	Department of Human Services Online Directives Information System	Index: Revised: Next Review:	POL1753 10/04/2019 10/04/2021

SUBJECT: Maintenance, Destruction, And Protection of Criminal History Records

Policy:

The Policy of the Department of Human Resources (DHS) Office of Inspector General (OIG) Background Investigations Unit (BIU) is to manage the maintenance and storage of all criminal history records information (CHRI) and summaries of investigations.

A. Authority

None

B. References

Criminal Justice Information Services (CJIS) Security Policy Version 5.2, 2013
Georgia Crime and Information Center Policy Manual Rev. 2011
Georgia Crime Information Council Rules, October 2007

C. Applicability

Any employee authorized by OIG to capture and/or transmit fingerprints via an electronic fingerprinting machine, who accesses the GCIC Network Terminal, and/or who have access to Criminal History Record Information.

D. Definitions

Criminal History Record Information (CHRI): Records that include direct responses from GCIC and National Crime Information Center (NCIC) received as a result of the submission of electronic fingerprints or GCIC Query Terminal responses

E. Responsibilities

1. When not in use, all criminal history records information (CHRI) and summaries of investigations will be secured in locked cabinets within a controlled access area in OIG/BIU. This area must be restricted to authorized OIG BIU personnel in the performance of their official duties.
2. All original GCIC/NCIC criminal history records must remain in the BIU secured area or storage containers under lock and key.
3. FBI/GBI encryption requirements must be followed for electronic storage of criminal history records information and data.
4. Hard copies of each request for criminal background checks must be printed and stored by date in a locked container for a period of three (3) years, except for records for employment which are kept indefinitely. CHRI records for ORS Licensed Facilities and contractors are maintained for a period of seven (7) years.
5. All information system devices (including computer monitor screens) must be positioned to prevent access or view by unauthorized persons.
6. Criminal history records in the custody of OIG BIU can only be reviewed by authorized DHS personnel who have successfully completed the GBI/GCIC Security and Integrity training (S&I) within the past two years; records can be

viewed **only** in the presence of authorized OIG BIU S&I trained personnel. Any DHS personnel who wish to access and/or review CHRI must have a signed and current GCIC Awareness Statement on file with OIG BIU.

7. OIG/BIU GCIC/NCIC criminal history records can only be audited by the Georgia Bureau of Investigation (GBI) or the Federal Bureau of Investigation (FBI). Any other entity wishing to perform an audit of the GCIC/NCIC criminal history records must obtain prior authorization from the GBI.

Destruction of criminal history records

- When no longer required to support criminal justice operations, all documents containing CHRI
- will be destroyed to preclude access by unauthorized persons.

- The destruction of criminal history records will be coordinated by the BIU Special Agent in
- Charge and the designated TAC and will be performed in a secure manner.

- The only approved method of destruction for criminal history records is shredding using a cross- cut shredder. A record of destruction of all criminal history records will be maintained by the TAC indicating the content, time, date, and purpose of the destruction of each record.

Destruction of electronic media

- Electronic media and data containing criminal history records information must be disposed of or destroyed in compliance with FBI and GCIC regulations governing the security and integrity of criminal history records. These measures must be taken to protect against unauthorized access to or use of records and information/data, and properly sanitize or destroy electronic media, information and data.

- **Hard Drives (PCs)**: Destruction of OIG BIU electronic records must be by erasing, or otherwise modifying the information of the record to make the record unreadable, undecipherable or unreconstructedly through generally available means. Means include, but are not limited to, degaussing or pulverizing the drive. Information that is stored electronically must be made irretrievable before disposal, for example, by overwriting the electronic file at least three times.

- **Hard Drives (MFPs)**: OIG BIU multifunctional devices (copiers, FAX machines, network printers and scan to email) that utilize hard drives to temporarily store data or images will be configured to immediately overwrite (delete) the data once transmitted to the destination. At the end of the product life cycle, the agency may purchase the hard drive to be degaussed or pulverized, rendering any data remaining on the drive irretrievable.

- **FLASH Drives**: OIG flash drives used for the portability of OIG BIU data must always be kept in the possession of the OIG authorized employee. Flash drives will be destroyed at the end of the life cycle. Destruction will be by pulverizing the drives, thus rendering them useless.

Physical Security and Security of Electronic Media:

- Physical security of paper CHRI files and electronic security of electronic media during a natural or manmade disaster will be in accordance with the OIG BIU Business Continuity Plan.

Protection of records during a natural or man-made disaster

- In the event of a natural or man-made disaster, the OIG BIU Special Agent in Charge and/or appointed designee will have the responsibility of ensuring that records maintained by the OIG BIU are secured and not in danger of being damaged or destroyed.
- In the event, that Department criminal history records are not secured or have been damaged and/or destroyed, the OIG BIU Special Agent in Charge will immediately notify the Inspector General and the GCIC. Depending on the circumstances, an OIG staff member or Capitol Police will be stationed in the area to secure the criminal history records area until corrective action can be taken, if necessary. Impacted areas include the three (3) work sections where OIG BIU records are held: GCIC Information Records, Live Scan and DHS Personnel and Contractors.

- The OIG BIU Special Agent in Charge will be responsible for taking the necessary steps to ensure that all records are secured on site or that such records are removed to another location where they can be secured until they can be returned and secured within the OIG BIU site.

F. History

Policy 1753, last reviewed 10/04/2019

G. Evaluation

The DHS OIG BIU Manager/Supervisor evaluates this policy by:

1. Completing quarterly internal audits to ensure responsibilities, certification, and dissemination are performed accurately and efficiently by each employee.
2. Passing any audit with no findings.