

DELAWARE CRIMINAL JUSTICE INFORMATION SYSTEM

Statutory Authority: 11 Delaware Code, Section 8605 (11 Del.C. §8605)

PROPOSED

PUBLIC NOTICE

Delaware Criminal Justice Information System Regulations

In compliance with the State's Administrative Procedures Act (APA - Title 29, Chapter 101 of the Delaware Code) and under the authority of Title 11 of the Delaware Code, Chapter 86, Section 8605, the Delaware Criminal Justice Information System (DELJIS) Board of Managers proposes to adopt regulations. These proposed regulations are applicable to all users of the Delaware Criminal Justice Information System (CJIS) and to any agency requesting access to CJIS from the Board. The proposed regulations will ensure that access to criminal justice information conforms to the statutory requirements outlined in Chapters 85 and 86 of Title 11 of the Delaware Code.

Copies of the proposed regulations are available for review in the October 1, 2014 edition of the *Delaware Register of Regulations*, accessible online at <http://regulations.delaware.gov> or by calling DELJIS at 302-739-4856.

The Board will hold a public hearing on the proposed regulations on October 22, 2014 from 1:00 p.m. until 3:00 p.m., at the Division of Accounting, New Castle Conference Room, 820 Silver Lake Boulevard, Dover, DE 19904.

Any person who wishes to make any written suggestions, compilations of data, briefs or other written materials concerning the proposed new regulations must submit same to Peggy A. Bell, Executive Director, DELJIS, 802 Silver Lake Blvd, Suite 101, Dover DE 19904, or by fax to 302-739-6285.

In accordance with 29 Del.C. §10118(a), the final date to receive written comments will be November 6, 2014, which is 15 days following the public hearing.

The action concerning the determination of whether to adopt the proposed regulations will be based upon the results of the Board and the consideration of the written comments filed by other interested persons.

Delaware Criminal Justice Information System Regulations

1.0 General Provisions

- 1.1 Authority. These regulations are promulgated pursuant to 11 Del.C. §8605 by the Delaware Criminal Justice Information System (DELJIS) Board of Managers.
- 1.2 Applicability. These regulations are applicable to all users of the Delaware Criminal Justice Information System (CJIS) and to any agency requesting access to CJIS from the Board.
- 1.3 Purpose. These regulations will ensure that access to criminal justice information conforms to the statutory requirements outlined in Chapters 85 and 86 of Title 11 of the Delaware Code.

2.0 Definitions

The definitions set forth in 11 Del.C. §8602 are hereby adopted and incorporated by reference in these regulations. The following words and terms, when used in these regulations, shall have the following meaning unless the context clearly indicates otherwise.

"Access" means the physical or logical (electronic) privilege to view, modify, or make use of criminal justice information, whether directly or indirectly.

"Direct access" means access to CJIS via authorized and approved DELJIS credentials (i.e., ACF2User ID and password).

"Indirect access" means access to criminal justice information, in oral, online or printed form, by an individual without approved DELJIS credentials for direct access.

"Administrative leave" means a temporary leave from employment, including without limitation, extended leave, family medical leave, or suspension from an agency.

"Authorized Agency" means any criminal justice agency or governmental agency, as defined by 11 Del.C. §8602(3) and 11 Del.C. §8602(7) respectively, having access to the CJIS.

"Authorized User" means any employee, intern, extern, contractor, volunteer, or other individual or group of individuals, acting on behalf of an Authorized Agency, who has been appropriately vetted by DELJIS and has been granted access to criminal justice information.

"Board" means the Delaware Criminal Justice Information System Board of Managers established by 11 Del.C. §8603.

"Criminal history record information" or **"CHRI"** means a subset of CJI, set forth in 11 **Del.C.** §8602(2), that includes identifiable descriptions and notations of arrests, detentions, indictments, informations or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision and release.

