRIME
INFORMATION CENTER
2011***

***Georgia Guide for Non-Criminal Justice
Agency Access to Criminal History
Record Information***

Table of Contents

Introduction	3
Authority	3
Umbrella Statute	5
Additional Statutes	6
Criminal History Record Information	7
Use and Dissemination	7
Retention and Security	8
Penalties for Misuse of CHRI	9
Outsourcing Standard	10
Fingerprint Information	10
GBI/GCIC's Role in the Fingerprint Process:	10
Submission of Fingerprints	11
Georgia Applicant Processing Service (GAPS)	11
Applicant Identity Verification	11
Determine Policy, Procedures, and Practices	12
Create an Identification Validation Guide	12
Create Chain of Custody Procedures	12
Training Requirements	13
Audits	14
Audit Assessment Overview	14
Sanctions for Noncriminal Justice Agency Violations	17
Contacts	18
Helpful Resources	18
Terms, Definitions and Acronyms	19
Acronyms	23
Appendix A	24
Appendix B	27
Appendix C	28
Appendix D	29
Appendix E	33
Appendix F	34

Introduction

This guide sets forth procedures and guidelines for non-criminal justice agencies that access criminal history record information (CHRI) through fingerprint submissions. It is designed to be a reference for agencies regarding the access, maintenance, dissemination and audit requirements for CHRI.

CHRI is available to employers; local, state and federal government agencies; licensing governmental agencies; and adoption/foster care providers upon the submission of fingerprints or via a name based search, however this guide will focus on national CHRI received from fingerprint submissions only.

The Georgia Crime Information Center (GCIC), a division of the Georgia Bureau of Investigation (GBI), maintains the database, which contains Georgia CHRI and is the access point for federal CHRI. In addition, GCIC is responsible for ensuring compliance with both state and federal rules for the use, security and dissemination of CHRI.

Authority

The non-criminal justice use of national CHRI is based on the following statutes, rules and regulations:

Federal

- Title 42, U.S.C., Chapter 140, Subchapter II, § 14616 established the Compact Council, which is authorized to establish rules, procedures and standards for use of the Interstate Identification Index (III) for non-criminal justice purposes. Determining compliance includes but is not limited to: assessing participation requirements; the continual maintenance; and security of CHRI.
- Title 5, U.S.C., § 552a, (The Privacy Act) requires agencies to maintain a system of records which establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records. *III/NFF Operations & Technical Manual Ch. 2, Section 2.1*
- Title 28, Code of Federal Regulations (CFR), 20.30, cites the administration of criminal justice shall include criminal identification activities, and the collection, storage and dissemination of CHRI.
- Title 28, CFR, 20.33 (a) (2), authorizes the dissemination of CHRI contained in the III to federal agencies authorized to receive it pursuant to federal statute or Executive Order.
- Title 28, CFR, 20.33(a) (3) authorizes the dissemination of criminal history information contained in the Interstate Identification Index (III) and the Fingerprint Identification Record System (FIRS), for use in connection with licensing or employment, pursuant to Public Law (Pub. L.) 92-544, 86 Stat. 1115, or other federal legislation, and for other uses for which dissemination is authorized by federal and state law.
- Pursuant to Pub. L. 92-544, the FBI is empowered to exchange identification records with officials of state and local governments for purposes of licensing and employment if authorized by a state statute which has been approved by the Attorney General of the United States. The Attorney General's approval authority is delegated to the FBI by Title 28, CFR, § 0.85(j). The standards employed by the FBI in approving Pub. L. 92-544 purposes

have been established by a series of memoranda issued by the Department of Justice (DOJ), Office of General Council (OGC) or Access Integrity Unity (AIU). The standards are:

- ⌚ The authorization must exist as the result of legislative enactment or its functional equivalent;
- ⌚ The authorization must require fingerprinting of the applicant;
- ⌚ The authorization must, expressly or by implication, authorize use of FBI records for screening of the applicant;
- ⌚ The authorization must not be against public policy;
- ⌚ The authorization must not be overly broad in its scope and it must identify the specific category of applicants/licensees.
- ⌚ The fingerprint submission must be channeled through the State Identification Bureau (SIB) for forwarding to the FBI;
- ⌚ The states must designate a governmental agency to be responsible for receiving and screening the results of the record check to determine an applicant's suitability for employment/licensing;
- ⌚ The results of the record check cannot be released outside the receiving governmental department or related governmental agency;
- ⌚ Processing fees are either by direct payment or billed to the SIB depending on arrangements made between the FBI and

the SIB, such as the execution of a Memorandum of Understanding for billing.

State

- Pub. L. 92-544 requires that a state law be passed and approved by the FBI for access to CHRI for licensing and employment purposes. Currently Georgia has thirty (30) such approved statutes. (*See appendix A for the list of approved statutes or click the following link*):
<http://gcicweb.gbi.state.ga.us/cjis/ori/Authorization%20for%20FBI%20Fingerprint%20Check%20s.pdf>

Approval of statutes must come through the GCIC by following the steps below:

- ⌚ Submit a draft to the GCIC with a request for review and approval by the FBI.
- ⌚ The FBI will review draft ordinances and communicate directly with the GCIC whether the ordinance and agency would qualify.

⌚ Upon adoption of the ordinance, the FBI will conduct a final review and if the adopted ordinance and agency qualify for an FBI fingerprint background check, the GCIC will notify the local agency.

⌚ Prior to submission of FBI fingerprint based background checks, the local agency must request an FBI non-criminal justice agency identifier (ORI). This request is submitted in writing to GCIC to forward to the FBI.

GCIC is responsible under Georgia law § 35-3-30 and the Rules of the GCIC Council to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records.

