

SB3816



104TH GENERAL ASSEMBLY

State of Illinois

2025 and 2026

SB3816

Introduced 2/6/2026, by Sen. Celina Villanueva

SYNOPSIS AS INTRODUCED:

New Act
5 ILCS 140/7

Creates the Automated License Plate Recognition System Act. Sets forth provisions regarding authorized uses of an automated license plate recognition system, data retention, prohibited uses of an automated license plate recognition system, restrictions, requirements for use, preservation and disclosure, required data collection, reporting requirements, admissibility, privacy, penalties, and a private right of action. Makes a conforming change in the Freedom of Information Act. Effective immediately.

LRB104 20207 LNS 33658 b

A BILL FOR

1 AN ACT concerning transportation.

2 **Be it enacted by the People of the State of Illinois,**
3 **represented in the General Assembly:**

4 Section 1. Short title. This Act may be cited as the
5 Automated License Plate Recognition System Act.

6 Section 5. Definitions. As used in this Act:

7 "ALPR user" means a person or entity that owns or operates
8 an ALPR device.

9 "Automatic license plate reader" or "ALPR" means software,
10 hardware or equipment, including mobile applications or fixed,
11 mobile, or portable cameras, used to automatically record
12 data, capture images, take photos and store vehicle license
13 plate information. "Automatic license plate reader" or "ALPR"
14 includes a device that is owned or operated by a person who is
15 not an employee of a law enforcement agency or government
16 entity to the extent that data collected by the reader is or
17 may be shared with a law enforcement agency or government
18 entity.

19 "Automated license plate reader system" or "ALPR system"
20 means a system, software, or computer algorithm, whether used
21 independently or in combination with one or more fixed,
22 mobile, or portable automated cameras or mobile applications,
23 that is used to read and convert images of license plates and

1 the characters they contain into computer-readable data, that
2 may result in a searchable computerized database. "Automated
3 license plate reader system" or "ALPR system" includes an
4 automated license plate recognition system.

5 "Biometric identifier" has the same meaning as in the
6 Biometric Information Privacy Act.

7 "Biometric information" means any information, regardless
8 of how it is captured, converted, stored, or shared, based on
9 an individual's biometric identifier used to identify an
10 individual. "Biometric information" does not include
11 information derived from items or procedures excluded under
12 the definition of biometric identifiers.

13 "Captured plate data" or "data" means the GPS coordinates,
14 date and time, photograph and other digital images, license
15 plate number, and any other information or data captured by,
16 derived from, or inferred from any automated license plate
17 reader system, including, but not limited to, make, model,
18 color, and automobile characteristics.

19 "Employee of a foreign entity" means an employee or
20 contractor of any branch of the federal government or federal
21 agency, a state or local agency or unit of local government
22 other than this State.

23 "Employee of a government entity" means an employee or
24 contractor of any State or local agency, unit of local
25 government, or private entity charged with the enforcement of
26 State, county, or municipal laws. "Employee of a government

1 entity" does not include law enforcement agencies.

2 "Employee of a law enforcement agency" means any
3 department or agency of this State or a political subdivision
4 of this State or local agency, or unit of local government,
5 charged with the enforcement of State, county, or municipal
6 laws or with managing custody of detained persons in this
7 State or jurisdiction, or vested by law with the duty to
8 maintain public order and to enforce criminal laws, or an
9 individual acting for or on behalf of the State or political
10 subdivision thereof.

11 "Facial recognition" means any combination of hardware,
12 software, firmware, application, or tools that assists in
13 identifying or verifying or persistently tracking an
14 individual based on a scan of an individual's face geometry in
15 still or video images, streams, or recordings.

16 "Forcible felony" means the following offenses as defined
17 in the Criminal Code of 2012 or substantially similar federal
18 or other State criminal laws: first degree murder, second
19 degree murder, predatory criminal sexual assault of a child,
20 aggravated criminal sexual assault, criminal sexual assault,
21 trafficking in persons, involuntary servitude, armed robbery,
22 home invasion, aggravated arson, arson, aggravated kidnaping,
23 kidnaping, and aggravated battery resulting in great bodily
24 harm or permanent disability or disfigurement.

25 "Foreign entity" means any branch of the federal
26 government or federal agency or a state or local agency or unit

1 of local government other than this State.

2 "Government entity" means a State or local agency, unit of
3 local government, or private entity charged with the
4 enforcement of State, county, or municipal laws. "Government
5 entity" does not include law enforcement agencies.

6 "Hot list" means a predetermined list or database of
7 license plates relevant and material to an ongoing
8 investigation for comparison against license plates or
9 vehicles scanned by ALPRs.

10 "Law enforcement agency" means any department or agency of
11 this State or a political subdivision of this State or local
12 agency, or unit of local government, charged with the
13 enforcement of State, county, or municipal laws or with
14 managing custody of detained persons in this State or
15 jurisdiction, or vested by law with the duty to maintain
16 public order and to enforce criminal laws, or an individual
17 acting for or on behalf of the State or a political subdivision
18 thereof.

