Rules

Of The
Georgia
Crime Information
Center Council

October 2007

Rules
Of The
Georgia Crime Information Center Council

Chapter 140-1

Organization

Table of Contents

140-1-.01 Organization. Amended.

(1) There is a Director responsible for development, maintenance and operation of the Georgia Crime Information Center (GCIC).

(2) There is a Council responsible for providing assistance and guidance. The GCIC Director or designee shall attend all Council meetings and maintain records of the proceedings.

(3) All legal notices and correspondence regarding administrative proceedings shall be directed to the GCIC Director.

(4) The GCIC mailing address is P. O. Box 370748, Decatur, Georgia 30037-0748.

(5) The Georgia Bureau of Investigation (GBI) functions as the State CJIS Systems Agency (CSA) for Georgia per the service agreement between Georgia and the Federal Bureau of Investigation (FBI), CJIS Division.

(6) The GCIC Director provides the Georgia representative to the governing body of the International Justice and Public Safety Information Sharing Network (Nlets) per the service agreement between the GBI and the Executive Director of Nlets.

(7) The GCIC Director serves as the state National Crime Prevention and Privacy Compact officer responsible for administering the compact within the state; ensuring compliance with compact provisions and rules, procedures and standards established by the compact council; and, regulating the in-state use of records received from the FBI or other states party to the compact.

(8) The Rules of the GCIC Council rest on the authority of federal law and rules as well as state law.

Authority: O.C.G.A. §§ 35-3-30, 35-3-31, 35-3-32, 35-3-39.1; 42 U.S.C. 3701, et seq., 42 U.S.C. § 14611-14616, 28 CFR 20, Public Law 92-544. **History.** Original Rule entitled "Organization" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983 as specified by the Agency. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984 as specified by the Agency. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed July 2, 1986, effective July 22, 1986. **Repealed:** New Rule of the same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Repealed:** New Rule, same title, adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-1-.02 General Definitions. Amended.

(1) All words defined in O.C.G.A. § 35-3-30 have the same meaning for these Rules.

(2) The following definitions apply generally to all Rules of the GCIC Council.

(a) Administration of criminal justice – Activities involving 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.

(b) Criminal justice agency – Courts, a governmental agency, or any subunit thereof that performs the administration of criminal justice pursuant to a statute or executive order and that allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

(c) Criminal justice information – Includes the following classes:

1. Criminal History Record Information (CHRI) – Information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising there from including acquittal, sentencing, correctional supervision and release. Such term also includes the age and sex of each victim as provided by criminal justice agencies. 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

2. Restricted data – CJIS network operational procedures, manuals, forms and data gathering techniques

3. Secret data – Information dealing with those operational and programming elements, which prevent unlawful intrusion into the GCIC/CJIS, the communications network and satellite computer systems handling criminal justice information

4. Sensitive data – Statistical information in the form of reports, lists and documents that may identify a group characteristic. It may apply to a group of persons, articles, vehicles, etc. such as white males or stolen guns.

(d) Criminal Justice Information System (CJIS) – All agencies, procedures, mechanisms, media and forms, as well as the information itself, which are or become involved in the organization, transmission, storage, retrieval and dissemination of information related to reported

offenses, offenders and the subsequent actions related to such events or persons.

(e) Designated representative – The person specifically named to receive CHRI from GCIC on behalf of any private person, business and commercial establishment or authorized public agency eligible to request such information.

(f) Disposition – The result of criminal proceedings including information disclosing that arresting agencies elected not to refer the matter to a prosecutor or that a prosecutor elected not to commence criminal proceedings and disclosing the nature of the termination in proceedings or, information disclosing the reason for such postponement.

(g) FBI CJIS and NCIC – The FBI's Criminal Justice Information Services Division (CJIS), which includes the National Crime Information Center (NCIC). The terms FBI CJIS and NCIC may be used interchangeably throughout the Rules.

(h) GCIC CJIS Security Policy – The Information Technology (IT) security program established by GCIC in conformance with the FBI CJIS Security Policy, as amended, which governs the operation of computers, access devices, circuits, hubs, routers, firewalls and other components that make up and support a telecommunications network and related CJIS systems used to process, store or transmit criminal justice information guaranteeing the priority, integrity and availability of service needed by the criminal justice community.

(i) Georgia Crime Information Center (GCIC) as created by O.C.G.A. § 35-3-31.

(j) Governmental dispatch center – A non-criminal justice agency established by an act of local government to provide communications support services to local government agencies, including criminal justice agencies.

(k) Hearing – A right of GCIC and parties affected by any GCIC action to present formally or informally, relevant information, testimony,

documents, evidence and arguments as to why specified actions should or should not be taken.

(l) Hot files – Computerized files maintained by the FBI's CJIS division. These files contain accurate and timely documents related to vehicles, license plates, boats, guns, articles, securities, wanted persons, foreign fugitives, United States Secret Service protective, missing persons, unidentified persons, violent gang and terrorist organizations, deported felons, protective orders, convicted sex offender registries, convicted persons on supervised release and vehicle/boat parts.

(m) Information Security Officer (ISO) – The person designated to administer GCIC's information security program. The ISO is the internal and external point of contact (POC) for all information security matters and ensures that each local agency having access to a criminal justice network has a security POC. {(See Local Agency Security Officer (LASO)}.

(n) Interface – A computer system independent of the State system that transactions must travel through to access the GCIC and FBI CJIS networks, including the NCIC.

(o) Local Agency Security Officer (LASO) – The local agency security POC for agencies that access the GCIC CJIS network.

(p) Management control – The authority to set and enforce priorities; standards for selection, supervision and termination of personnel; and, policy governing the operation of computers, circuits and telecommunications terminals used to process, store or transmit CHRI and /or other criminal justice information.

(q) National Crime Prevention and Privacy Compact – Allows a party state to disseminate its CHRI to other states for non-criminal justice purposes in accordance with the laws of the receiving state. Georgia became a compact state in 1999.

(r) Non-criminal justice agency – Any agency that does not meet the definition of a criminal justice agency.

(s) Non-criminal justice purpose – Using CHRI for purposes authorized by state or federal law other than the administration of criminal justice. Authorized purposes include employment suitability, licensing determinations, immigration and naturalization matters and national security clearances.

(t) Practitioner – An agency employee who accesses the Georgia CJIS network, the FBI CJIS system and other CJIS network databases needed to perform official duties and responsibilities.

(u) Public network – A telecommunications infrastructure consisting of network components not owned, operated and managed solely by a criminal justice agency. This includes, but is not limited to, a common carrier ATM or Frame Relay network where, by design, the redundancy provided is through use of shared public switches within the network cloud. Dedicated criminal justice local or wide area networks (LAN/WAN) that contain no public network component are not considered public networks.

(v) Secondary dissemination – The re-dissemination of CHRI other than for the intended purpose by an authorized recipient to someone unauthorized to receive the CHRI.

(w) Terminal Agency Coordinator (TAC) – An agency employee designated by the agency head to be responsible for ensuring compliance with state and federal policies, regulations and laws established by GCIC, the FBI's CJIS Division and Nlets. Responsibilities include adherence to GCIC/FBI CJIS validation program procedures for specified Georgia and FBI CJIS records.

(x) Terminal operator – An agency employee whose primary job function includes accessing the CJIS network.

(y) The International Justice & Public Safety Information Sharing Network (Nlets) – A message switching network owned by the states that links local, state and federal agencies together to provide the exchange of criminal justice and public safety related information.

(z) User Agreement – A current, signed written agreement between the appropriate signatory authority of the user agency and the Director authorizing the provision of said access set forth within the agreement. The agreement refers to the necessary security-related provisions therein.

Authority: O.C.G.A. § 35-3-30; 28 CFR 20.3**;** FBI CJIS Security Policy as amended. History. Original Rule entitled "General Definitions" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed July 2, 1986, effective July 22, 1986. **Amended:** Filed Jan. 6, 1988, effective Jan. 27, 1988, as specified by the Agency. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Repealed:** New Rule, same title, adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

Chapter 140-1-.03 Administrative Declaratory Rulings. Amended.

(1) Availability of declaratory ruling. Any persons whose legal rights are impaired by the application of any statutory provision or any GCIC Rule or order may petition GCIC and request a declaratory ruling. GCIC will not render advisory opinions, resolve questions that are moot or hypothetical or otherwise act hereunder except in actual controversies or in other cases upon which a superior court would be required to act under the Georgia declaratory judgement statutes as construed by the appellate courts of Georgia.

(2) Form of petition. Each petition filed with GCIC shall be in writing and include:

(a) The name and post office address of the petitioner

(b) The full test of the statute, rule or order upon which a ruling is requested

(c) A detailed statement of all pertinent facts necessary for a determination

(d) The petitioner's contention, if any, as to the applicability of cited legal authorities that authorize, support or require a decision in accordance therewith

(e) A detailed statement setting forth the petitioner's interest in the matter. The statement shall be verified under oath by, or on behalf of, the petitioner.

(3) Proceedings on petition. If GCIC determines a decision can be rendered on the petition without further proceedings, a summary decision shall be rendered. Otherwise, parties shall be notified and the matter reviewed in an informal hearing.

(4) Informal interpretations and rulings

(a) Any person may request GCIC to interpret or otherwise rule informally upon the applicability of any pertinent statute or Rule by personal appearance at GCIC or by letter, telegram or facsimile addressed to the GCIC Director.

(b) GCIC may respond to such requests at its own discretion, or may issue interpretive rulings on its own initiative.