Umbrella Statute

Georgia has a state umbrella statute that has been approved by the FBI which allows a city or county government to receive federal fingerprint-based background check results when a county code or city ordinance has been enacted meeting the requirements of Pub. L. 92-544. Any locality considering an ordinance requiring a national fingerprint background check must go through the following process:

⌚ Submit a draft to the GCIC with a request for review and approval by the FBI.

⌚ The FBI will review draft ordinances and communicate directly with the GCIC whether the ordinance and agency would qualify.

⌚ Upon adoption of the ordinance, the FBI will conduct a final review and if the adopted ordinance and agency qualify for an FBI fingerprint background check, the GCIC will notify the local agency.

⌚ Prior to submission of FBI fingerprint based background checks, the local agency must request an FBI non-criminal justice agency identifier (ORI). This request is submitted in writing to GCIC to forward to the FBI.

Additional Statutes

National Child Protection Act/Volunteers for Children Act (NCPA/VCA)

The National Child Protection Act/Volunteers for Children Act (O.C.G.A. § 35-3-34.2)

authorizes national fingerprint-based background checks for public agency employment for:

⌚ Child Care Provider/Care Placement

⌚ Mental Health Care Provider/Care Placement

⌚ Elder Care Provider/Care Placement

And for Volunteers when they are working with the following groups:

- ⌚ Child Care
- ⌚ Mental Health Care
- ⌚ Elder Care

Adam Walsh Child Protection and Safety Act

The Adam Walsh Child Protection and Safety Act [Section 153-Schools Safely Acquiring Faculty Excellence (SAFE) Act] authorizes national fingerprint-based background checks for public and private elementary and secondary schools and state and local educational agencies per Public Law 109-248.

Criminal History Record Information

Criminal History Record Information (CHRI) is defined as information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments or other formal criminal charges, and any disposition arising there from including acquittal, sentencing, correctional supervision and release. CHRI may also include the age and sex of each victim as provided by the criminal justice agency. The term *does not* include identification information, such as fingerprint records not related to an arrest, to the extent that such information does not indicate involvement of the individual in the criminal justice system. (GCIC Council Rule 140-1-.02).

The FBI Interstate Identification Index (III or Triple I) provides access to criminal record information contributed by participating states and the FBI. The FBI Criminal Justice Information Services (CJIS) Division operates the Interstate Identification Index (III).

The National Fingerprint File (NFF) places primary responsibility for maintenance and dissemination of criminal history record information on each state repository, instead of the FBI. Georgia is one of ten states that serve as an NFF state. The other states are Colorado, Florida, Idaho, Kansas, Montana, New Jersey, North Carolina, Oklahoma, and Oregon. Unless Georgia statute mandates a national criminal history check for a specific type of employment, license or permit, etc., GCIC will only provide a State of Georgia criminal history report. Refer to Appendix A for a list of Georgia laws requiring FBI Fingerprint Background Checks.

Use and Dissemination

- Fingerprints or other approved forms of positive identification shall be submitted with all requests for criminal history record checks for non-criminal justice purposes (Title 42, U.S.C. § 14616, Article V).

- Agencies must have either an Originating Agency Code (OAC) number or Originating Agency Identifier (ORI) number assigned to them as a prerequisite to obtaining fingerprint-based criminal history record checks.

- ⌚ An OAC number is assigned by the GBI to agencies that are only authorized to obtain a Georgia criminal history record check.

☎ An ORI number is assigned by the FBI to governmental or other authorized private agencies (such as private probation companies) that are authorized by Georgia and Federal law to obtain a national criminal history record check.

To request an OAC or ORI number you must send in a written request to GCIC for a service agreement to the address below (see appendix “D” for an example of the agreement):

**CCH/IDENT APPLICANT SERVICES
P.O. BOX 370748
DECATUR, GEORGIA 30037-0748**

There is **NO** fee for obtaining an OAC or ORI number. If you have any questions about this process you may contact CCH/Identification Applicant Services at 404-244-2639, Option 2. To obtain national CHRI, there must be an approved statutory authority (per Public Law 92-544).

Use of CHRI

Use of Georgia and FBI criminal history records obtained by the non-criminal justice agency are solely for the purpose requested and cannot be disseminated outside the receiving agency. O.C.G.A. § 35-3-38 establishes criminal penalties for requesting, obtaining, communicating or attempting to communicate criminal history record information under false pretenses or in a negligent manner. Authorization to disseminate Federal CHRI is governed by Title 28, U.S.C., § 534 and provides that access to CHRI is subject to cancellation if dissemination is made outside of the authorized recipient.

Dissemination of CHRI

Results from fingerprint searches should not be given directly to the applicant but should be mailed or given to the requesting agency only.

Retention and Security

Agencies are required to maintain a system of records that establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records per Title 5, U.S.C., § 552a, (the Privacy Act). (c)(1)(A); III/NFF Operational Technical Manual, Chapter 2, Section 2.1 (the Privacy Act).

Record Storage

All criminal history record information received from GCIC and/or the FBI for background check purposes shall be stored in a secure location. Areas in which the information is processed and handled shall be restricted to authorized personnel in the performance of their duties. In order to ensure a secure environment agencies are required to have a written policy on the storage and destruction of CHRI.

Agencies who wish to use outside entities for record storage must contact the GCIC to make a fitness determination. The agencies must then enter into agreements with contractors if the results of the CHRI are to be managed by or accessible by contract personnel per the Outsourcing Standard. (*Refer to the section below on Outsourcing for more information on the Outsourcing Standard*).

Disposal of CHRI

When CHRI is no longer needed, it shall be destroyed by burning, shredding or other method rendering the information unreadable. Record destruction must be conducted under the supervision of authorized recipients.

Physical Security

Recipients of CHRI **must** provide a secure area, out of the view of the public and unauthorized personnel, for the handling and retention of CHRI. Agencies shall institute reasonable procedures to protect any central repository of criminal history record information from any unauthorized access, theft, sabotage, fire, wind, flood, power failure or other natural or manmade disasters. In addition, the agency **must** meet all standards provided by the FBI CJIS Security Policy. (*Refer to the training cd for a copy of the Security Policy and to the audit assessment portion of this guide for more information on specific requirements*).