"Criminal justice information" or **"CJI"** is an abstract term used to refer to all CJIS data necessary for Authorized Agencies to perform their mission and enforce the laws, including but not limited to: biographic or biometric data, identity history, person, organization, property, division of motor vehicles information, and/or case or incident history. In addition, CJI refers to the CJIS-provided data necessary for Authorized Agencies to make hiring decisions.

"Biographic data" means information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

"Biometric data" means data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.

"Case or incident history" means all relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regard to criminal justice information, it is the information about the history of incidents.

"Identity history" means textual data that corresponds with an individual's biometric data, providing a history of criminal or civil events for the identified individual.

"Property data" means information about vehicles and property associated with a crime.

"Criminal Justice Information System" or **"CJIS"** means the computer hardware, software and communication network used for the collection, warehousing, and timely dissemination of relevant CJI to qualified law enforcement, criminal justice agencies and the courts, governmental agencies, and other agencies, that is managed, operated and maintained by DELJIS.

"Delaware Criminal Justice Information System" or **"DELJIS"** means the administrative body created within 11 **Del.C.** Ch. 86 that manages, operates, and maintains CJIS in the State of Delaware.

"Improper Access or Breach" means any improper dissemination, unauthorized use, or obtaining CJI, directly or indirectly, whether oral, online or printed form, without a specific business reason, and shall include access for the purpose of confirming the existence or non-existence of CJI or CJIS, or the transmission or non-transmission of information improperly obtained.

"National Crime Information Center" or **"NCIC"** means an information system that stores CJI that can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

"National Instant Criminal Background Check System" or **"NICS"** means a system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

"Secondary dissemination" means the promulgation of CJI from an Authorized Agency to an agency or individual not authorized by Chapters 85 and 86 of Title 11 of the Delaware Code or these regulations.

"Serious motor vehicle violation" means any violation of the motor vehicle code that is classified as a felony or driving while under the influence

"Victim's copy" means the automated Victim's copy of a police report created pursuant to 11 **Del.C.** §9410. For purposes of these regulations, a Victim's copy includes all police report details up to but not including the police narrative or statement.

3.0 Officers of the DELJIS Board of Managers

- 3.1 The officers of the Board shall be a Chairperson, Vice-Chairperson, and a Secretary. These officers shall perform the duties prescribed herein.
- 3.2 The Chairperson, Vice-Chairperson, and Secretary shall be elected from the voting members of the Board.
- 3.3 At the regular meeting held in March of each calendar year, the officers shall be elected by ballot to serve for one year or until their successors are elected; their term of office shall begin at the close of the meeting at which they are elected.
- 3.4 No member shall hold more than one office at a time, and no member shall be eligible to serve more than two consecutive terms in the same office.
- 3.5 The duties and responsibilities of the officers shall be:

- 3.5.1 Chairperson: chairs meetings, prepares or approves agendas, acts to implement Board policy, and other such duties as prescribed by the Board or these regulations.
- 3.5.2 Vice-Chairperson: assumes chair in the absence of the Chairperson.
- 3.5.3 Secretary: assumes chair in the absence of the Chairperson and Vice-Chairperson. Reviews minutes of the Board meetings prior to dissemination.

4.0 Committees of the DELJIS Board of Managers

4.1 Executive Committee

- 4.1.1 The Executive Committee shall be composed of not less than three members of the Board and shall be chaired by the Board Chairperson.
- 4.1.2 The Executive Committee shall have the power to act between meetings of the Board. Actions of the Executive Committee are subject to confirmation by a quorum of the Board.

4.2 Nominating Committee

- 4.2.1 There shall be a Nominating Committee for the purpose of developing a slate of potential candidates to fill the officer positions. The Board Chairperson shall appoint, as approved by the Board, the Nominating Committee Chairperson and members. This action and approval shall be accomplished no later than the December Board meeting of each calendar year. The Nominating Committee shall provide said slate of potential officer candidates to the Board at the subsequent January meeting.