(5) Requests presented in any manner other than in accordance with the provision of 140-1-.03(2) above shall be answered with an informal interpretation.

Authority: O.C.G.A. § 50-13-9. **History.** Original Rule entitled "Administrative Declaratory Rulings" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed July 2, 1986, effective July 22, 1986. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Repealed:** New Rule, same title adopted. Filed Mar. 4, 1998,

effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002; effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-1-.04 Petition for Adoption of Rules. Amended.

(1) Form of petition. Each petition for adoption of Rules pursuant to the Georgia Administrative Procedure Act shall be filed with GCIC in writing under oath and include:

(a) The name and post office address of the petitioner

(b) The full text of the Rule(s) requested to be amended, repealed or promulgated

(c) A detailed statement of why such Rule should be amended, repealed or promulgated, including a statement of the petitioner's interest in the matter

(d) Citations of legal authorities, if any, that authorize, support or require the action requested by the petitioner.

(2) Proceedings on petition. The GCIC Council shall consider each petition at regularly scheduled meetings. The Council may decline to take action or may initiate Rule making or Rule changing proceedings in accordance with the Georgia Administrative Procedure Act. The Council shall notify the petitioner by certified mail of its decision and shall state its reasons if it declines to act.

Authority: O.C.G.A. § 50-13-9. **History.** Original Rule entitled "Petition for Adoption of Rules" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed July 2, 1986, effective July 22, 1986. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Repealed:** New Rule, same title, adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-1-.05 Approval and Disciplinary Procedures. Amended.

(1) Information exchange and service from GCIC. Persons and agencies shall exchange information and receive service from GCIC only when approved by the Director. GCIC shall not provide any service or exchange any information unless the Director finds:

(a) The person or agency is permitted by Georgia law and these Rules to exchange information or receive service

(b) There is no significant danger that the person or agency will use the information or service in a manner that would violate Georgia law, these Rules or applicable federal law or rules.

(2) Notification and resolution of violations. When the Director determines that any law, Rule, regulation or policy of the GCIC Council concerning criminal justice information was violated, is being violated or about to be violated, he shall immediately advise the person or responsible agency head of the existence and nature of such violation. If possible, the Director and concerned parties should agree on a mutually satisfactory resolution, which is documented and signed. Upon review and approval by the GCIC Council, the resolution will be the final disposition of the matter. If the GCIC Council requires modification of the agreement and the concerned parties accept the modification, it shall be the final disposition of the matter. Suspension proceedings are possible when there is failure to agree on a resolution that is satisfactory to the GCIC Council and concerned parties.

(3) Suspension. If an agreement satisfactory to the Director and concerned parties cannot be reached within 45 days of the initial notification of violation the Director may, at his discretion, cause any or all services rendered by GCIC to be suspended. In such cases, the Director shall notify the Chairman of the GCIC Council; however, suspension shall be immediate when major violations exist.

(4) Reinstatement. Upon petition of concerned parties that have had any service suspended the Director may, at his discretion, reinstate full or partial service pending a final decision by the Council, if he finds that reinstatement will not create a significant danger of future violations.

(5) Contested cases. Hearings and appeals regarding refusals by the Director to exchange information or provide services or regarding any disciplinary measure taken by the Director or the GCIC Council pursuant to this Rule shall be conducted pursuant to the Georgia Administrative Procedure Act and the following.

(a) Initiating a contested case. Any person or agency legally entitled to contest a refusal to exchange information, or provide services or to contest any disciplinary measure under this Rule may do so by filing a request for hearing with the Director, which shall include:

1. The complete name and post office address of the party filing the request

2. The name and post office address of all other interested parties

3. A detailed statement of the facts upon which the GCIC action is contested

4. A statement describing the relief sought

5. The name and post office address of counsel, if the party filing the request is represented by counsel.

(b) Limitations on right to a hearing. A hearing to contest the imposition of a disciplinary measure will be granted as a matter of right only if it is filed within 30 days of the imposition of the action. A hearing upon a refusal to exchange information or provide services upon a request for reinstatement of suspended services shall be granted as a matter of right at any time while service is partially or wholly suspended. A petition for such a hearing may be denied only when the petition presents no substantial grounds that have not been previously presented. The Council may, at its discretion, allow extensions of time and amendment of requests for good cause.

(c) Responses to requests for hearing. The GCIC Council will respond to all requests for hearings with scheduling notices or orders denying requests and reasons for denials.

(d) Motions. Any application to the Director or the GCIC Council to enter any order or to take any action, after filing a request for hearing, shall be made by motion that, unless made during the hearing, shall be in writing stating the specific grounds therefore and set forth the action or order sought. No motion shall be ruled upon except when the case-in-chief is ruled upon, unless the moving party specifically requests a ruling at some other time and the Council deems such ruling appropriate.

(e) Hearings. Three members of the GCIC Council appointed by the Chairman or his designee shall conduct hearings in contested cases. Following each hearing, Council members shall notify the Director and each interested party of their findings. Each party shall have 20 days following the notification to file written exceptions and briefs. At the next scheduled meeting of the GCIC Council, the Director and all concerned parties shall have an opportunity to present oral arguments. The Council shall then render a final decision.

(6) Notwithstanding anything previously stated, if it appears that the provisions of O.C.G.A. § 35-3-38 have been violated, the Director or the GCIC Council may refer the matter to the appropriate prosecuting authority.

Authority: O.C.G.A. §§ 35-3-32, 35-3-33; 42 U.S.C. 3771, 28 CFR 20.21. **History.** Original Rule entitled "Approval and Disciplinary Procedures" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed July 2, 1986, effective July 22, 1986. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Repealed:** New Rule, same title, adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002; effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-1-.06 Contested Cases Governed by Express Statutory Provisions. Amended.

Contested cases, which arise under O.C.G.A. § 35-3-37 concerning an individual's right to access and correct his criminal record are governed

and processed by provisions contained therein, rather than the Administrative Procedure Act.

Authority: O.C.G.A. § 35-3-37. **History.** Original Rule entitled "Contested Cases Governed by Express Statutory Provisions" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed July 2, 1986, effective July 22, 1986. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Repealed:** New Rule, same title, adopted. Filed Mar. 4, 1998; effective Mar. 24, 1998. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

Rules
Of The
Georgia Crime Information Center Council

Chapter 140-2

Practice and Procedure

Table of Contents

140-2-.01 Scope. Amended.

(1) These Rules apply to Georgia criminal justice agencies and all other agencies or persons with access to criminal justice information as defined in Georgia law and Rule 140-1-.02 (c).

(2) These Rules do not restrict any criminal justice agency from publicly disclosing certain information to include:

(a) The status of a current investigation

(b) The recent arrest, release or prosecution of an individual.

(3) A criminal justice agency may release prior CHRI to the news media or any other person if the CHRI is based on data contained in:

(a) Posters, announcements, flyers or computerized databases created to aid in the identification or arrest of fugitives, wanted persons, habitual offenders, career criminals or highly dangerous offenders

(b) Incident reports, arrest/booking reports and other reports prepared by criminal justice agencies and defined by law as public records

(c) Official records of public judicial proceedings.

(4) The names of living victims of sexual offenses and juveniles involved in police investigations are not to be released.

(5) Nothing in these Rules shall close any record that is now or hereafter made public by law.

(6) Nothing in these Rules shall mandate the exchange of criminal justice information except where specifically required by these Rules.

Authority: O.C.G.A §§ 16-6-23, 35-3-34, 35-3-35, 50-18-72; 42 U.S.C. 3371, 28 CFR 20.21. **History.** Original Rule entitled "Scope" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983; as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule

repealed and a new Rule of same title adopted. Filed July 2, 1986, effective July 22, 1986. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 7, 1988, effective July 27, 1988. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Amended:** Filed Dec. 2, 1992, effective Dec. 22, 1992. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.02 Security Policy for Criminal Justice Information. Amended.

(1) Handling procedures

(a) Secret data (as defined in Rule 140-1-.02 (2) (c) 3):

1. When not in use it shall be stored in locking, fire-resistant vaults or safes. Computer programs and data files should be backed-up on electronic media and secured in a location separate from the building in which the computer system is located.

2. Areas where the information is processed and handled shall be restricted to authorized personnel in the performance of official duties.

3. The information shall be under the absolute control of criminal justice agencies with access regulated by agency heads or their designees.

4. A log or other record shall be maintained when information is removed from, or returned to the physically secured storage defined above in paragraph (1) (a) 1.

(b) CHRI, as defined in Rule 140-1-.02 (2) (c) 1, shall be:

1. Stored in a secure location when not under the control of authorized criminal justice agency employees.

2. Processed in areas restricted to authorized personnel in the performance of official duties.

3. Under the absolute control of criminal justice agencies except as exempted by these Rules.

(c) Restricted and Sensitive data, as defined in Rule 140-1-.02 (2) (c) 2 and 4, shall be used and stored in a controlled access area.

(2) Secret information, CHRI or restricted information is a "Secret of State", which is required by State policy, the interest of the community and the right of privacy of the citizens of this State to be confidential. Such information shall not be divulged except as permitted by Georgia law and these Rules. Criminal justice agencies must destroy documents containing secret information, CHRI or restricted information no longer required for operations in a manner precluding access to the information by unauthorized persons.

(3) Criminal justice agencies shall disseminate CHRI only to agencies or persons requiring such information to perform duties serving the administration of criminal justice or as otherwise provided by statute, executive order or these Rules. Under no circumstances will CHRI be transmitted via the CJIS network to devices not authorized to access such information, which may exist in the GCIC computerized files, FBI Interstate Identification Index (III) or computerized files maintained in other states.

