GBI Policies and Procedures for Fingerprinting Fire Personnel

Presented by Hilary Huett, CJIS Training Specialist, Non-Criminal Justice Unit, Georgia Bureau of Investigation
Learning Objectives

• Establish necessity of obtaining fingerprint-based background checks for employment

• Explore policy regarding use and dissemination of CHRI as it pertains to state and federal regulations

• Discuss the Applicant Privacy Rights and Privacy Act Statement requirement

• Examine the NCJ audit process

• Take time to discuss questions and answers with conference attendees
Authorization to Obtain Results

• State statute establishes authority to obtain national criminal history results under Federal Law 92-544, Title 34 U.S.C. §41101
O.C.G.A. § 25-4-8

• Establishes fingerprinting mandate for Georgia firefighters

• (c)(1) The local or state law enforcement agency shall submit to the Georgia Crime Information Center two complete sets of fingerprints of the applicant for appointment or employment, the required records search fees, and such other information as may be required. Upon receipt thereof, the Georgia Crime Information Center shall promptly transmit one set of fingerprints to the Federal Bureau of Investigation for a search of bureau records and an appropriate report and shall retain the other set and promptly conduct a search of its own records and records to which it has access. The Georgia Crime Information Center shall notify the local or state law enforcement agency in writing of any derogatory finding, including, but not limited to, any conviction data regarding the fingerprint records check or if there is no such finding. All conviction data received by the local or state law enforcement agency shall not be a public record, shall be privileged, and shall not be disclosed to any other person or agency except as provided in this subsection and except to any person or agency which otherwise has a legal right to inspect the employment file. All such records shall be maintained by the local or state agency pursuant to laws regarding such records and the rules and regulations of the Federal Bureau of Investigation and the Georgia Crime Information Center, as applicable.
Why Fingerprint-Based Background Checks?

Establish necessity of obtaining fingerprint-based background checks for employment
Criminal History Record Checks

Name Based
• Based on demographics
• Name changes
• State of Georgia only
• 3rd party check

Fingerprint Based
• Based on biometrics
• Fingerprints are unique
• GCIC information
• National results
Criminal Prints

- Taken at the time of arrest
- Maintained by GCIC via AFIS

Civil Prints

- Submitted by applicant
- Civil prints not retained in GA
Fingerprint Process

1. NCJA to GBI
2. GBI to FBI
3. FBI to CHRI
4. CHRI to IDHS

- NCJA
- GBI
- FBI
- IDHS
- CHRI
Policy on Use and Dissemination

Explore policy regarding use and dissemination of CHRI as it pertains to state and federal regulations.
The Criminal Justice Information Services (CJIS) Security Policy includes a number of technical safeguards designed to protect and secure criminal justice information. Compliance with this policy is mandatory for any agencies requiring access to FBI CJIS Division systems and information.
Authorized Use of CHRI

- Employment
- Licensing
- Volunteers
Dissemination and Use

- O.C.G.A. §35-3-38 establishes criminal penalties for requesting, obtaining, communicating or attempting to communicate CHRI 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.
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).
What is Considered CHRI?

- Any document, note, etc. that eludes to the existence or non-existence of a criminal history.
  - Can include notes, details within certification packet, emails, determination letters, etc.

John Doe
SID Number
GA12345678
Felony >10 years ago
Secondary Dissemination Log

Dissemination log should include:

- Name
- Transaction Control Number (TCN)
- Date
- Applicant signature
NEVER store CHRI in personnel files.
Destruction

Cross-cut shredding
Burning
Things to consider when sharing CHRI:

- Am I authorized to release this CHRI outside of my department?
- Did I verify the ID of this applicant before releasing the IDHS?
- Does this person have a need for this CHRI or are they just curious?
- Do I need to log this dissemination of CHRI?
Security Awareness Training

- Within 60 days of assignment
- Every 2 years
Applicant Privacy Rights

Discuss the Applicant Privacy Rights and Privacy Act Statement requirement
Applicant Privacy Rights
Applicant’s criminal history record information must be handled in a manner that protects the applicant’s privacy.
Provide the applicant written notice that his/her fingerprints will be used to check the criminal history records of the GBI and FBI.
Provide the applicant the opportunity to complete or challenge the accuracy of the information in the record.
List
procedures for obtaining a change, correction, or updating of an GBI/ FBI criminal history record.
Information

in the criminal history record should not be used to deny a job, license or other benefits until an applicant has been given the opportunity to correct or challenge their record or declined to do so.
Criminal History Records
must be used solely for the purpose requested.
Agency policy may dictate whether or not a copy of the criminal history record can be provided to the applicant.
Never disseminate CHRI outside of the receiving department, related agency, or other authorized entity unless authorized by law.
Time allowed to correct or complete criminal history records, and any appeals process that is afforded the applicant should reasonable and documented by the agency.
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.