Personnel Security

All persons directly associated with the accessing, maintaining, processing, dissemination or destruction of CHRI must sign an awareness statement (*see appendix C*) and shall be specially trained. The training shall provide employees with a working knowledge of federal and state regulations and laws governing the security and processing of criminal history information. Employers are responsible for ensuring that their personnel receive such training within 60 days of employment or job assignment and every three years; to include Security and Integrity training for criminal justice and all other authorized employees. (*Refer to the training section of this guide for instructions regarding training requirements*).

Penalties for Misuse of CHRI

Title 28, U.S.C., § 534, Pub. L. 92-544 and Title 28, CFR, 20.33(b), provide that the exchange of records and information is subject to CANCELLATION if dissemination is made outside the receiving departments or related agencies. Furthermore, depending upon the nature of the offense and the identity of the offender, federal or state crimes may be charged for the willful, unauthorized disclosure of CHRI.

O.C.G.A. § 35-3-38 establishes criminal penalties for specific offenses involving obtaining, using, or disseminating criminal history record information except as permitted by law.

Outsourcing Standard

Outsourcing occurs when a contractor or third party is contracted out to have control or management of an agency's CHRI. The Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the III System and criminal history information are not compromised. The security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security per Title 28, CFR, Part 906.

The National Crime Prevention and Privacy Compact Council (Compact Council) is a 15-member body of local, state and federal government officials which prescribes system rules and procedures for the effective and proper operation of the Interstate Identification Index (III) for noncriminal justice purposes.

The provisions of the Outsourcing Standard are established and published by the Compact Council pursuant to Title 28, CFR, Part 906 and are subject to the scope of that rule.

The provisions apply to:

- 🕒 All Personnel

- ⌚ Systems
- ⌚ Networks
- ⌚ Facilities supporting and/or acting on behalf of the Authorized Recipient of CHRI

Please refer to the training cd for a complete copy of the Outsourcing Standard.

Fingerprint Information

GBI/GCIC's Role in the Fingerprint Process:

If a fingerprint background check is authorized or required, either by Georgia law or for employment or licensing purposes, it must be done through the GBI.

*Refer to Appendix "B" for a sample consent form. **Submission of Fingerprints***

The GBI does not provide fingerprinting services. Agencies can submit fingerprints electronically via the Georgia Applicant Processing Service (GAPS), a local law enforcement agency or a GCIC certified livescan device that resides at an agency capable of submitting prints electronically to GCIC.

Please note that GCIC no longer accepts paper fingerprint card submissions except for criminal justice employment or non-criminal justice applicants that reside out of state.

Georgia Applicant Processing Service (GAPS)

The Georgia Bureau of Investigation has contracted with Cogent Systems, Inc. to provide electronic fingerprint submission services for applicants in the State of Georgia. GAPS provides the ability for applicants to have fingerprint background checks processed electronically in a non-criminal justice environment.

GAPS provides fixed office locations throughout the state so that Georgia residents will not have to travel more than 25 to 30 miles to a GAPS office.

Search results of the fingerprint background check, as well as rapsheets, are available for the agency to retrieve from the GAPS website within 24 to 48 hours after the applicant is fingerprinted and the transaction is submitted to GCIC for processing.

Any Georgia agency or business that holds an ORI or Georgia OAC number may participate in the GAPS program. However, you will need to enroll with Cogent Systems to utilize GAPS. Additional information can be found on the GAPS website at www.ga.cogentid.com under the "General Information" tab and view the link titled "Procedures for Using GAPS".

GAPS Applicant Waiver

I authorize Cogent Systems, Inc. to conduct a fingerprint based criminal history record check of me.

I understand that Cogent Systems, Inc. will send my fingerprints to the Georgia Crime Information Center for a search of criminal history information in its files and to the Federal Bureau of Investigation for a search of its files when a federal record check is so authorized.

I understand that the electronic results of this fingerprint check will be received by Cogent Systems, Inc. and forwarded to the agency responsible for determining my suitability for the position for which I have applied.

I further understand that Cogent Systems, Inc. will not maintain a copy of my record and that Cogent Systems, Inc. meets all confidentiality and security requirements for handling and dissemination of state and federal criminal history

Title 5, U.S.C., § 552a, (c)(1)(A); III/NFF Operational Technical Manual, Chapter 2, Section 2.1 (the Privacy Act).

Applicant Identity Verification

The Compact Council suggests and GCIC requires agencies develop written policy, procedures, and practices for applicant identity verification in order to decrease the likelihood of applicants with a criminal history record having someone pose as the applicant for fingerprinting purposes.

Determine Policy, Procedures, and Practices

May Include:

- Training in the capture of fingerprints (rolled or flats, and electronic or manual).
- Certification of employees which may include recognizing and validating authorized identification forms, identification documents, and source documents for identity confirmation.
- Security Considerations:
 - 🕒 Train employees to recognize and handle the various identification form security features and machine-readable technology.
 - 🕒 Assign a unique identification number to each employee to be included with each fingerprint submission.
 - 🕒 Train employees to recognize official identification forms, documents, and fraudulent or counterfeit documents.

Create an Identification Validation Guide

The Compact Council suggests agencies accept only current, valid, and unexpired government issued picture identification documents. As a primary form of picture identification, a state-issued driver's license or state identification card should be presented by an applicant when being fingerprinted. However, in the absence of a driver's license or identification card, applicants may provide one or more secondary documents. Please refer to the GAPS website (www.ga.cogentid.com) and view the link titled "Identification Needed for Fingerprinting" to access the procedures necessary for verifying an applicant's identity. Each agency should keep these procedures readily available to all employees who will be involved in fingerprinting applicants.