(4) Local agency heads shall provide the GCIC Director with written notification of security policy violations for criminal justice information committed by employees of their agencies or agencies over which they exercise management control.

(5) The Director shall establish an information security structure that provides for an ISO. The Director shall also ensure that each local agency having access to the CJIS network designates a LASO.

Authority: O.C.G.A. §§ 35-3-30, 35-3-32; 28 C.F.R. 20.21, FBI CJIS Security Policy as amended. **History.** Original Rule entitled "Data Security Requirements for Criminal Justice Information" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of the same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule entitled "Security Policy for Criminal Justice Information" adopted. Filed July 2, 1986, effective July 22, 1986. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective. Nov. 27, 1990.

Repealed: New Rule, same title, adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.03 Completeness and Accuracy of Criminal Justice Information. Amended.

(1) Each law enforcement agency is responsible for obtaining fingerprints of persons charged with criminal offenses described in O.C.G.A. § 35-3-33. Additionally, O.C.G.A. § 15-11-83 requires agencies charging juveniles (16 years of age and younger) with felony offenses to submit criminal cards to GCIC in the same manner prescribed for adult offenders. Fingerprint images may be transmitted electronically to GCIC utilizing GCIC certified livescan/cardscan devices, or submitted manually (rolled, inked prints) on FBI provided fingerprint cards preprinted with the arresting agency's Originating Agency Identifier (ORI). Only black printer's ink or an alternative medium authorized by the FBI is acceptable for fingerprint images submitted manually to GCIC; additionally, two original arrest fingerprint cards are required for manual submissions. Agencies should seek GCIC approval before using other criminal fingerprint cards**,** or buying/using any alternative medium or system.

(a) All required fields on arrest fingerprint cards or electronic transmissions must be complete and legible. When applicable, agencies should indicate 'Treat as Adult' status (persons 13 to 16 years of age) by checking the appropriate block on the reverse side of fingerprint cards, or keying the appropriate code in designated field(s).

(b) Only law enforcement personnel may obtain fingerprints and complete the data fields necessary to submit an arrest record to GCIC. At no time should arrested persons or inmates of jails or correctional institutions assist in obtaining fingerprints or completing data fields.

(c) Agencies must forward individual arrest data and fingerprint images to GCIC within 24 hours of arrest; however, this time may be extended to cover any intervening holiday or weekend.

(2) Each law enforcement agency arresting persons under paragraph (1) above is also responsible for forwarding the Offender Tracking Number (OTN) and Charge Tracking Number (CTN), and other associated information, along with arrest warrants, citations or charges to appropriate prosecutors or courts. Prosecutors and courts use the OTN and CTN to report the final disposition of charges to GCIC. Agencies may electronically transmit disposition information to GCIC via systems and programs meeting GCIC requirements. Final disposition reporting is required for complete and accurate adult and juvenile criminal history records.

(a) When a district attorney or solicitor makes a final disposition decision, it is the duty of this official to forward the disposition information to GCIC.

(b) When a final disposition or modification of earlier disposition decision occurs in a court of competent jurisdiction, it is the court's duty to forward the disposition information to GCIC.

(c) When the State Board of Pardons and Paroles modifies a sentence, revokes parole or discharges a parolee, it is the Board's duty to forward the disposition information of sentence modification to GCIC.

(d) When a probation sentence is successfully completed (under provisions of Georgia's First Offender Act) , revoked, or there is a disposition arising from a revocation hearing, it is the duty of probation offices under the direct supervision of the Department of Corrections to forward disposition information to GCIC.

(e) When the Georgia Court of Appeals or Supreme Court of Georgia issues a decision or order to modify or suspend a trial court's decision regarding an individual defendant, it is the duty of the clerk of the Court of Appeals or the Supreme Court of Georgia and the clerk of the trial court to forward the disposition information of such modification or suspension to GCIC.

(f) Juvenile courts must submit final dispositions on juvenile offenses reported under O.C.G.A. § 15-11-83. Final dispositions are required for a complete and accurate juvenile criminal history database.

1. Criminal justice agencies must report final dispositions of juvenile cases.

2. The specific name and ORI of the judicial agency handling the juvenile case must be in the disposition information. Superior Court Clerks will forward juvenile disposition information to GCIC for counties without a juvenile court and should indicate “Juvenile” in the final disposition information to ensure use of the appropriate juvenile codes when processing the record. Juvenile courts that do not have an ORI may make application for an ORI through GCIC.

3. Juvenile records are available to criminal justice agencies only for the administration of criminal justice using purpose code C.

4. Juvenile records are not automatically purged from the criminal history database. A court order to seal, expunge, or destroy a juvenile record is required and must contain sufficient identifying information (juvenile’s name, sex, race, date of birth, date of arrest, OTN and CTN) to carry out actions required. Further guidance may be found in O.C.G.A. §§ 15-11-79, 15-11-79.2, 15-11-81 and 15-11-82.

(3) Responsible agencies must forward final disposition information to GCIC within 30 days of the final disposition decision.

(4) GCIC will publish a list of fingerprintable offenses as prescribed by Georgia law and the Attorney General of Georgia and revise the list when necessary as determined by the Attorney General.

Authority: O.C.G.A. **§§** 15-11-79.2, 15-11-81, 15-11-82, 15-11-83, 35-3-33, 35-3-36; 42 U.S.C. 3773, 28 C.F.R. 20.21. **History.** Original Rule entitled "Completeness and Accuracy of Criminal History Record Information" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 2, 1986, effective July 22, 1986. **Amended:** Filed Jan. 6, 1988, effective Jan. 27, 1988, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 7, 1988, effective July 27, 1988. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective November 27, 1990. **Repealed:** New Rule entitled "Completeness and Accuracy of Criminal Justice

Information" adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.04 Criminal Justice Information Exchange and Dissemination. Amended.

(1) Exchange and dissemination of criminal justice information by criminal justice agencies:

(a) Criminal justice agencies shall exchange criminal justice information with other criminal justice agencies and authorized private contractors to facilitate the administration of criminal justice and criminal justice employment. Dissemination of criminal justice information to such agencies will follow the provisions of user agreements executed between GCIC and criminal justice agency heads. If there is a question as to whether an agency is a criminal justice agency as defined by these Rules, the Director will determine the agency's status.

1. Local criminal justice agencies must refer private attorneys requesting CHRI in criminal cases to GCIC.

2. Local criminal justice agencies may process CHRI requests from a Public Defender's Office when that Office has a State assigned ORI (ends in S). When processing these CHRI requests, the local agency must use the Public Defender's ORI and purpose code L. Consent of the individual (criminal defendant or witness) is not required.

3. Local criminal justice agencies may process private attorney requests for CHRI in civil cases when provided the signed consent of the persons whose records are sought utilizing the appropriate purpose code.

4. Criminal records containing information on arrest charges disposed of under provisions of the Georgia First Offender Act may be disseminated by Georgia criminal justice agencies as described in subparagraph (2) (a) 3 of this Rule.

(b) Criminal justice agencies may disseminate CHRI to private persons, businesses, public agencies, political subdivisions, authorities and other

entities, including state or federal licensing and regulatory agencies or their designated representatives. In these cases, CHRI shall contain only Georgia or local criminal justice agency information, excluding information relating to any arrest disposed of under provisions of the Georgia First Offender Act after the person's successful discharge from First Offender status. The exchange of CHRI obtained from NCIC, or the III for a non-criminal justice purpose is prohibited except when permitted by federal law.

1. Requesters must provide the fingerprints or signed consent of persons whose criminal history records they are seeking at the time of each request. The signed consent must be in a format approved by GCIC and include the person's full name, address, social security number, race, sex and date of birth. When the requester represents a county Board of Voter Registrars or a county Board of Voter Registration and Elections, neither the fingerprints nor signed consent of persons whose records are sought shall be required, if the sole purpose is to verify information provided on a voter registration card by a voter registration applicant. In addition, criminal justice agencies may disseminate Georgia felony conviction records to any requester, without the person's consent, as provided for by Georgia law.

2. Criminal justice agencies may charge fees for disseminating criminal history records or "no record" reports to private individuals, public and private agencies or their designated representatives. Fees should approximate as nearly as possible the direct and indirect costs associated with providing such information services.

3. Criminal justice agencies that disseminate CHRI to private individuals and public and private agencies shall advise all requesters that if an adverse employment, licensing, housing or other decision is made, the individual or agency making the adverse decision must inform the applicant of all information pertinent to that decision. This disclosure must include that a CHRI check was made, the specific contents of the record and the effect it had on the decision. Failure to provide all such information to the applicant is a misdemeanor under Georgia law.

(c) Federal law exempts the FBI, State Department, Defense Investigative Service, Central Intelligence Agency and Office of

Personnel Management from these provisions of Georgia law. Authorized representatives of these agencies are not required to provide the fingerprints or signed consent of persons whose CHRI is sought. All criminal justice agencies are required by federal law to provide these agencies with CHRI, as described in subparagraph (1) (b) of this Rule, on security clearance applicants and applicants for employment in sensitive national security jobs. However, the Office of Personnel Management (OPM) contracts with companies that perform its background investigations. OPM contractors with Georgia offices have NCIC assigned ORIs, which end in R (GAOPM010R) and access Georgia's CJIS network to run background investigations under purpose code S (Security Clearance Information Act).