- 4.3 The Board Chairperson shall have the authority to establish such Standing or Ad Hoc Committees as deemed necessary to conduct DELJIS business. The Board Chairperson shall:

- 4.3.1 Provide a mission or purpose statement for each committee established;
- 4.3.2 Provide the objectives to be accomplished by each committee established; and
- 4.3.3 Determine the number of members of each committee and appoint the respective members and chairperson.

5.0 Agency Access to CJIS

- 5.1 To determine if access should be granted to an agency, the Board will consider whether the agency meets the conditions outlined in 11 **Del.C.** §8610.
- 5.2 An application for access to CJIS shall be submitted to the DELJIS Security Manager on forms approved by the Board.
- 5.3 The Board may require additional information or explanation when it has questions about an agency's qualifications or application materials. An application is not complete or in proper form until the Board has received all required and requested documents, materials, and information.
- 5.4 Agencies requesting access to CJIS must demonstrate a reasonable business need.
- 5.5 Approval of the agency's application, which may be in whole, in part, or as modified by the Board, shall require a two-thirds majority of the entire Board as prescribed by 11 **Del.C.** §8610(3).
- 5.6 Upon approval of the agency's application, which may be in whole, in part, or as modified by the Board, the agency shall enter into a user's agreement as prescribed by 11 **Del.C.** §8614(4), with the State Bureau of Identification (SBI) pursuant to 11 **Del.C.** §8514.
- 5.7 The Board's decision to approve, modify, or deny the agency's application is final and is not subject to appeal or further review.

6.0 Responsibilities of Authorized Agencies

- 6.1 Authorized Agencies shall obtain a fingerprint based criminal history report from SBI & FBI for each Authorized User.
- 6.2 Authorized Agencies must ensure all Authorized Users within their agency annually acknowledge that they have read and understand these regulations. The Authorized Agency shall be responsible for returning a signed acknowledgment for each Authorized User to the DELJIS Security Manager.
- 6.3 Authorized Agencies must ensure that Authorized Users within their agency comply with Chapters 85 and 86 of Title 11 of the Delaware Code and these regulations.
- 6.4 The Authorized Agency head or designee is responsible for ensuring all Authorized Users attend the DELJIS training commensurate to each Authorized User's employment position, as set forth by DELJIS.
- 6.5 The Authorized Agency head or designee shall certify for completeness and accuracy a list of Authorized Users provided annually by DELJIS to the agency head. The list shall be certified as is, or corrected to delete,

add, or change Authorized Users and returned to DELJIS within 60 days of receipt of said list by the agency head or designee.

- 6.6 Authorized Agencies are responsible for notifying the DELJIS Security Manager or designee immediately upon an Authorized User's departure (transfer, termination, resignation, or retirement) from the agency.
- 6.7 Authorized Agencies are responsible for notifying the DELJIS Security Manager or designee immediately upon an Authorized User's administrative leave from the agency, if the administrative leave exceeds 24 hours or results in loss of agency privileges, identification credentials, or departmental weapon.
- 6.8 Authorized Agencies are responsible for notifying the DELJIS Security Manager or designee immediately upon an Authorized User's arrest, charge, or conviction of a criminal violation or offense in any jurisdiction immediately upon receiving notification of the same.
- 6.9 Authorized Agencies are responsible for notifying the DELJIS Security Manager or designee immediately upon discovery of an Authorized User's Improper Access or Breach.
- 6.10 Authorized Agencies are required to follow the Records Retention and Destruction procedures provided in Section 7.0, that require CJIS, NCIC or NICS information be securely disposed of. Whether the information is in a physical form (printout) or an electronic form (hard drive, flash drive, etc.) the information must be disposed of in such a way that unauthorized people cannot retrieve it. For most agencies, this means ensuring printed information is shredded onsite by the user.
- 6.11 The DELJIS Security Manager or designee will conduct an Authorized Agency site inspection when required to ensure physical site suitability and security.
- 6.12 Authorized Agencies must maintain secondary dissemination logs consistent with 11 Del.C. §8513(e).