When 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.

Create Chain of Custody Procedures

Agencies are encouraged to create a process to protect the integrity of the applicant's fingerprints when they are forwarded to the state identification bureau (GBI) and/or the FBI.

Agencies can use the following information to develop a chain of custody process: Establish provisions for the agency to manage electronically captured and manually (only with instruction from GCIC) captured fingerprints. Establish an agency tracking system (applicant log) using the employee's name or some other method for identifying the individual capturing the fingerprints and verifying the applicant's identity. Establish procedures that document the type of identification used by the applicant. Implement the use of forms, which may include the:

1. Date of fingerprinting
2. Reason for fingerprinting
3. Printed name, signature, and/or identification number of the employee taking the fingerprints
4. Name of employee's supervisor
5. Supervisor's signature
6. Address of agency to receive information
7. Name of agency and physical address where fingerprinting was performed
8. Type of fingerprinting capture (rolled ink, flat ink, live scan, etc.)
9. Applicant's disclosure information

For further information, please visit the Compact Council website at: www.fbi.gov/hq/cjisd/web%20page/cc.htm.

Training Requirements

In accordance with the GBI Security Policy, employers shall ensure that all personnel receive Security and Integrity of Criminal Justice Information training and/or Security and Awareness Training at least every **Two years**. New employees must complete the training within sixty (60) days of employment. Security and Integrity of Criminal Justice Information Training and/or Security and Awareness training video is required for all personnel directly associated with the accessing, maintaining, processing, dissemination or destruction of CHRI. Training records must be kept by all agencies on their employees that complete Security and Integrity training as they will be required for auditing purposes.

You can access the Security Awareness CBT through the following link: <http://www.firstnetcampus.com/GBI/entities/vendors/logon.htm>

Registration Instructions:

If you are new to the CBT system, please create a username and password by clicking the "I Am a New User" button.

- If you have trouble remembering your username or password, can't view the course or have any other CBT issues, contact CBTHelp@gbi.ga.gov for assistance.

Viewing Instructions:

Once you are successfully logged in, click on the block in the middle of the page that says "GBI Vendor & Non-Criminal Justice Agency Training", then click on "Information Security Video Training" on the left, click "Enroll" to register for the course, then go to the "My Courses" tab to launch the video.

Certificate Generation

Once you view the video, please print the certificate and retain for two years for audit purposes. GBI will automatically receive confirmation of the completion of the security training through the CBT system. It is not necessary to send a copy of the certificate to GBI.

☎ If your agency has an Originating Agency Identifier (ORI), contact your GCIC Customer Support Representative for information on Security and Integrity training options (see *attached map in Appendix "F" for contact information*).

☎ If your agency does not have an ORI, go to the following Internet Website to complete your Security and Integrity training requirement:

http://gta.georgia.gov/00/article/0,2086,1070969_84340779_110482448,00.html

Audits

GCIC Council Rules (2007) 140-2-.04(c)(3) directs auditors to perform periodic audits of public agencies and officials requesting criminal history record checks to assure compliance with the relevant provision of Georgia law, Council Rules, and applicable Federal law. *Please note that all Non-Criminal Justice Agencies are subject to all rules and restrictions as any criminal justice agency.*

GCIC has implemented the non-criminal justice information audit based on the requirements of O.C.G.A § 35-3-30 to ensure the security and confidentiality of records maintained in the III and the Fingerprint Identification Record System (FIRS). Criminal history information obtained under this authority may be used solely for the purpose requested and cannot be disseminated to the person fingerprinted, outside the receiving departments, related agencies, or other authorized entities.

A sample of Non-Criminal justice agencies will be assessed for compliance with state and federal law. The audit will be by correspondence and follow up of audit results will be by letter to notify agencies of any violations. If any violations are found, the agency will be required to send notification of the actions taken to correct the violations. The intention of the audit process is to evaluate compliance with appropriate laws, policies, and regulations which pertain to the use, dissemination, and security of criminal history information.

Violations of regulation, policy, and/or compliance issues discovered during the audit may be subject to sanctions based on the state's operation standards and procedures per GCIC Rule 140-2-.20 and GCIC Policy 6.3. *(Refer to the section below on Sanctions for more information on how violations are handled).*

Audit Assessment Overview

The following guidelines provide a description of each area of assessment as well as the authority that governs that specific area so that each agency can effectively prepare for the audit that will be conducted by GCIC (see *attached map in Appendix "E" for contact information*).

General Areas of Assessment

1. Administrative Functions –

Authority: GCIC Council Rules (2007) 140-2-.04

Adam Walsh Child Protection and Safety Act of 2006

CJIS Security Policy – 4.2.2 – Proper Access To and Use of CHRI

CJIS Security Policy – 5.4.7 – Logging Assessment:

- ⌚ Establishment of audit trail
- ⌚ Access for authorized purpose
- ⌚ Signing of User Agreement with GCIC (if appropriate)
- ⌚ Service Agreement with another agency

2. Access of Interstate Identification Index (III) data –

Authority: CJIS Security Policy:

4.2.2 – Proper Access To and Use of CHRI

4.2.4.1 – Justification

5.8.1 – Storage

Appendix C.14 – Custody and Storage
Assessment:

- ⌚ Purpose of criminal history request
- ⌚ Storage of criminal history data
- ⌚ Access to criminal history within agency
- ⌚ Original intent of criminal history request

3. Personnel Security and Training –

Authority: CJIS Security Policy:

5.12 – Personnel Background Screening for Systems Access and Computer
Terminal/Records

5.2 – Awareness and Training

GCIC Council Rules (2007) 140-2-.16 – Training

GCIC Policy (2008)

Assessment:

- ⌚ Employee background checks (per GCIC Rule 140-2-.09)
- ⌚ Training for electronic submission of fingerprints
- ⌚ Training of terminal operators
- ⌚ Security and Awareness Training