(d) Pursuant to signed GCIC user agreements and management control agreements, criminal justice agencies may provide criminal justice information and CHRI to individuals and agencies to provide for the development and operation of computerized information systems or for the operation of consolidated governmental communications centers supporting the administration of criminal justice. These individuals and agencies shall be under the management control of the criminal justice agencies they support. These agreements shall authorize specific access to information, limit the use of information to purposes for which it was disseminated, require the review and signing of Awareness Statements and ensure the security and confidentiality of information consistent with the Rules of the GCIC Council.

(e) Criminal justice agencies may disseminate criminal justice information and CHRI to individuals and agencies for the express purpose of research when the Director has approved the research project in advance. In each case, GCIC shall execute a special user agreement with requesters prior to the dissemination of such information. The agreement shall provide for non-identification of specific individuals in published research reports and that information furnished by criminal justice agencies shall be immune from legal process and shall not, without consent of the criminal justice agency providing the information, be admitted as evidence for any purpose in any action, suit or other judicial or administrative proceedings.

(f) Criminal justice agencies must advise recipients of CHRI that use of this information shall be limited to the intended purpose and may not be secondarily disseminated.

(g) Criminal justice agencies have authority to access the FBI's III files for criminal justice administration and criminal justice employment. In addition, this information may be used in civil or criminal courts in domestic violence or stalking cases and other purposes authorized by federal law. Criminal justice agencies shall not access III files for information pursuant to state license/permit applications or for non-criminal justice employment purposes, unless specifically provided for by federal law or regulation.

(h) The FBI CJIS Security Policy documents the minimum level of Information Technology (IT) security requirements determined acceptable for the transmission, processing and storage of the nation's CJIS data. It further stipulates that III CHRI may be accessed only for an authorized purpose. Dissemination to another agency is permissible if the other agency is an authorized recipient of such information. This policy also identifies the requirements for methods of disseminating III CHRI data.

1. Transmitting III CHRI via the internet and associated electronic media such as email facilities, remote access file transfers and any other file modifications is allowed, provided all technical security requirements have been met.

2. Transmitting III CHRI via electronic devices using wireless or radio technology is allowed when an officer determines there is an immediate need for this information to further an investigation or there is a situation affecting the safety of an officer or the public.

3. Transmitting III CHRI via a facsimile device not connected to a CJIS system is allowed when both agencies involved in the transmission have an authorized NCIC ORI number. Prior to the transmission, the sending agency shall verify the receiving agency's authenticity.

4. Georgia CHRI may be disseminated via the internet, wireless or radio technology, or facsimile to authorized agencies as described in the FBI CJIS Security Policy.

5. Additionally, a criminal justice agency may only disseminate Georgia CHRI via facsimile to a non-criminal justice or entity provided the receiving facsimile is located in an area not readily accessible by persons other than the individual authorized to receive the CHRI.

(i) Private contractors are permitted access to GCIC and FBI CJIS systems pursuant to a specific agreement/contract to provide services for the administration of criminal justice. The agreement/contract between the government agency and the private contractor must incorporate the Security Addendum approved by the Director of the FBI (acting for the U.S. Attorney General), as referenced in Title 28 CFR 20.33 (a) (7). Private entities performing the administration of criminal justice must meet the same training and certification criteria required by governmental agencies performing a similar function. All private entities performing criminal justice functions, including administration of private correctional facilities, police crime labs and the administration of probation services are included.

(j) No criminal justice information shall be disseminated except as provided by law and these Rules.

(2) Exchange and dissemination of criminal justice information by GCIC.

(a) GCIC shall exchange criminal justice information with criminal justice agencies and those non-criminal justice agencies under a specific contract to a criminal justice agency to serve the administration of criminal justice and to facilitate criminal justice employment, based on the following criteria:

1. GCIC shall execute appropriate user agreements with all criminal justice agencies

2. GCIC shall provide any information in its files or in files available to GCIC, which may aid these agencies in the performance of their duties

3. Use of information relating to any arrest disposed of under provisions of the Georgia First Offender Act is unauthorized for licensing or employment purposes after successful discharge of an individual from First Offender status, except as specifically authorized by Georgia law and these Rules

4. When requested electronically, GCIC may electronically disseminate CHRI of in-state felony convictions, pleas and sentences provided there is sufficient identifying information.

(b) GCIC shall exchange criminal justice information with:

1. The Governor, when acting as Chief Law Enforcement Officer of the State

2. The Attorney General, when performing activities relating to the apprehension or prosecution of criminal offenders

3. The Supreme Court, when the Court's administrative arm is evaluating candidates for the Georgia bar.

(c) GCIC shall exchange CHRI with public agencies and officials, private businesses and individuals.

1. Public agencies, private individuals and businesses requesting fingerprint-based criminal history record checks shall submit applicant fingerprints using GCIC approved means and pay the prescribed fees for each criminal history record or "No Record" report disseminated by GCIC.

2. If CHRI provided by GCIC is for employment, licensing or other decisions, GCIC shall provide guidance to requesters as contained in subparagraph (1) (b) (3) of this Rule.

3. Public agencies and officials requesting criminal history record checks shall be subject to periodic audits by GCIC to assure compliance with the relevant provisions of Georgia law and these Rules.

4. Georgia law authorizes GCIC to conduct certain criminal history record checks for criminal defense purposes based on personal identifiers supplied by authorized requesters. All such record checks are conducted in a manner determined by the Director. Criminal history records provided by GCIC pursuant to this subparagraph shall contain the entire Georgia criminal history record to include completed first offender records. Authorized requesters shall pay prescribed fees.
(d) GCIC will perform criminal history record checks for non-criminal justice purposes only after fulfilling its duties and obligations to criminal justice agencies as required by law.

(e) GCIC may allow access to the CJIS network and other computerized files containing criminal justice information and/or CHRI, pursuant to special user agreements and management control agreements with governmental computerized information systems and governmental dispatch centers in support of criminal justice agencies. These governmental agencies shall be under the management control of the criminal justice agencies they support. User agreements and management control agreements shall authorize access to information, limit the use of information to purposes for which it was disseminated, require the signing of Awareness Statements and ensure the security and confidentiality of data consistent with these Rules.

(f) The commercial dissemination of state or federal hot file records obtained from NCIC is prohibited. Information derived for other than criminal justice purposes from national hot file records can be used by authorized criminal justice personnel only to confirm the status of a person or article, e.g. wanted or stolen. Any advertising of services providing "data for dollars" is prohibited. Authorized agencies are allowed to charge a processing fee for disseminating data for authorized purposes. The wholesale marketing of data for profit is not permitted, as in the example of a pre-employment screening or background check company requesting that wanted person checks from NCIC be conducted on individuals for various non-criminal justice employments.

(g) Use of information disseminated by GCIC shall be limited to the purposes for which it was disseminated. Recipients shall be so advised.

(h) No information shall be disseminated by GCIC except as provided by Georgia law or these Rules.

Authority: O.C.G.A. §§ 3-3-2, 7-1-682(c), 7-1-702(c), 7-1-1004(e), 10-9-9, 15-16-1, 16-11-129, 17-6-50, 19-8-16(d), 20-1A-34, 20-2-211, 25-4-8, 31-7-254, 35-3-33, 35-3-34, 35-3-34.2, 35-3-35, 35-3-35 (a)(1), 35-8-8, 38-3-27, 40-5-2, 40-5-82, 42-8-60, 42-8-62, 42-8-63, 42-8-63.1, 42-8-65, 43-12A-4, 43-38-6, 43-38-7, 43-38-7.1, 43-39A-22.1, 43-40-27.1, 43-47-6, 49-2-14, 49-5-64, 49-5-69.1; 42 U.S.C. 3771; 5 U.S.C. 9101; 28 C.F.R. 20.21; Pub. L. 92-544; FBI Security Policy, as amended. History. Original Rule entitled "Criminal Justice Information Exchange and Dissemination" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Filed June 11, 1976, effective July 1, 1976. **Amended:** Filed July 29, 1976, effective Aug. 18, 1976. **Amended:** Filed Aug. 25, 1976, effective Sept. 14, 1976. **Amended:** Filed June 10, 1977, effective June 30, 1977. **Amended:** Filed May 26, 1978, effective July 1, 1978, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Sept. 6 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 2, 1986, effective July 22, 1986. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Jan. 6, 1988, effective Jan. 27, 1988, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 7, 1988, effective July 27, 1988. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Amended:** Filed Dec. 4, 1991, effective Dec. 24, 1991. **Amended:** Filed Mar. 4, 1992, effective Mar. 24, 1992. **Amended:** Filed Dec. 2, 1992, effective Dec. 22, 1992. **Amended:** Filed Oct. 13, 1999, effective Nov. 2, 1999. **Amended:** Filed Oct. 12, 2000, effective Nov. 1, 2000. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.05 Integrity of Criminal Justice Information. Amended.

Documents containing criminal justice information, regardless of its source, shall not be altered, obtained, copied, destroyed, delayed, misplaced, misfiled, given, bought or sold when the intent of such action is to obstruct justice or facilitate the violation of any law or these Rules.

Authority: O.C.G.A. §§ 35-3-35, 35-3-38; 42 U.S.C. 3771, 28 C.F.R. 20.21. **History.** Original Rule entitled "Security and Privacy of Criminal Justice Information" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Jan. 7, 1983, effective Feb.

1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 2, 1986, effective July 22, 1986. **Repealed:** New Rule entitled "Integrity of Criminal Justice Information" adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Repealed:** New Rule, same title, adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998.

140.2-.06 Criminal History Dissemination Logs. Amended.