7.0 CJIS Records Retention and Destruction

- 7.1 All information retrieved via CJIS, NCIC, or NICS is highly confidential and shall be afforded security to prevent unauthorized access to or use of that data. To prevent the misuse or improper dissemination of information, any printed information must be immediately destroyed after its intended use. Documents stored in electronic form (hard drive, flash drive, etc.) must be disposed of in such a way that unauthorized people cannot retrieve it.
- 7.2 Under no circumstances should printed information be maintained in personnel files by any Authorized Agency or in court records by any Delaware court.
- 7.3 Printed information shall be destroyed by shredding as follows:
 - 7.3.1 In-state information, including CJIS information, may be shredded onsite or added to the purge list and delivered to the Delaware Public Archives for shredding, and must follow the destruction protocols used by Delaware Public Archives in accordance with 29 Del.C. §504(b).
 - 7.3.2 Out-of-state information, including NCIC or NICS information, must be shredded onsite and witnessed or carried out by authorized personnel. Paper shredding service providers are prohibited from shredding printed information offsite, but may conduct agency supervised onsite shredding. Regardless of who destroys the records, they must follow the destruction protocols used by Delaware Public Archives in accordance with 29 Del.C. §504(b).
- 7.4 Electronic information shall be destroyed as follows:
 - 7.4.1 The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel and follow the destruction protocols used by Delaware Public Archives in accordance with 29 Del.C. §504(b).

8.0 User Access to CJIS

- 8.1 To determine if a user credential should be granted to an individual, the Executive Director or designee may consider whether the individual has:
 - 8.1.1 Been charged with or convicted of a criminal offense or serious motor vehicle violation;
 - 8.1.2 An active warrant or capias;
 - 8.1.3 An active Protection from Abuse Order or Protection Order entered against him/her;
 - 8.1.4 Intentionally falsified any official record;
 - 8.1.5 Improperly accessed CJIS previously;
 - 8.1.6 Engaged in any other activity that could endanger the security, privacy, or integrity of CJIS.

8.2 Denial Procedure

- 8.2.1 The Executive Director or designee makes the initial determination to deny access.
- 8.2.2 The DELJIS Security Manager or designee will notify the Authorized Agency head or designee in writing by email, fax or U.S. Mail if the user is denied. A notice of denial will include the following:
 - 8.2.2.1 Name of user requesting access; and
 - 8.2.2.2 The reasons for the denial.
- 8.2.3 The DELJIS Security Manager or designee will also notify the user in writing by email, fax, or U.S. Mail if the user is denied.
- 8.2.4 An appeal may be initiated by the user by submitting a request for a hearing in writing by email, fax or U.S. Mail to the attention of the Chairperson of the Board within fifteen (15) days of receipt of the notice of denial.
- 8.2.5 The Board shall review the appeal and the user shall be given the opportunity to be heard by the Board within sixty (60) days of receipt of the letter of appeal, unless extenuating circumstances require a longer period.

9.0 Responsibilities of Authorized Users

- 9.1 Authorized Users must hold themselves to the highest ethical standards and must conduct themselves in a manner that will ensure the security, integrity, and confidentiality of the information contained within CJIS.
- 9.2 Authorized Users shall not access information contained within CJIS for any reason other than an authorized business related reason.
- 9.3 Authorized Users agree to comply with Chapters 85 and 86 of Title 11 of the Delaware Code and these regulations.
- 9.4 Authorized Users must annually acknowledge that they have read and understand these regulations.
- 9.5 Authorized Users must complete DELJIS training prior to being granted an Authorized User credential. The DELJIS Training Supervisor may approve temporary or conditional access to CJIS by an Authorized User before completing DELJIS training.
- 9.6 Authorized Users are required to follow the Records Retention and Destruction procedures provided in Section 7.0, that require CJIS, NCIC or NICS information be securely disposed of.
- 9.7 Authorized Users who improperly access or become aware of improper access of CJIS by another user, or by any other entity, shall immediately report the violation to their agency head, management, or directly to the DELJIS Security Manager or designee, and shall cooperate with and assist in the conduct of any administrative investigation pursuant to Section 12.0.
- 9.8 Authorized Users who have been arrested, charged, convicted of a criminal offense, a serious motor vehicle offense, or a violation in any jurisdiction shall notify their agency head or designee within 24 hours of the arrest, charge, or conviction.
- 9.9 Authorized Users employed with local and municipal agencies must annually read and submit a Department of Technology and Information Acceptable Use Policy to DELJIS. Authorized Users employed with an agency of the State must annually read and submit a Department of Technology and Information Acceptable Use Policy to their respective agency.
- 9.10 Authorized Users must maintain secondary dissemination logs consistent with 11 **Del.C.** §8513(e).