4. Physical Security –

Authority: CJIS Security Policy:

1.1 – Purpose

3.2.2 – CJIS Systems Officers

5.8.3 – Disposal of All Media

5.9.1 – Physically Secure Location

4.2.3 – Storage

Appendix C.5 – FBI Security Addendum

GCIC Council Rules (2007) 140-2-.02 – Security Policy for Criminal Justice Information Assessment:

- ⌚ Security of Live Scan or Automated Fingerprint Identification System (AFIS)
- ⌚ Storage of criminal history data
- ⌚ Disposal of criminal history data
- ⌚ Physical Security of office/agency or area in which criminal history data is stored

5. Information Security –

Authority: CJIS Security Policy:

4.2 – Standards and Discipline

5.9.1 – Physically Secure Location

5.9.1.1 – Non-secure Locations

5.9.1.1 – Authentication/Passwords

4.2 – Use and Dissemination of CHRI and NCIC Hot File Information

4.2.2 – Proper Access to and Use of CHRI

4.2.4.1 – Justification

5.4.7 – Logging

Appendix J – Transfers of FBI CJIS CHRI via the Internet

4.2.3 – Storage

Appendix C.5 – Security Violations

Appendix C.7 – Robust Passwords

Appendix C.10 – WLAN Security Plan Guidelines

GCIC Council Rules (2007) – 140-2-.04 – Consent

Assessment:

User ID / Passwords

Access and/or receipt of CHRI

Storage of CHRI

Consent for CHRI access

Purpose of request

Dissemination of CHRI

Fingerprinting process

Disciplinary policy

Please refer to the training cd for additional information contained in the CJIS Security Policy, GCIC Council Rules and the Outsourcing Standard. All of the above audit assessment areas are based on these documents.

****Please be advised that the security policy contained on the training cd should not be posted on public websites or in public areas and is not to be disseminated outside of official channels.***

Sanctions for Noncriminal Justice Agency Violations

Agencies are subject to GCIC administrative sanctions for violation of the laws governing the operation of the CJIS network, of the GCIC Council Rules, GCIC CJIS Security Policy or of CJIS network policies published by GCIC. Sanctions for noncriminal justice agencies may include, but are not limited to: access and suspension/revocation of the agencies' access to the GAPS network.

Failure to abide by federal and state laws, federal rules and regulations, and Georgia Crime Information Center (GCIC) Rules regarding access, use and dissemination of information available via the Criminal Justice Information System (CJIS) Network may result in criminal prosecution by the State of Georgia and/or administrative sanctions by the employing agency.

1. All local agencies *must* have disciplinary procedures that address violations of GCIC Rules, Georgia law, or federal rules and regulations relative to the GCIC/NCIC Criminal Justice Information System (GCIC Rule 140-2-.09).
2. The preferred process is for the agency head to take appropriate disciplinary action against the employee to prevent further policy violations. Agency heads are encouraged to create an environment of compliance within their departments by following normal accepted disciplinary procedures to ensure full compliance by all employees.
3. If the disciplinary action against an employee is not appropriate for the violation, GCIC reserves the right to implement additional sanctions on the individual(s)/agency involved.
4. The sanctions may include, but are not limited, to:

Removal of authority to access the GAPS network and criminal history record information Mandatory retraining in the form of the completion of another Security and Integrity Training Update class/Security and Awareness Video After completion of any training, the operator shall read and sign an updated GCIC Awareness Statement.

5. Individual violators are also subject to criminal prosecution when their actions constitute violations of applicable state and federal statutes (GCIC Rule 140-2-.20).

Contacts

CCH: Agencies with criminal history questions should contact the GCIC Criminal History/Identification Services at (404) 244-2639.

Compliance: Agencies with compliance or audit questions should contact their respective auditor. (Please see Appendix "E".)

Customer Support and Training: Agencies with questions regarding training and access to CHRI should contact their respective customer support representative. (Please see Appendix "F").

Helpful Resources

- **Authorization for FBI Fingerprint Checks:**

<http://gicweb.gbi.state.ga.us/cjis/ori/Authorization%20for%20FBI%20Fingerprint%20Checks.pdf>

(Also included on the training cd)

- **CJIS Security Policy:** *(please refer to the training cd for a copy of this document – be advised that this security policy should not be posted on public websites or in public areas nor should it be disseminated outside of official channels).*

- **Compact Council Website:** www.fbi.gov/hq/cjisd/web%20page/cc.htm

- **GAPS Website:** www.ga.cogentid.com

- **GCIC Council Rules:** www.gbi.georgia.gov

Record Challenges

http://gbi.georgia.gov/00/channel_modifieddate/0,2096,67862954_67866875,00.html

🕒 Click on the Georgia Crime Information Center Link in the center of the page

🕒 Scroll to the bottom of the page and click on the pdf file entitled “Official Rules of Georgia Crime Information Center”

(Also included on the training cd)

- **GTA Website for Training of Non-ORI agencies:**

http://gta.georgia.gov/00/article/0,2086,1070969_84340779_110482448,00.html

- **Outsourcing Standard:** *(please refer to the training cd)*

Terms, Definitions and Acronyms

Access to CHRI - to use, exchange, retain/store, or view CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means.

Administration of Criminal Justice - the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment.

Agency Head - The individual responsible for daily activities at the local department office and is authorized to sign the Audit Questionnaire.

Audit - the independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures and to recommend any indicated changes in controls, policy, or procedures.

Audit Logging - the process of gathering and saving information in a written or automated electronic form to record the session initiation and termination messages, logins and failed login attempts, logout, file access or other various activities to include all forms of access violations such as attempts to access data beyond the level of authorized access.

Authorized Recipient - (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes. **Authorized User** - an individual who has been appropriately vetted, has been properly trained in livescan submissions and has been authorized to access CJIS Data.