19 Section 10. Authorized uses.

20 (a) It is unlawful for any law enforcement agency or
21 government entity to use, operate, or access any ALPR, ALPR
22 system, or captured plate data, except when authorized by
23 subsections (b), (c), and (d) and used in compliance with this
24 Act.

25 (b) An ALPR, ALPR system, or captured plate data may be

1 used, operated, or accessed by a law enforcement agency for
2 the comparison of captured plate data with (i) Illinois Amber
3 Alert, Silver Search, Endangered Missing Person Advisory, and
4 FBI Kidnapping and Missing Persons lists, (ii) the Secretary
5 of State Department of Police and Vehicle Services Department
6 databases maintained by the Secretary of State, (iii) the Law
7 Enforcement Agencies Data System maintained by the Illinois
8 State Police, and (iv) license plate numbers that have been
9 manually entered into a State or local ALPR system database
10 upon an officer's determination that the vehicles or
11 individuals associated with the license plate number are
12 relevant and material to an investigation of a vehicle that
13 is:

14 (1) associated with a missing person as defined by
15 Illinois Amber Alert, Silver Search or Endangered Missing
16 Person Advisory criteria;

17 (2) stolen;

18 (3) associated with a hit and run crash;

19 (4) registered to an individual for whom there is an
20 outstanding felony warrant; or

21 (5) related to or involved in a forcible felony.

22 (c) An ALPR, ALPR system, or captured plate data may be
23 used, operated, or accessed by a government entity:

24 (1) for the purpose of electronic toll assessment and
25 collection;

26 (2) by parking enforcement entities for regulating the

1 use of parking facilities or enforcing time restrictions
2 on the use of parking spaces; or

3 (3) for controlling access to secured areas that have
4 clear boundaries, entry only through specific controlled
5 points and limited access.

6 (d) An ALPR, ALPR system, or captured plate data may be
7 used, operated, or accessed by a law enforcement agency or
8 government entity to identify and track vehicles used by
9 foreign entities, or employees of foreign entities, for the
10 purpose of investigating whether vehicles, individuals, or
11 agencies associated with the license plates are engaged in the
12 following unlawful conduct:

13 (1) monitoring, tracking, or detaining individuals or
14 groups engaging in political protests, marches,
15 demonstrations, or other assembly protected by the First
16 Amendment;

17 (2) immigration enforcement without a judicial order;

18 (3) vehicle crashes;

19 (4) swapping, altering, tampering with, or otherwise
20 making any change to a license plate that is properly
21 displayed on a vehicle in violation of subsection (1) of
22 Section 3-413 of the Illinois Vehicle Code;

23 (5) displaying or affixing to a vehicle any license
24 plate not authorized by law and issued by the Secretary of
25 State for use on that vehicle in violation of paragraph
26 (4) of subsection (a) of Section 4-104 of the Illinois

1 Vehicle Code;

2 (6) actions of foreign entities, and employees of
3 foreign entities, that are relevant to the Illinois
4 Accountability Commission's work, or that of any other
5 State, city, municipal, or federal body created to gather
6 information, documentation, and reports of potential
7 violations of law by federal agencies, employees, or
8 contractors, for investigation purposes; or

9 (7) violations of State, county or municipal laws or
10 ordinances.

11 (e) Law enforcement agencies and government entities
12 authorized to use ALPRs, ALPR systems or captured plate data
13 under this Section are required to update their ALPR systems
14 in real-time at the beginning of each shift, or whenever such
15 updates are available, and must document the reason for each
16 manually entered license plate.

17 Section 15. Data retention for authorized uses. Captured
18 plate data collected by or on behalf of a law enforcement
19 agency or government entity, as authorized for collection
20 under Section 10, shall not be used, operated, or accessed for
21 any other purpose and shall be deleted within 3 days, except
22 that such data may be retained:

23 (1) for as long as such captured plate data is needed
24 as evidence of specific unlawful conduct enumerated in
25 subsection (b) of Section 10, as long as captured plate

1 data is a confirmed hit and is destroyed at the conclusion
2 of either an investigation that does not result in any
3 criminal charges being filed, or any criminal action
4 undertaken in the matter involving the captured plate
5 data;

6 (2) for purposes of and only to the extent necessary
7 under subsection (c) of Section 10;

8 (3) for as long as such captured plate data is needed
9 for identification, tracking, or investigation purposes
10 under paragraphs (1) through (5) and (7) of subsection (d)
11 of Section 10;

12 (4) for as long as such captured plate data is needed
13 to document and investigate the conduct of federal
14 agencies, employees, or contractors under paragraph (d)(6)
15 of Section 10, and is destroyed at the conclusion of (i) an
16 Illinois Accountability Commission investigation that does
17 not result in a referral, (ii) an investigation conducted
18 by an agency or entity based on a referral by the Illinois
19 Accountability Commission as authorized by Executive Order
20 2025-06, or (iii) any other State, municipal, or federal
21 investigation described in paragraph (6) of subsection (d)
22 of Section 10;

23 (5) Pursuant to a preservation request or disclosure
24 order under Section 35; or

25 (6) Pursuant to a valid criminal warrant issued upon a
26 judicial determination of probable cause, and in

1 compliance with the requirements of the Fourth Amendment
2 to the U.S. Constitution and Article I, Section 6 of the
3 Illinois Constitution.