10.0 Suspension of CJIS Access for Any Arrest or Criminal Offense of an Authorized User

- 10.1 Upon notification or discovery of an arrest for a criminal offense, violation, or serious motor vehicle offense, the Executive Director or designee will make the initial determination if the charge warrants a temporary suspension of the Authorized User's credentials.
- 10.2 If the Executive Director or designee temporarily suspends the Authorized User's credentials, access will be suspended immediately and the DELJIS Security Manager or designee will notify the Authorized Agency head or designee in writing by email, fax, or U.S. Mail of the following:
 - 10.2.1 Name of Authorized User who was suspended; and
 - 10.2.2 Date of the arrest, conviction, or violation.
- 10.3 The DELJIS Security Manager or designee will also notify the Authorized User in writing by email, fax, or U.S. Mail of any suspension.
- 10.4 An appeal may be initiated by the user by submitting a request for a hearing in writing by email, fax or U.S. Mail to the attention of the Chairperson of the Board within fifteen (15) days of receipt of the notice of suspension.

- 10.5 The Board shall review the appeal and the user shall be given the opportunity to be heard by the Board within sixty (60) days of receipt of the letter of appeal, unless extenuating circumstances require a longer period.

11.0 Suspension of CJIS Access for Improper Access or Breach

- 11.1 Upon notification or discovery of any violation involving Improper Access or Breach, the Executive Director or designee will authorize an administrative investigation pursuant to Section 12.0. The Executive Director or designee will also make an initial determination as to whether the apparent violation warrants a temporary suspension of the Authorized User's credentials.
- 11.2 If the Executive Director or designee suspends the Authorized User's credentials, access will be suspended immediately and the DELJIS Security Manager or designee will notify the Authorized Agency head or designee in writing by email, fax, or U.S. Mail of the following:
- 11.2.1 Name of Authorized User who was suspended; and
- 11.2.2 The alleged violation and date thereof.
- 11.3 The DELJIS Security Manager or designee will also notify the Authorized User in writing by email, fax, or U.S. Mail of any suspension.