(1) GCIC will maintain computer system logs of all criminal history record inquiries and record requests transmitted to GCIC.

(2) The following minimum information shall be maintained in GCIC computer system logs.

(a) Date, time and purpose of each inquiry or request

(b) Identification of each requester

(c) Identification of the terminal operator or practitioner

(d) Identification of each person inquired

(e) Each record subject's GCIC assigned state identification (SID) and/or FBI number(s)

(f) Agency reference numbers (ARN) are required for all criminal justice (purpose code C), firearm permits or purchases (purpose code F), defense attorney (purpose code L), POST certification (purpose code Z) and DHR exigent circumstances (purpose code X) record checks. ARNs shall be unique, significant numbers and limited to incident report numbers, other criminal case numbers, docket numbers, inmate numbers or any other numbers that link criminal history record requests to criminal investigations or specific files.

(3) Criminal justice agencies that access Georgia's CJIS network may establish local paper or computer system logs to control and document requests for criminal history records, CJIS inquiries and/or secondary disseminations within their agencies. These agencies may request

printouts of GCIC system logs when required for internal investigations or other special circumstances. Agencies establishing computer system logs may record information items listed above; detailed criminal history record information shall not be recorded in computer system logs.

Authority: O.C.G.A. §§ 35-3-33, 35-3-35; 42 U.S.C. 3771, 28 C.F.R. 20.21. **History.** Original Rule entitled "Criminal History Logs" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 2, 1986, effective July 22, 1986. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 7, 1988, effective July 27, 1988. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Amended:** Filed Dec. 2, 1992, effective Dec. 22, 1992. **Repealed:** New Rule of same title adopted. Filed Apr. 16, 1993, effective May 6, 1993. **Repealed:** New Rule entitled "Criminal History Dissemination Logs" adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.07 Audit Procedures. Amended.

(1) The Director shall appoint auditors to conduct performance audits of criminal justice agencies that access Georgia's CJIS network to assess and enforce compliance with these Rules, O.C.G.A. §§ 35-3-34 through 35-3-38, other relevant Georgia code sections and pertinent federal statutes and regulations.

(a) The GCIC audit program shall be designed and conducted to meet the performance audit standards and practices set out in the General Accounting Office (GAO) publication Government Auditing Standards also adhered to by the FBI CJIS Division audit staff.

(b) GCIC auditors shall audit these agencies triennially as required by NCIC operating policy. A representative sample of agencies that do not access Georgia's CJIS network will be audited, based on the availability of auditor resources.

(c) Agency heads shall receive at least 15 days advance notice of on-site GCIC audits. Written notification will identify all areas of audit program interest and the applicable performance standards.

(d) Upon completion of each performance audit, GCIC auditors shall discuss their findings with agency heads, TACs, or their designees. GCIC auditors will recommend strategies for remedial action to resolve any area of non-compliance. In addition, GCIC auditors will assist agency heads in obtaining agency personnel training or any other assistance related to efforts to resolve areas of non-compliance.

(e) GCIC auditors will provide agency heads with written reports, which identify areas of compliance, non-compliance and other written comments specific to audit assessments. The Audit Program Manager will report the results of completed audits to the Assistant Deputy Director for Compliance and Customer Support and the Director.

(f) The Director shall report the status of the Georgia audit program to the Chairman and members of the GCIC Council. In cases of continued non-compliance, the Director shall provide recommendations to the Council for sanctions or other actions per the provisions of GCIC Council Rule 140-2-.20 (Sanctions).

(2) Agencies scheduled for audit shall make the following available to GCIC auditors:

(a) Facility access policy

(b) Personnel records (maintained in agency files) to include results of employee fingerprint-based background checks, GCIC Awareness Statements, records of relevant training, e.g. CJIS Network Terminal Operator workbooks, end of chapter tests and final certification tests, as well as any other training materials used for practitioners and any other documents deemed appropriate to accomplish the audit responsibilities

(c) Local criminal history record files

(d) CHRI handling procedures

(e) Standard operating procedures governing the access, use, security and discipline regarding the dissemination of criminal justice information

(f) Case files that support GCIC/NCIC computerized record entries, e.g. incident and supplemental reports, missing persons reports, family violence reports, arrest warrants

(g) Computer system hardware, when requested

(h) Computer system software, when requested

(i) Computer system documentation to include system topologies, when requested.

Authority: O.C.G.A. §§ 35-3-31, 35-3-32, 35-3-34, 35-3-38; 42 U.S.C. 3771, 28 C.F.R. 20.21. **History.** Original Rule entitled "Audit Procedures" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 2, 1986, effective July 22, 1986. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Repealed:** New Rule of same title adopted. Filed Dec. 2, 1992, effective Dec. 22, 1992. **Amended:** Filed Apr. 16, 1993, effective May 6, 1993. **Repealed:** New Rule, same title, adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.08 Physical Security Standards. Amended.

(1) Criminal justice agencies, governmental dispatch centers and other governmental agencies approved by the Director for direct CJIS network access shall provide secure areas out of public view in which criminal justice information is handled.

(2) Such agencies shall place CJIS network devices in secure areas with adequate physical security to protect at all times against any unauthorized viewing or access to computer terminals, access devices or stored/printed data. This includes locations or vehicles housing Mobile

Data Terminals (MDTs) or personal/laptop computers capable of accessing criminal justice information.

(3) Such agencies shall institute reasonable procedures to protect any central depository of CHRI from unauthorized access, theft, sabotage or damage resulting from fire, wind, flood, power failure or other natural or manmade disaster~~s~~.

(4) Such agencies operating computer systems connected to the Georgia CJIS network should provide adequate backup and recovery plans to protect these systems and ensure system recovery within minimal time. Recovery should focus on hardware and software.

(5) Authorized personnel must accompany visitors to CJIS computer centers and/or terminal areas at all times. Access to terminal areas should be restricted to the minimum number of authorized employees required for operations.

Authority: O.C.G.A. §§ 35-3-32, 35-3-33; 28 C.F.R. 20.21, FBI Security Policy as amended. **History.** Original Rule entitled "Physical Security Standards for Criminal Justice Agencies" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule entitled "Physical Security Standards" adopted. Filed July 2, 1986, effective July 22, 1986. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Amended:** Filed Dec. 4, 1991, effective Dec. 24, 1991. **Amended:** Filed Dec. 2, 1992, effective Dec. 22, 1992. **Repealed:** New Rule, same title, adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.09 Personnel Security Standards. Amended.

(1) Criminal justice agency employees, and other personnel as identified by the GCIC Director, who handle criminal justice information shall consent to investigations of their moral character, reputation and honesty. All applicants, including appropriate information technology (IT) personnel having access to CJIS systems information, shall submit to a state and national fingerprint-based identification check to be conducted

within 30 days of employment, assignment or subsequent re-employment. Investigations should produce information sufficient to determine applicants' suitability and fitness for employment.

(2) Criminal justice agencies, governmental dispatch centers and other governmental agencies handling criminal justice information shall disqualify applicants convicted by any state or the federal government of any felony, or have convictions of sufficient misdemeanors to establish a pattern of disregard for the law. If the applicant appears to be a fugitive or have an arrest history without conviction for a felony or serious misdemeanor, the Director or criminal justice agency head, or his/her designee, will review the matter and decide if access/employment is appropriate.

(3) Giving false information shall disqualify applicants and be cause for employee dismissal.

(4) Agencies identified in subparagraph (2) of this Rule shall establish security constraints for all personnel who work in secure areas where criminal justice information is stored, collected or disseminated. Terminal operators and practitioners shall access the CJIS network only for purposes within their authority. Each criminal justice agency authorized to access CJIS network information must have a written disciplinary policy for violators of GCIC Council Rules and GCIC/FBI CJIS Security Policy as amended.

(5) Within their political subdivisions, criminal justice agencies must monitor the selection, utilization and retention of non-criminal justice personnel who are authorized direct access to criminal justice information in support of criminal justice operations.

(6) All personnel whose jobs require them to access or process criminal justice information shall sign an Awareness Statement for permanent filing in the employees' personnel file. Should the content of the Awareness Statement change by act of law, action by the Director or other official act, agency heads shall direct their employees to sign amended Awareness Statement forms when provided by GCIC.

Authority: O.C.G.A. §§ 16-9-90 et seq., 35-3-32, 35-3-33; 28 C.F.R. 20.21**;** FBI Security Policy, as amended. **History.** Original Rule entitled "Personnel

Security Standards for Criminal Justice Agencies" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule entitled "Personnel Security Standards" adopted. Filed July 2, 1986, effective July 22, 1986. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Amended:** Filed Dec. 2, 1992, effective Dec. 22, 1992. **Repealed:** New Rule, same title, adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.10 Procedures for Criminal History Record Inspection by Record Subjects. Amended.

(1) GCIC processing procedures:

(a) All applications for criminal history record inspection must include a current set of the record subject's fingerprints taken by a GCIC employee or trained employee of a local criminal justice agency. GCIC personnel will request identification documentation at time of fingerprinting

(b) Applications are processed upon payment of a $3.00 fee payable in cash or money order

1. GCIC will issue receipts for cash payments

2. Money orders shall be made payable to the Georgia Bureau of Investigation

(c) GCIC will accept applications from 8:00 a.m. to 4:30 p.m., Monday through Friday, except for State holidays. Appointments are preferred.

(2) An attorney may, upon written application and payment of fees, inspect and obtain a copy of his or her client's criminal history record maintained by GCIC.