Background Check - a check of all appropriate information sources to include a state of residency and national 10-print fingerprint-based record check

CJIS Data - data considered to be criminal justice in nature to include images, files, records, and intelligence information. FBI CJIS data is information derived from state or Federal CJIS systems.

CJIS Systems - computer network infrastructure dedicated to criminal justice uses that facilitate interfaces with the national CJIS Division systems.

Compact Council – The National Crime Prevention and Privacy Compact Council (Compact Council) is a 15-member body of local, state and federal government officials which prescribes system rules and procedures for the effective and proper operation of the Interstate Identification Index (III) for noncriminal justice purposes.

Contractor - a government agency, a private business, non-profit organization or individual, that is not itself an authorized recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an authorized recipient to perform noncriminal justice administrative functions requiring access to CHRI.

Criminal History Record Check - for the purposes of this guide only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository (GCIC) and/or the FBI system.

Criminal History Record Information - arrest-based data and any derivative information from that record, i.e. descriptive data, FBI number, conviction status, sentencing data, incarceration, probation and parole information.

Criminal Justice Agency - the courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Purposes - See Administration of Criminal Justice.

FBI CJIS data - is information derived from the national CJIS Division systems.

Logging - the process of storing information about events that occurred on the firewall, host system, or network. This process creates audit logs.

Misuse - illicit activity that exploits system vulnerabilities or file access privileges.

Noncriminal Justice Administrative Functions - the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:

1. Making fitness determinations/recommendations
2. Obtaining missing dispositions
3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
4. Other authorized activities relating to the general handling, use, and storage of CHRI

Noncriminal Justice Agency - a governmental agency or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

Noncriminal Justice Purpose - the uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Originating Agency Code (OAC) - a unique alphanumeric number assigned by GCIC to public and private entities. An OAC is required to obtain a Georgia criminal history record check.

Originating Agency Identifiers (ORIs) - a unique alphanumeric number assigned by the FBI to individual law enforcement or other authorized government agencies. An ORI is required to obtain a FBI record check. The FBI will not process any request that does not have an ORI.

Outsourcing Standard - a document approved by the Compact Council which is to be incorporated by reference into a contract between an authorized recipient of CHRI and a contractor. This document authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.

Password - a string of characters used to authenticate an identity or to verify access authorization.

Physical Security - (1) The measures used to provide physical protection of resources against deliberate and accidental threats. (2) The protection of building sites and equipment (and information and software contained therein) from theft, vandalism, natural and manmade disasters, and accidental damage.

Physically Secure Location - a location where CHRI can be obtained and adequate protection is provided to prevent any unauthorized access to CHRI.

Positive Identification - a determination based upon a comparison of fingerprints or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identification based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, *shall not* constitute positive identification.

Robust Passwords - secure password attributes. The users must follow the strong password construction guidelines which include upper case letters, lower case letters, numbers and symbols.

Secondary Dissemination - the re-dissemination of FBI CJIS data or records from an authorized agency that has direct access to the data to another authorized agency.

Security Requirements - types and levels of protection necessary for a system to maintain an acceptable level of security.

Security Violation - the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

Terminal Agency Coordinator (TAC) - generally, the primary point of contact at the local level which serves as liaison between the CJIS Systems Officer and the local agencies that have access to a CJIS Systems Agency criminal justice network. The responsibilities afforded to the TAC may vary from state to state.

Unauthorized Access - illegally obtaining access to an area, system or resource that has been designated for authorized personnel only.

User Agreements - a current, signed written agreement with the appropriate signatory authority of the CJIS Systems Agency (CSA) that will authorize the provision of said access set forth within the agreement. The agreement will refer to the necessary security-related provisions therein. The CSA for Georgia is the Georgia Crime Information Center.

User ID Identification - any of several methods utilizing a unique symbol or character string used by an automated information system to recognize a specific user.

Acronyms

AFIS Automated Fingerprint Identification System
CHRI Criminal History Record Information
CJIS Criminal Justice Information Services
CSA CJIS Systems Agency (GCIC)
DFACS Department of Family and Children Services
FBI Federal Bureau of Investigation
FIRS Fingerprint Identification Record System
GAPS Georgia Applicant Processing Service
GBI Georgia Bureau of Investigation
GCIC Georgia Crime Information Center
III Interstate Identification Index
IT Information Technology
LAN Local Area Network
NCIC National Crime Information Center
NCJA Non-criminal Justice Agency
OAC Originating Agency Code
ORI Originating Agency Identifier
PC Personal Computer
SIB State Identification Bureau
TAC Terminal Agency Coordinator
VPN Virtual Private Network
WAN Wide Area Network

Appendix A

(Revision Date October 2008)

Georgia Public Law 92-544 Statutes Requiring/Authorizing National Fingerprint based Background Checks for Licensing/Employment Purposes by Governmental Entities

1. O.C.G.A. §§ 3-3-1 Alcohol Beverage Control Applicant, Retail Liquor and 3-3-2 License
2. O.C.G.A. § 7-1-682 (d), (e) Check or Money Order Licensee, Applicant or Employee
3. O.C.G.A. § 7-1-702 (c), (d) Check Cashing Business Licensee or Employee
4. O.C.G.A. § 7-1-1004 (e), (f) Mortgage License Applicant or Employee
5. O.C.G.A. § 10-9-9 Georgia World Congress Center Officers/Employees
6. O.C.G.A. § 16-11-129 Pistol Permit
7. O.C.G.A. § 17-6-50 Professional Bondsman
8. O.C.G.A. § 19-8-16 (d) Petitioners for Adoption
9. O.C.G.A. § 20-1A-34 GA Dept. of Early Care & Learning – Directors, Owners and Employees of Child Care Centers, Group Day Care Homes and Family Day Care Homes
10. O.C.G.A. § 20-2-211 School Teacher, Principal, Other Certified Professional and all Persons Employed in Local School Districts