12.0 Procedure for Conducting Administrative Investigations of Improper Access or Breach by an Authorized User

- 12.1 No Authorized User shall refuse to cooperate in the administrative investigation of a suspected violation or breach, whether such investigation is conducted by SBI or DELJIS. Refusal to cooperate shall result in a permanent suspension of the Authorized User.
- 12.2 An SBI investigator will conduct an administrative investigation of any Authorized User who is an employee, intern, extern, contractor, volunteer, or other individual or group of individuals acting on behalf of the Delaware State Police (DSP). DELJIS will work with the SBI investigator to explain the CJIS system functionality and screen access, if needed.
- 12.3 A DELJIS investigator will serve as the SBI designee to conduct any administrative investigation for all Authorized User's excluding any Authorized User of DSP.
- 12.4 The investigator will schedule a date and time to interview the user at a mutually agreed upon location.
- 12.5 The interviews will be conducted in a respectful, non-hostile and or non-aggressive manner.
- 12.6 At the conclusion of the interview, the investigator will advise the user of the possible sanctions which may be imposed by the Board.
- 12.7 The investigator will fill out a written law enforcement investigative support system (LEISS) report, detailing the facts of the investigation.
- 12.8 The LEISS report will be approved by the Executive Director or the supervisor of the DSP officer who investigated the complaint.
- 12.9 At the conclusion of the investigation, the facts of the investigation will be submitted to the Attorney General's office by the Executive Director to determine if there was any violation of Delaware law warranting criminal prosecution.
- 12.10 At the conclusion of the investigation, the DELJIS Security Manager or designee will notify the Authorized Agency head or designee in writing by email, fax, or U.S. Mail of the following:
- 12.10.1 Name of Authorized User who was suspended;
- 12.10.2 The alleged violation and date thereof; and
- 12.10.3 Status of the matter following the administrative investigation.
- 12.11 The DELJIS Security Manager or designee will also notify the Authorized User in writing by email, fax, or U.S. Mail of the status of the matter following the administrative investigation.
- 12.12 An appeal may be initiated by the user by submitting a request for a hearing in writing by email, fax or U.S. Mail to the attention of the Chairperson of the Board within fifteen (15) days of receipt of the notice of suspension.
- 12.13 The Board shall review the appeal and the user shall be given the opportunity to be heard by the Board within sixty (60) days of receipt of the letter of appeal, unless extenuating circumstances require a longer period.

13.0 Hearings

- 13.1 All hearings will be conducted in accordance with the Delaware Freedom of Information Act, 29 Del.C. Ch. 100.
- 13.2 Presence of the appellant is required. Failure to appear within 10 minutes of the time indicated on the notice will result in the Board hearing the appeal in the absence of the appellant or dismissal of the appeal.

- 13.3 At any hearing, a party may appear pro se or be represented by an attorney-at-law duly admitted to practice law in the State of Delaware or by a union representative at his or her own expense. The appellant will have the right to appear and testify at the hearing; the right to call witnesses and to present other evidence in the form of testimony and/or documents; and the right to cross-examine any witnesses who may testify at the hearing.
- 13.4 The Board or its attorney may administer oaths, examine any witness, receive exhibits into evidence, and move the admissions of documents and things into evidence.
- 13.5 Strict rules of evidence shall not apply.
- 13.6 At any hearing involving Improper Access or Breach, the investigator or their designee shall attend and present the facts of the administrative investigation directly to the Board.
- 13.7 The Board will render a decision based on the substantial evidence presented.
- 13.8 The Board may affirm, modify, or reverse, in whole or in part, any decision to temporarily suspend, revoke, reject, or deny access to CJIS, and may order that such suspension, revocation, rejection, or denial become permanent.
- 13.9 A written decision shall be rendered by the Board within sixty (60) days of the hearing, unless extenuating circumstances require a longer period.
- 13.10 The Board's decision on appeal is final and is not subject to further appeal or review.

14.0 Sanctions

- 14.1 If the Board determines there has been a violation of Title 11, Chapter 85 or 86 or these regulations by an Authorized Agency or Authorized User, it may impose any of the following sanction(s), singularly or in combination:
 - 14.1.1 Require retraining on the CJIS system, specifically the security training.
 - 14.1.2 Require a log of all CJIS transactions for a specific period of time. The log will be provided to the DELJIS Security Manager or designee based on the time line imposed by the Board.
 - 14.1.3 Require monitoring for a specific period of time. The DELJIS Security Manager or designee may contact the user at any time, requesting justification as to why the User accessed a specific record.
 - 14.1.4 Suspend the agency's or user's access for a specific period of time.
 - 14.1.5 Suspend the agency's or user's access permanently.
- 14.2 Failure to comply with any imposed sanctions will result in additional sanctions, up to and including permanent suspension.
- 14.3 The DELJIS Security Manager or designee will notify the Authorized Agency head or designee in writing by email, fax, or U.S. Mail of any sanctions imposed by the Board.
- 14.4 The DELJIS Security Manager or designee will also notify the Authorized User in writing by email, fax, or U.S. Mail of any sanctions imposed by the Board.

18 DE Reg. 265 (10/01/14) (Prop.)