(3) General processing procedures:

(a) Pursuant to these Rules, a local criminal justice agency may prescribe its own applicable forms and procedures for a record subject, or his or her attorney**,** to review and obtain a copy of the record subject's criminal history record

(b) Local agencies may charge reasonable fees to offset costs of handling inspection requests

(c) Agencies providing record inspection services shall impose only such procedures and restrictions reasonably necessary to

1. Ensure the integrity of its records

2. Verify the identity of those who seek to inspect their records; verification procedures may include fingerprinting

3. Establish orderly and efficient inspection procedures.

(4) Criminal history records determined by GCIC or other criminal justice agencies to be in error shall be corrected without undue delay; the record subject or attorney of representation shall be notified when record corrections have been made.

(5) For criminal history records determined by GCIC or other criminal justice agencies as accurate, the individual may initiate further actions under the provisions of Georgia law.

Authority: O.C.G.A. §§ 35-3-33 35-3-37; 42 U.S.C. 3771, 28 C.F.R. 20.21. **History.** Original Rule entitled "Procedures Whereby An Individual May Access His Criminal History Record File" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule entitled "Procedures for an Individual to Inspect His Criminal History Record File" adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 2, 1986, effective July 27, 1988. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Amended:** Filed Dec. 2, 1992, effective Dec. 22, 1992. **Repealed:** New Rule, same title, adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.11 Security Requirements for Criminal Justice Information in a Data Processing Environment. Amended.

(1) Computers used to collect, store or disseminate CHRI shall be protected from unauthorized access by means of software or hardware control systems, which log all access attempts. Each individual authorized to store, process and/or transmit CJIS information will use a unique identifier. The unique identification is also required for personnel who administer and maintain the system. The unique identification can take the form of a full name, badge number, serial number or other unique alphanumeric identifier. The identifier shall be authenticated.

(2) CHRI transmitted from one point to another by computer shall be protected from unauthorized access by means of software or hardware control systems. Standards for control systems outlined here must meet FBI CJIS Security Policy requirements.

(a) Procedures to prevent unauthorized copying or retaining of messages containing CHRI must be in place.

(b) Computers may log any message traffic and record such data elements as date, time, message number, origin and destination.

(c) CJIS information passing through a public network segment shall be protected with encryption.

(d) CJIS information transmitted over dial-up or internet connections shall be protected with encryption.

(e) The Director may grant authorization for internet access to support CJIS processing when a minimum set of technical and administrative requirements, which assure the security of the CJIS system from unauthorized access via the internet are in place.

(f) CJIS information passing over wireless links shall be protected with encryption. Transmitting hot file data over wireless links is allowed with either encryption or a proprietary data transmission protocol that prevents recognizable clear text transmissions. All wireless links or

server access points shall be protected by authentication to ensure protection from unauthorized system access.

(g) Networks having terminals or devices that access CJIS and/or the internet must be protected by firewalls meeting the GCIC/FBI CJIS Security Policy standard as amended.

(3) Computers storing or disseminating CHRI may perform logging activities pursuant to Rule 140-2-.06.

(4) Computers and the agencies operating or administratively responsible for the operation of computers utilized in whole or part for the collection, storage, dissemination or message switching of CHRI shall be subject to GCIC audits pursuant to Rule 140-2-.07.

(5) Physical security standards for these computers shall be maintained pursuant to Rule 140-2-.08.

(6) Personnel security standards for persons employed to operate, program or maintain these computers shall be established pursuant to Rule 140-2-.09 as follows:

(a) A criminal justice agency responsible for collecting, storing, disseminating or transmitting CHRI by computers not under its direct administrative control shall not employ any person convicted by any state or the federal government of any felony or sufficient misdemeanors to establish a pattern of disregard for the law

(b) A criminal justice agency responsible for collecting, storing, disseminating or transmitting CHRI by a computer center not under its direct administrative control has the right and responsibility to investigate computer center job applicants and employees and disqualify any person convicted by any state or the federal government of any felony or sufficient misdemeanors to establish a pattern of disregard for the law.

(7) Secret data or CHRI contained in a computer system, whether dedicated or shared, shall be kept under maximum-security conditions. Documents containing secret data or CHRI no longer required to support

criminal justice operations, must be destroyed in a secure manner that precludes unauthorized access to the information.

(8) The agency administratively responsible for the supervision of persons, computer hardware or software assumes liability for any misuse of secret data or CHRI stored in a shared computer environment.

Authority: O.C.G.A. §§ 35-3-32, 35-3-33, 35-3-34, 35-3-35, 35-3-38; 42 U.S.C. 3771, 28 C.F.R. 20.21, FBI Security Policy as amended. **History.** Original Rule entitled "Security Requirements for Criminal Justice Information in a Data Processing Environment" filed Feb. 25, 1976, effective Mar. 16, 1976. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 2, 1986, effective July 22, 1986. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Amended:** Filed Dec. 2, 1992, effective Dec. 22, 1992. **Amended:** Filed Apr. 16, 1993, effective May 6, 1993. **Repealed:** New Rule, same title, adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.12 Uniform Crime Reporting. Amended.

(1) Each law enforcement agency is required by Georgia law (O.C.G.A. § 35-3-36) to participate in the Uniform Crime Reporting (UCR) program. GCIC is similarly required (O.C.G.A. § 35-3-33) to manage Georgia's UCR program and participate in the FBI's national UCR program.

(2) Law enforcement agencies are required to submit UCR and Family Violence reports to GCIC in a manner prescribed by GCIC.

(3) GCIC will provide general crime and offender data derived from UCR reports to the Governor, the General Assembly, state and local criminal justice agencies and the public.

(4) Law enforcement agencies shall retain case file copies (or an equivalent) of incident and Family Violence reports in manual or automated format that supports active wanted/missing person and/or

stolen serial numbered property records entered in GCIC/NCIC computerized files until these records are cleared, canceled or purged.

(5) Local agency UCR program procedures, records and supporting documents are subject to GCIC and FBI audit.

Authority: O.C.G.A. §§ 17-4-20.1, 35-3-33, 35-3-36; U.S. DOJ/FBI UCR Handbook, 1984. **History.** Original Rule entitled "Uniform Crime Reporting" filed Jan. 7, 1983, effective Feb. 1, 1983, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 2, 1986, effective July 22, 1986. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 7, 1988, effective July 27, 1988. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Repealed:** New Rule, same title, adopted. Filed Dec. 4, 1991, effective Dec. 24, 1991. **Amended:** Filed Dec. 2, 1992, effective Dec. 22, 1992. **Repealed:** New Rule, same title, adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Repealed:** New Rule, same title, adopted. Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.13 Wanted/Missing Persons and Stolen/Abandoned Serial Numbered Property. Amended.

Responsible agencies shall enter (or cause entry of) information in GCIC and/or NCIC computerized files pertaining to wanted/missing persons, protected persons, sex offenders, unidentified deceased persons and serial-numbered property reported as stolen; entries shall be made when required data elements become available. O.C.G.A. § 35-3-36 requires agencies to enter records within 12 hours of determining that persons should be arrested or serial-numbered property was stolen. Provisions for entry of GCIC/NCIC computerized records regarding missing persons are contained in GCIC Council Rule 140-2-.15.

(a) Criminal justice agencies accessing Georgia's CJIS network shall use GCIC/NCIC codes, formats and operating procedures when making record entries. GCIC will provide procedural manuals and operations bulletins containing codes, procedures and guidance for record entry. GCIC will also provide updates and revisions as needed.

1. Heads of criminal justice agencies authorized to make GCIC/NCIC record entries or otherwise access databases maintained by Georgia, other states and the FBI are responsible for ensuring that current GCIC publications are maintained and used as authoritative CJIS network operational directives within their respective agency.

2. Heads of criminal justice agencies accessing Georgia's CJIS network are responsible for ensuring the proper training of employees authorized to enter, modify, locate, clear, cancel and validate GCIC/NCIC record entries identified by this Rule. The training program shall emphasize that a second employee must verify each record entry for completeness and accuracy. Training requirements are contained in GCIC Council Rule 140-2-.16.

(b) Criminal justice agencies accessing Georgia's CJIS network shall assist criminal justice and other authorized agencies by providing controlled and monitored network access.

(c) Each record entered in GCIC/NCIC computerized files shall contain the ORI of the agency responsible for the record entry.

1. Any criminal justice agency or governmental dispatch center connected to the CJIS network may act as "holder" of GCIC/NCIC record entries on behalf of another agency responsible for criminal cases or other actions involving GCIC/NCIC computerized files. An agency may use its own ORI in GCIC/NCIC record entries only when a signed Holder of Record Agreement exists between the entering agency and the non-terminal agency. The Holder of Record Agreement must outline each agency's legal responsibilities for records entered in GCIC/NCIC computerized files.

2. Record responsibilities include entry, update and confirmation of positive inquiry responses (known as "hits") made by other agencies when these agencies confront persons who may be wanted or missing, violators of protection orders, or come into contact with serial-numbered property which may be stolen.

(d) Record entries shall be made within 12 hours of a determination by the investigating criminal justice agency that a wanted person should be

arrested or serial-numbered property is stolen. Missing person record entries shall be made in accordance with Rule 140-2-.15 (2) (a). Record entries shall be made within the above period as soon as minimum information for records is obtained. Agencies responsible for record entries shall take necessary actions to obtain minimum data to meet the 12-hour entry requirement.

(e) All record entries must have supporting official documents that reflect initial and continuing efforts to apprehend wanted persons, validate registered sex offender information, protect victims of domestic violence, or recover identifiable, serial-numbered stolen property. Arrest warrants must be available to support GCIC/NCIC wanted person record entries.