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.

NON-CRIMINAL JUSTICE APPLICANT’S PRIVACY RIGHTS

As an applicant that is the subject of a Georgia only or a Georgia and Federal Bureau of Investigation (FBI) national fingerprint/biometric-based criminal history record check for a non-criminal justice purpose (such as an application for a job or license, immigration or naturalization, security clearance, or adoption), you have certain rights which are discussed below.

- You must be provided written notification that your fingerprints/biometrics will be used to check the criminal history records maintained by the Georgia Crime Information Center (GCIC) and the FBI when a federal record check is so authorized.
- If your fingerprints/biometrics are used to conduct a FBI national criminal history check, you are provided a copy of the Privacy Act Statement that would normally appear on the FBI fingerprint card.
- If you have a criminal history record, the agency 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 agency must advise you of the procedures for changing, correcting, or updating your criminal history record as set forth in Title 28, Code of Federal Regulations (CFR), Section 16.34.
- If you have a Georgia or FBI 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 agency denies you the job, license or other benefit based on information in the criminal history record.
- In the event an adverse employment or licensing decision is made, you must be informed of all information pertinent to that decision to include the contents of the record and the effect the record had upon the decision. Failure to provide all such information to the person subject to the adverse decision shall be a misdemeanor (O.C.G.A. § 35-3-34(b) and 35-3-35(a)).

You have the right to expect the agency 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 state and/or federal statute, regulation or executive order, rule, procedure or standard established by the National Crime Prevention and Privacy Compact Council.

If the employment/licensing agency policy permits, the agency may provide you with a copy of your Georgia or FBI criminal history record for review and possible challenge. If agency policy does not permit it to provide you a copy of the record, information regarding how to obtain a copy of your Georgia, FBI or other state criminal history may be obtained at the GBI website (http://gbi.georgia.gov/obtaining-criminal-history-record-information).

If you decide to challenge the accuracy or completeness of your Georgia or FBI criminal history record, you should send your challenge to the agency that contributed the questioned information. Alternatively, you may send your challenge directly to GCIC provided the disputed arrest occurred in Georgia. Instructions to dispute the accuracy of your criminal history can be obtained at the GBI website (http://gbi.georgia.gov/obtaining-criminal-history-record-information).
NCJ Audit Process
<table>
<thead>
<tr>
<th>Territory</th>
<th>Compliance Auditor</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>North</td>
<td>Wes Anderson</td>
<td>404-783-2657</td>
</tr>
<tr>
<td>Metro/Southwest</td>
<td>Corella Mosen</td>
<td>404-821-1092</td>
</tr>
<tr>
<td>Central</td>
<td>Abigail Krogh</td>
<td>470-548-4788</td>
</tr>
<tr>
<td>East</td>
<td>Samantha Balkaran</td>
<td>678-371-2177</td>
</tr>
<tr>
<td>South</td>
<td>Greg Houston</td>
<td>404-273-6235</td>
</tr>
<tr>
<td>NCJ Trainers</td>
<td>Hilary Huett</td>
<td>404-519-9285</td>
</tr>
<tr>
<td></td>
<td>Shauntrice Montgomery</td>
<td>678-371-8887</td>
</tr>
</tbody>
</table>
Audits

WHAT

WHEN

WHY

HOW

WHO

WHERE
Audit Documentation

- User Agreements
- Training Records
- Policies
- Applications
- Privacy Rights
- Fingerprint Survey
- Outsourcing
User Agreements

Signed within the last 2 years listing current agency head and POC.

(located on the Applicant Services Blog)
Identify each employee, contractor, vendor, volunteer, etc. who has access to CHRI and maintain a list.
Policies

✓ Disciplinary
✓ Media Protection
✓ Natural/Man-Made Disaster
✓ Applicant Privacy Rights Notification

Samples of each policy are located on the Applicant Services Blog however, each policy should be modified and be agency specific.
Fingerprint Survey & Applications

Agencies will need to provide applications for each applicant fingerprinted under the ORI assigned to the agency.

Sample fingerprint survey is located on the Applicant Services Blog.
Pre-Audit

A preliminary E-Audit will be sent to the agency’s POC approximately 15 to 30 days prior to the onsite audit.

The E-Audit will contain important documentation which **must** be completed prior to the onsite audit.
On-site Audit

The auditor will contact the POC to schedule the onsite Audit once the E-Audit documentation has been received.

The POC must be onsite during the audit and prepared to provide all documentation requested during the audit.
If your agency is found out of compliance, you will get an E-Audit notification via email to include an “Agency Response” on all out-of-compliance areas. Your agency has ten (10) days to respond.
Congratulations

If an agency is found to be in full compliance, a “Final Response Notification” will be sent via email to the agency.
Common Areas of Non-Compliance

- Applicant Privacy Rights Notification
- Storage and Security of CHRI
- Security Awareness Training