11. O.C.G.A. § 25-4-8 Firefighter Applicant
12. O.C.G.A. § 31-7-254 Personal Care Homes – Licensing of Directors
O.C.G.A. § 31-7-259 Personal Care Homes – Director or Employee
During Abuse Investigation
13. O.C.G.A. § 33-23-5.1 Dept. of Insurance – licensing applicants for agencies, agents, subagents, counselors and adjusters
14. O.C.G.A. § 35-3-33 (15) Bar Admission Applicant
15. O.C.G.A. § 35-3-35 (a)(1) Delegates authority to obtain national background checks by the governing authority of any county or municipality on any applicant or licensee in a specified occupation for which such local governing authority has adopted an ordinance or resolution
 - A. City of Doraville – Petroleum Terminal Operators Ordinance No. 07-08
16. O.C.G.A. § 35-8-8 (b) Students Attending Pre-service POST (submitted Authorization for State/Federal Fingerprint Background Checks October 2008 by authorized CJ agency)
17. O.C.G.A. § 38-3-27 Local Emergency Management Director Applicant
18. O.C.G.A. § 40-5-82 Operator/Instructor of a DUI of Alcohol or Drug Use Risk Reduction Program
19. O.C.G.A. § 43-12A-4 Dept. of Driver Services Applicants for Certification as Ignition Interlock Device Providers
20. O.C.G.A. § 43-26-7 Registered Professional Nurses
21. O.C.G.A. §§ 43-38-6/7/7.1 Private Detective/Private Security Business License and Registration of the Licensee’s Detectives and Security Guards
22. O.C.G.A. § 43-39A-22.1 Real Estate Appraisers
23. O.C.G.A. § 43-40-27.1 Real Estate Brokers and Salespersons
24. O.C.G.A. § 43-47-6 Used Motor Vehicle & Used Motor Vehicle Parts Dealer License
25. O.C.G.A. § 49-2-14 Department of Human Resources
 - A. Applicants for employment with GA DHR, contractors, district or county health agencies which duties involve direct care, treatment or custodial responsibilities of its’ clients.

B. Any adult person residing in a home where children in the custody of GA DHR have been or may be placed or any adult who resides in the home of or provides care to a child who is the subject of a child protective services referral, complaint or investigation. Includes placement of children in exigent circumstances.

26. O.C.G.A. § 49-2-14.1 DHR Facilities Licensing to include Personal Care Homes, Private Home Care, Community Living Arrangements and Child Welfare Agencies
27. O.C.G.A. § 49-5-64 Licensing of Directors and Employees of Child Care Centers
28. O.C.G.A. § 49-5-69.1 Foster Parents or Other Adult Persons Residing in Homes Providing Care to Children

National Child Protection Act/Volunteers for Children Act (NCPA/VCA)

1. O.C.G.A. § 35-3-34.2 Public Agency Employment for: Child Care Provider/Care Placement Mental Health Care Provider/Care Placement Elder Care Provider/Care Placement

Volunteer for:

 - Child Care
 - Mental Health Care
 - Elder Care

**Adam Walsh Child Protection and Safety Act
Section 153 – Schools Safely Acquiring Faculty Excellence (SAFE) Act**

1. Public Law 109-248 Public and Private Elementary and Secondary Schools and State and Local Educational Agencies

Law Enforcement/Criminal Justice Purpose – No User Fee

1. O.C.G.A. § 15-16-1 Candidate for Sheriff (submitted by Probate Court)
2. O.C.G.A. § 35-8-8 Peace Officers Standards & Training Council (submitted by authorized CJ agency)

**Appendix B
Georgia Bureau of Investigation
Georgia Crime Information Center
Consent Form**

I hereby authorize _____
to receive any Georgia criminal history record information pertaining to me which may be in the files of any state or local criminal justice agency in Georgia.

Full Name (print)

Address

Sex Race Date of Birth Social Security Number

Signature

Date

Special employment provisions (check if applicable):

- Employment with mentally disabled (Purpose code 'M')
- Employment with elder care (Purpose code 'N')
- Employment with children (Purpose code 'W')
- Employment with criminal justice agency – civilian (Purpose code 'J')
- Employment with criminal justice agency – P.O.S.T. certified (Purpose code 'Z')

One of the following must be checked:

- This authorization is valid for 90/180/ _____ (circle one) days from date of signature.
- I, _____ give consent to the above named to perform periodic criminal history background checks for the duration of my employment with this company. 27 **Appendix C**

**GEORGIA CRIME INFORMATION CENTER
AWARENESS STATEMENT**

Access to Criminal Justice Information, as defined in GCIC Council Rule 140-1-.02 (amended), and dissemination of such information are governed by state and federal laws and GCIC Council Rules. Criminal Justice Information cannot be accessed or disseminated by any employee except as directed by superiors and as authorized by approved standard operating procedures which are based on controlling state and federal laws, relevant federal regulations, and the Rules of the GCIC Council.

O.C.G.A. §35-3-38 establishes criminal penalties for specific offenses involving obtaining, using, or disseminating criminal history record information except as permitted by law. The same statute establishes criminal penalties for disclosing or attempting to disclose techniques or

methods employed to ensure the security and privacy of information or data contained in Georgia criminal justice information systems.

The Georgia Computer Systems Protection Act (O.C.G.A. §16-9-90 et seq) provides for the protection of public and private sector computer systems, including communications links to such computer systems. The Act establishes four criminal offenses, all major felonies, for violations of the Act: Computer Theft, Computer Trespass, Computer Invasion of Privacy, and Computer Forgery. The criminal penalties for each offense carries maximum sentences of fifteen (15) years in prison and/or fines up to \$50,000.00, as well as possible civil ramifications. The Act also establishes Computer Password Disclosure as a criminal offense with penalties of one (1) year in prison and/or a \$5000.00 fine.