1. CJIS network terminal agencies shall require non-terminal agencies to provide copies of such supporting documents prior to making GCIC/NCIC record entries on behalf of such agencies. If emergencies arise, where immediate or prompt record entry is critical to apprehending a wanted person or recovering serial-numbered property reported as stolen, supporting documents may be provided after record entries are made. CJIS network terminal agencies and non-terminal agencies should establish Service Agreements to ensure proper and timely handling of record entries and responsibilities.

2. If supporting documents are not provided within 48 hours of entry, record entries shall be removed from GCIC/NCIC computerized files. CJIS network terminal agencies shall notify non-terminal agencies upon removal of GCIC/NCIC record entries from GCIC/NCIC files.

3. CJIS network terminal agencies shall maintain supporting documents in their files until arrest warrants are served or recalled, stolen serial-numbered property is recovered, missing persons are located or record entries are otherwise removed from GCIC/NCIC computerized files.

(f) Any agency with records entered in GCIC/NCIC computerized files shall respond to hit confirmation request messages. Responses may include notification that a specific amount of time will be required for record verification or deemed as official verification.

1. Responses to priority messages must be made within ten minutes; responses to routine messages must be made within one hour. Obvious abuse of this process, such as a priority hit request (10 minutes) for wanted/missing persons who are in custody or stolen property that has been recovered, shall be subject to GCIC disciplinary procedures as determined by the Director.

2. Verification messages must include the status of record entries representing wanted/missing persons, protected persons, or stolen serial-numbered property.

(g) GCIC/NCIC record entries that are no longer valid must be removed immediately from GCIC/NCIC computerized files.

1. CJIS network terminal agencies are responsible for the timely removal of their records when no longer valid.

2. Non-terminal agencies are likewise responsible for the timely removal of their records when no longer valid by submitting **a** request for record removal to the CJIS network agency providing service.

(h) GCIC provides a computerized file for entry of abandoned motor vehicles recovered by law enforcement agencies and/or reported to them by wrecker service operators or vehicle storage facilities. Georgia law requires a law enforcement agency to make record entries**,** or have record entries made if the law enforcement agency does not have access to Georgia's CJIS network, in the designated GCIC computerized file. Georgia law also requires law enforcement agencies to furnish wrecker service operators, or vehicle storage facilities, with the name and address of the last known registered owner and title/lien holder information. Such information is available from the Georgia Department of Revenue via the CJIS network. The name and address of the last known owner of an abandoned vehicle registered in another state is available from that state's motor vehicle file through Nlets via a CJIS network inquiry. Georgia law further requires owners of abandoned motor vehicles, which later are determined as stolen, to receive recovery notification from law enforcement agencies after receiving reports that such vehicles were stolen. GCIC abandoned vehicle file records are automatically purged

90 days after entry if not removed sooner by entering agencies. NCIC does not maintain an abandoned vehicle file.

Authority: O.C.G.A. §§ 35-3-33, 35-3-36, 40-11-2. **History.** Original Rule entitled "Wanted/Missing Persons and Stolen Property" filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule entitled "Wanted/Missing Persons and Stolen Property" adopted. Filed July 2, 1986, effective July 22, 1986. **Amended:** Filed Jan. 6, 1988, effective Jan. 27, 1988, as specified by the Agency. **Amended:** Rule repealed and a new Rule entitled "Wanted/Missing Persons and Stolen/Abandoned Property" adopted. Filed July 7, 1988, effective July 27, 1988. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Amended:** Filed Dec. 2, 1992, effective Dec. 22, 1992. **Repealed:** New Rule entitled "Wanted/Missing Persons and Stolen/Abandoned Serial Numbered Property" adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.14 Validation Procedures for Wanted/Missing Person and Stolen Property Records. Amended.

All criminal justice agencies with wanted/missing persons, protected persons and/or stolen property record entries in GCIC and NCIC computerized files are required to participate in the record validation program established and administered by GCIC and NCIC.

(a) Record entries subject to validation are wanted/missing persons, protected persons, unidentified deceased persons, stolen vehicles, stolen guns, stolen boats, stolen securities, protection order records, records on violent gangs and terrorist organizations, persons on supervised released and abandoned vehicles.

(b) GCIC produces monthly listings of record entries for validation. Specifically, a CJIS network terminal agency will receive a validation package for its own records and records established for another agency under a Holder of Record Agreement. When a CJIS network terminal agency establishes GCIC/NCIC records for another criminal justice agency the agency of record, not the terminal agency, will receive validation packages.

(c) Agencies of record shall review validation listings by (1) comparing each record to supporting documentation such as the original arrest warrant (has it been served) and the court of jurisdiction; criminal case file (is information accurate, complete and valid); protection order; missing persons report, including available criminal history records; documented extradition limit changes, if any, from the District Attorney; wanted persons record; (2) checking with issuing authorities or prosecutors to determine if warrants remain valid or cases will be prosecuted; (3) determining from owners of stolen serial-numbered property if recovery has been made or ownership has changed; (4) verifying that missing persons have not returned; and, (5) contacting the Clerk of Superior Court to ensure Protection Orders are valid.

(d) Agencies shall cancel record entries that are no longer valid.

(e) Agencies shall modify record entries that contain erroneous information or are incomplete and create supplemental record entries as required when additional information becomes available.

(f) When record entries are verified as accurate and current or have been modified or canceled, persons responsible for processing validation packages shall complete validation certification using procedures prescribed by GCIC.

(g) Non-receipt of certification messages by GCIC cited suspense dates will result in the removal of all record entries contained in validation listings processed from GCIC/NCIC files.

(h) Validation procedures, records and supporting documents are subject to GCIC and NCIC audits.

Authority: O.C.G.A. §§ 35-3-33, 35-3-36. **History.** Original Rule entitled "Validation Procedures for Wanted/Missing Person and Stolen Property Records" filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 2, 1986, effective July 22, 1986. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 7, 1988, effective July 27, 1988. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Amended:** Filed Dec. 2, 1992, effective Dec. 22, 1992. **Repealed:** New Rule, same title, adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:**

Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140.2-.15 Procedures for Handling Missing and Unidentified Deceased Persons. Amended.

(1) All law enforcement agencies shall collect information about each person reported missing by a parent, guardian or next of kin. Information about unknown deceased persons shall also be collected and preserved for identification purposes. Information collected includes physical descriptions, descriptions of clothing, dental charts, fingerprints if available and other personal data useful in identifying missing or unknown deceased persons.

(2) Agencies receiving missing person reports shall enter appropriate records in GCIC/NCIC computerized files. Agencies investigating unknown deceased cases shall enter, or authorize entry of, unidentified deceased persons in NCIC. In compliance with federal law (42 USC 5779, Section 3701), GCIC will advise the Georgia Missing Person Clearinghouse of all such record entries.

(a) Record entries for missing minors, including juveniles reported as runaways, shall be made immediately. Entries for all other persons reported missing must be made within 12 hours, pursuant to O.C.G.A. § 35-3-36.

(b) Within sixty (60) days of entry of a missing juvenile, the agency must attempt to update the record with any available medical/dental records for identification purposes.

(c) Thirty-days after missing person records are entered in the NCIC computerized file, NCIC will check all records for completeness. NCIC sends messages to agencies of record when records are incomplete.

(d) A non-terminal agency should request assistance in making missing person record entries from the terminal agency that provides it CJIS network service.

(e) Agencies that enter or authorize the entry of missing person and unidentified deceased person records in GCIC/NCIC computerized files shall respond within 10 minutes to priority messages from other agencies reference possible identifications. Responses to messages classified as 'routine' shall be made within one hour. NCIC conducts daily matches to determine if identifiers in a missing person record are similar to those of a recent unidentified deceased person entry.

(3) Agencies authorizing entry of missing person and unidentified deceased person records shall cause these record entries to be removed from GCIC/NCIC computerized files immediately upon identification of missing or unidentified deceased persons.

Authority: O.C.G.A. §§ 35-1-8, 35-3-4, 35-3-33, 35-3-36; 42 U.S.C. 5779, Sec. 37.01. **History.** Original Rule entitled "Special Handling Provisions for Missing and Unidentified Deceased Persons" filed Sept. 6, 1984, effective Oct. 8, 1984, as specified by the Agency. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 2, 1986, effective July 22, 1986. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 7, 1988, effective July 27, 1988. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Amended:** Filed Dec. 4, 1991, effective Dec. 24, 1991. **Repealed:** New Rule entitled "Procedures for Handling Missing and Unidentified Deceased Persons" adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002; effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.16 Training. Amended.

(1) Criminal justice officials and agency heads shall provide training and retraining, as required by policy, to ensure their employees' effective performance of job-specific tasks relating to

(a) Use of the Georgia CJIS network and information files to which it provides access and CJIS network terminal operations

(b) Use of NCIC

(c) Use of Nlets

(d) Dissemination and use of CHRI

(e) State and national UCR programs

(f) Fingerprinting arrested persons and use of the OTN and CTN when reporting an arrest, update or modification of an offender's criminal history record

(g) Preparing and submitting OBTS reports with final dispositions of charges.

(2) All personnel directly associated with maintaining, processing or disseminating CHRI shall be specially trained. The training shall provide a working knowledge of federal and state regulations and laws governing the security and processing of criminal justice information. Agency heads are responsible for ensuring their personnel receive such training as supported by the GCIC Policy Manual. In cases where agency head requests for training cannot be accommodated within a reasonable time, employees are required to read the Rules of the GCIC Council as contained herein. This will provide basic knowledge regarding the access, use, control and dissemination of criminal justice information until training occurs.