The Georgia Criminal Justice Information System Network is operated by the Georgia Crime Information Center in compliance with O.C.G.A. §35-3-31. All data bases accessible via CJIS Network terminals are protected by the Computer Systems Protection Act. Similar communications and computer systems operated by municipal/county governments are also protected by the Act.

By my signature below, I acknowledge that I have read and understand this Awareness Statement.

Print Name:

Signed: Date:

Witnessed: Date: 28

Appendix D
Georgia Crime Information Center
Service Agreement

Criminal History Record Checks by Employers and Licensing Authorities

Georgia law authorizes the Georgia Crime Information Center (GCIC), a division of the Georgia Bureau of Investigation (GBI), to disseminate criminal history record information to private persons and businesses, public agencies and political subdivisions as provided in the Official Code of Georgia (O.C.G.A) §§ 35-3-34 and 35-3-35. Certain agencies are authorized by Georgia and federal law to obtain a national criminal history record check. Federal law, commonly referred to as Public Law (Pub. L.) 92-544, requires that a state enact a statute authorizing the check of national criminal history records. The state statute must be specific in nature, identify the category of applicants, require fingerprinting of the applicants and authorize submission of the fingerprints to the FBI for a national criminal history record check. Public agencies with this authority must have a Federal Bureau of Investigation (FBI) assigned Originating Agency Identifier (ORI). Agencies authorized to obtain only a Georgia criminal history record check must have a GCIC assigned Originating Agency Code (OAC). The agency head for each authorized agency or licensing authority must also designate an agency contact. The agency head and contact will sign a GCIC Service Agreement and will receive criminal history record information from GCIC (and the FBI when authorized) on behalf of any private person, business, commercial establishment or authorized governmental agency eligible to request such information. GCIC must be notified in writing whenever there is a change in the agency head or contact and the new agency head or contact must sign a new Service Agreement. Service Agreements must be re-signed **every two (2) years**, even if the agency head or contact remains the same.

Requesting agencies shall provide the fingerprints of individuals whose records are being requested in a manner prescribed by the GCIC and with the appropriate fee. Agencies should inform each individual that his or her fingerprints will be used to perform Georgia and FBI (when authorized) criminal history record checks for the purpose of determining suitability for licensing or employment.

When the results of a criminal history record check cause an adverse employment or licensing decision, Georgia law requires that the applicant must be informed by the individual, business or agency making the adverse decision of all information pertinent to that decision. This disclosure must include information that a criminal history record check was conducted, the specific contents of the record, and the affect the record had upon the employment/licensing decision. O.C.G.A. §§ 35-3-34(b) and 35-3-35(b) classifies failure to provide all such information to the person subject to the adverse decision as a misdemeanor offense. Use of Georgia and FBI criminal history records 29 30

obtained under this Service Agreement are solely for the purpose requested and cannot be disseminated outside the receiving agency. O.C.G.A. § 35-3-38 establishes criminal penalties for requesting, obtaining, communicating or attempting to communicate criminal history record information under false pretenses or in a negligent manner. All criminal history record information received from GCIC and/or the FBI for background check purposes shall be stored in a secure location. Areas in which the information is processed and handled shall be restricted to authorized personnel in the performance of their duties. When such information is no longer needed, it shall be destroyed by burning, shredding or other method rendering the information unreadable.

Agencies utilizing this service agree to keep all records necessary to facilitate a security audit by the GCIC and to cooperate in such audits as GCIC or other authorities may deem necessary. Examples of records that may be subject to audit are: criminal history records, notification that an individual has no criminal history, agency policies and procedures articulating the provisions for physical security, records of all disseminations of criminal history record information, and a current executed Service Agreement with GCIC.

Employers or licensing authorities assume liability for fees incurred with all fingerprint submissions, including fingerprints submitted as undocumented duplicate submissions, fingerprints submitted in error, unannounced test records, etc. Agencies mailing applicant fingerprint cards directly to GCIC may arrange with the GBI Finance Office to be billed for these services. However, agencies submitting applicant fingerprint cards electronically to GCIC must establish billing arrangements prior to beginning submissions. Agencies submitting fingerprint submissions to GCIC via the Georgia Applicant Print Service (GAPS) must register and make payment arrangements with Cogent Systems, Inc. prior to beginning submissions.

All agencies that are billed for services must maintain fiscal responsibility. Failure to comply with the terms of the GBI Finance Billing Agreement will result in termination of the billing arrangement and can result in termination of this Service Agreement. Agencies submitting requests via the GAPS must comply with fee schedules and payment requirements as outlined in that program. GCIC will provide this service as long as a valid Service Agreement exists.

Georgia Crime Information Center (GCIC)
Service Agreement
Criminal History Record Checks by Employers and Licensing Authorities

Agency Name
Agency Address
City/State/Zip Code
Agency Mailing Address
City/State/Zip Code
Agency Phone Number
Agency Email Address
Agency ORI or OAC#
(As assigned by FBI or GCIC)

NOTE: If your agency/business does not have an ORI or OAC number, leave the ORI or OAC field blank. An ORI or OAC will be assigned to your agency and mailed to the above address.

31

IMPORTANT: The agency head, or designee, of a non-criminal justice agency, i.e. State, County or City government, public or private school requesting an ORI number must submit a letter, on agency letterhead, with a brief description of services provided. Additionally, the request must state whether the agency is requesting an ORI to conduct FBI fingerprint-based record checks under the authority of 1) a specific state law (O.C.G.A.) that is a FBI approved Public Law (Pub. L.) 92-544 statute or, 2) federal authority (such as the Adam Walsh Child Protection and Safety Act. Further information may be necessary for ORI requests submitted for FBI record checks under federal authority to verify the entity qualifies as an authorized entity under the authority.