(3) Managers of computer centers and governmental dispatch centers shall ensure that employees supporting criminal justice operations are trained to perform job-specific tasks relating to the functions described in paragraph (1) above.

(4) Each CJIS network terminal agency head shall immediately appoint a TAC to serve as the agency point of contact on GCIC/NCIC record validations, hit confirmations, training and all other NCIC/CJIS network related matters. GCIC shall provide job-specific training for TACs and any assistant TACs.

(5) TACs must be trained as CJIS terminal operators before admission to the TAC certification course. The minimum requirement is terminal operator practitioner.

(6) TACs shall be subject to certification training and testing within 90 days of appointment.

(7) Each TAC must attend a TAC refresher course, as required by GCIC policy, to maintain TAC certification.

(8) Agency heads and TACs are responsible for developing agency specific policies and procedures relating to CJIS network operations and the administration of terminal operator and practitioner training programs developed by GCIC. Agency heads have discretion to designate CJIS network terminals users as either terminal operators or practitioners.

(9) Terminal operators are subject to certification testing within six months of their employment or assignment of terminal operator duties and subject to re-certification testing every two years thereafter for the duration of their employment as terminal operators. Additionally, practitioners must receive training in the components of CJIS network operations they use in performing their official duties. Practitioners must also successfully complete performance tests administered by TACs and are subject to retesting every two years thereafter for the duration of their employment in which CJIS network access in necessary to complete job assignments.

(10) The appointment of a TAC, the immediate appointment of a new TAC when required to fill a TAC vacancy, the training, testing and certification of the TAC, and the training, testing, certification and recertification of terminal operators and practitioners are mandatory for initial and on-going terminal agency status on the Georgia CJIS network.

Authority: O.C.G.A. § 35-3-33. **History.** Original Rule entitled "Training" filed July 2, 1986, effective July 22, 1986. **Amended:** Rule repealed and a new Rule of same title adopted. Filed July 7, 1988, effective July 27, 1988. **Repealed:** New Rule of same title adopted. Filed Nov. 7, 1990, effective Nov. 27, 1990. **Amended:** Filed Dec. 2, 1992, effective Dec. 22, 1992. **Repealed:** New Rule, same title, adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Amended**: Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.17 Brady Handgun Violence Prevention Act. Amended.

(1) Effective November 1998, the Federal Brady Law established a National Instant Criminal Background Check System (NICS) that Federal Firearms Licensees (FFLs) must contact before transferring any

firearm to an unlicensed individual. GCIC has authority to provide criminal history, wanted person and involuntary hospitalization records information to the FBI in conjunction with the NICS and in accordance with the federal 'Brady Handgun Violence Prevention Act'.

(2) GCIC records shall include information as to whether a person has been involuntarily hospitalized. Notwithstanding any other provisions of law, and in order to carry out O.C.G.A § 16-11-172, GCIC shall be provided – in a manner agreed upon by the Probate Judges Training Council and the Georgia Bureau of Investigation (GBI) – such information and no other mental health information, to preserve the confidentiality of patient's rights in all other respects, from the involuntary hospitalization records of the probate courts concerning persons involuntarily hospitalized after March 22, 1995. Further, notwithstanding any other provisions of law and in order to carry out the provisions of O.C.G.A. § 16-11-172, GCIC shall be provided information as to whether a person has been adjudicated mentally incompetent to stand trial or not guilty by reason of insanity at the time of the crime, has been involuntarily hospitalized or both from the records of the clerks of the superior courts concerning persons involuntarily hospitalized after March 22, 1995, in a manner agreed upon by the Council of Superior Court Clerks of Georgia and the GBI to preserve the confidentiality of patient's rights in all other respects. Five years from the date that GCIC receives a person's involuntary hospitalization information, the center shall purge its records of such information as soon as practicable and, in any event, within 30 days of the expiration of such five-year period.

Authority: O.C.G.A. §§ 16-11-172, 35-3-32, 35-3-34, 35-3-38, 37-3-81; 18 U.S.C. Secs. 921-923. **History.** Original Rule entitled "Sanctions" adopted. Filed Dec. 4, 1991, effective Dec. 24, 1991. **Repealed:** New Rule entitled "Georgia Instant Background Checks for Firearms Purchases" adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Amended:** Filed Sept. 5, 2002, effective Sept. 25, 2002. **Repealed:** New Rule, same title, adopted. Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.18 The Georgia Sexually Violent Offender Registry. Amended.

(1) Georgia law places responsibility for the establishment, operation and management of a sexually violent offender registry within the Georgia Bureau of Investigation and principally, GCIC. Accordingly, GCIC will perform the following functions:

(a) Provide public access to the registry via the internet

(b) Participate in the National Sex Offender Public Registry (NSOPR)

(c) Mail non-forwarding verification letters to the last known address of each registered sex offender, as required by law. The verification letter will serve as official notification to sex offenders that they must re-register with the Sheriff's Department in their county of residence

(d) Notify sheriffs when a sex offender record is entered, updated, or deleted from the registry

(e) Publish periodic reports for sheriffs that list sex offenders and sexually dangerous predators residing in each county

(f) Notify appropriate out-of-state law enforcement agencies when a sex offender relocates to their state

(g) Conduct training on issues related to operation and maintenance of the sex offender registry.

(2) The Department of Corrections, State Board of Pardons and Paroles and the Director of Private Probation agencies will enter sex offender records on the registry. They will submit updates including photos to the CJIS file as prescribed by statute and GCIC policy.

(3) Each sheriff must maintain accurate information on all registered sex offenders residing within their jurisdiction, as required by law.

(a) Each sheriff must update all required information, i.e. residence address, employment, school, etc. as required by law.

Authority: O.C.G.A. § 42-1-12. **History:** Original Rule entitled "Georgia Sex Offender Registry" adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998.

Amended: Filed Sept. 5, 2002, effective Sept. 25, 2002. **Repealed:** New Rule, same title, adopted. Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.19 The Georgia Protective Order Registry.

(1) Georgia law places responsibility for the establishment, operation and management of a protective order registry within the GBI and principally, GCIC. Accordingly, GCIC will perform the following functions:

(a) Provide access via a secure internet web site to a centralized database for statewide protective orders

(b) Assign law enforcement officers, prosecuting attorneys and the courts a unique user ID and password established specifically for access to the registry

(c) Ensure entry into the registry of any protective order or modification thereof received from the Clerk of Court

(d) Ensure transmission to the NCIC Protection Order File of all protective orders and modifications entered in the registry that meet NCIC data requirements

(e) Authorize an alternative method of transmitting protective orders to the registry in the event of electronic failure

(f) Consult with the Georgia Commission on Family Violence regarding the effectiveness of the registry in enhancing the safety of the victims of domestic violence and stalking.

(2) The Superior Court Clerk will scan the protective orders issued by the judge and enter data requested, if available, required by NCIC.

(a) The Court Clerk shall electronically transmit a copy of the protective order or modification thereof to the registry as prescribed by statute.

(b) The Court Clerk shall provide the local Sheriff with a hard copy of all protective orders transmitted to the registry.

(3) Each Sheriff shall be responsible for the validation of all NCIC protective order entries made on its behalf by the Superior Court Clerks office.

(a) Each Sheriff shall validate in accordance with the validation steps and file retention schedule established by both GCIC and NCIC.

(b) Each Sheriff shall respond to and confirm hit confirmation requests based on the records maintained in their office.

(4) The Courts of this state shall use a standardized form or forms for the issuance of any protective order.

(a) Standardized form or forms shall be subject to approval as to form and format by GCIC and the Georgia Superior Court Clerks Cooperative Authority (GSCCCA).

(b) The form or forms shall be promulgated by the Uniform Superior Court Rules Committee.

(c) The Administrative Office of the Courts shall distribute the forms.

Authority O.C.G.A. § 19-13-50 et seq. **History.** Original Rule entitled "Sanctions" adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Repealed:** New Rule, entitled "The Georgia Protective Order Registry" adopted. Filed Sept. 25, 2007, effective Oct. 15, 2007.

140-2-.20 Sanctions. Amended.

(1) Criminal justice agencies, governmental dispatch centers and other governmental agencies are subject to GCIC administrative sanctions for violating laws governing operation of the CJIS network, these Rules or CJIS network policies published by GCIC pursuant to O.C.G.A. § 35-3-33 (13). Administrative sanctions for terminal agencies may include, but not limited to purging wanted/missing person and stolen property serial-numbered records entered in GCIC/NCIC computerized files by CJIS network agencies or established by these agencies for non-terminal agencies pursuant to signed service agreements; restricted access to the CJIS network; and suspension/revocation of an agency's CJIS network access.

(2) Administrative sanctions may be imposed on individual violators. Such sanctions may include mandatory re-training and/or re-certification of TACs, terminal operators and/or practitioners and suspension from access to the CJIS network.

(3) Individual violators are also subject to criminal prosecution when their actions constitute violations of applicable state or federal statutes.

Authority: O.C.G.A. §§ 16-9-90 et seq., 35-3-32, 35-3-38; 18 U.S.C. 641, 1030, 1343, 1951, 1952. **History:** Original Rule 140-2-.19 entitled "Sanctions" adopted. Filed Mar. 4, 1998, effective Mar. 24, 1998. **Repealed:** New Rule, same title, adopted. Filed Sept. 25, 2007, effective Oct. 15, 2007.