4 Section 20. Prohibited uses.

5 (a) It is unlawful for any law enforcement agency or
6 government entity to:

7 (1) sell, lease, rent, or purchase any captured plate
8 data;

9 (2) share, transfer, or otherwise provide captured
10 plate data to any foreign entity or employee of a foreign
11 entity, except if authorized under subparagraph (B) of
12 paragraph (3) of subsection (b) of Section 25;

13 (3) use or allow access to any ALPR, ALPR system, or
14 captured plate data to seek or compile information on any
15 individual, group, or organization based solely on:

16 (A) political, social, or religious views or
17 activities;

18 (B) participation in non-criminal organizations or
19 lawful events;

20 (C) race, ethnicity, citizenship, age, disability,
21 gender, gender identity, sexual orientation, or other
22 classification protected by law; or

23 (D) seeking or providing access to lawful health
24 care as defined in Section 28-10 of the Lawful Health
25 Care Activity Act;

1 (4) use, or allow access to, any ALPR, ALPR system or
2 captured plate data to:

3 (A) monitor, track, investigate or detain
4 individuals (i) engaging in political protests,
5 marches, demonstrations, trainings and community
6 gatherings, or other assembly protected by the First
7 Amendment, (ii) seeking or providing lawful health
8 care as defined in Section 28-10 of the Lawful Health
9 Care Activity Act, or (iii) for immigration
10 enforcement purposes;

11 (B) monitor, track, or investigate organizations
12 that organize or provide support for (i) activities
13 related to freedom of speech, freedom of the press,
14 the right to peaceably assemble, and the right to
15 petition the government as protected by the First
16 Amendment and Illinois law or (ii) access to lawful
17 health care as defined in Section 28-10 of the Lawful
18 Health Care Activity Act; or

19 (C) gather location data or compile information,
20 including for the purpose of creating or populating
21 any database, watch list, or any other mechanism that
22 can be used to target and surveil (i) political
23 protests, marches, demonstrations, community
24 trainings, or gatherings or other assembly protected
25 by the First Amendment, (ii) health facilities that
26 provide lawful health care as defined in Section 28-10

1 of the Lawful Health Care Activity Act, or (iii)
2 public schools, public libraries, courthouses, and
3 shelters for immigration enforcement purposes;

4 (5) use, or allow access to, an ALPR, ALPR system, or
5 captured plate data for immigration enforcement;

6 (6) use facial recognition software or technology, or
7 other biometric information, in combination with any ALPR,
8 ALPR system, or captured plate data; or

9 (7) enter into a contract, continue to contract with,
10 or share information with a vendor when the agency or
11 entity knows, or should have known, that captured plate
12 data shared using the vendor's ALPR or ALPR system has
13 been or will be used to:

14 (A) monitor, track, investigate or detain
15 individuals (i) engaging in political protest,
16 marches, demonstrations, trainings and community
17 gatherings, or other assembly protected by the First
18 Amendment, (ii) seeking or providing lawful health
19 care as defined in Section 28-10 of the Lawful Health
20 Care Activity Act, or (iii) for immigration
21 enforcement purposes; or

22 (B) monitor, track, or investigate organizations
23 that organize or provide support for (i) activities
24 related to freedom of speech, freedom of the press,
25 the right to peaceably assemble, and the right to
26 petition the government as protected by the First

1 Amendment and State law or (ii) access to lawful
2 health care as defined in Section 28-10 of the Lawful
3 Health Care Activity Act.

4 (b) It is unlawful for any vendor or contractor to sell,
5 share, allow access to, or transfer captured plate data with
6 any foreign entity unless the requesting agency has obtained a
7 criminal warrant issued upon a judicial determination of
8 probable cause, and in compliance with the requirements of the
9 Fourth Amendment to the U.S. Constitution and Article I,
10 Section 6 of the Illinois Constitution.

11 (c) It is unlawful for any law enforcement agency,
12 government entity, or vendor, to operate, maintain or access
13 an ALPR, an ALPR system, or captured plate data unless that
14 agency, entity or vendor is in full compliance with the
15 requirements set forth in this Act.

16 Section 25. Restrictions on use.

17 (a) Beginning after the effective date of this Act, all
18 new, updated expansions of, or addenda of contractual
19 agreements with ALPR vendors shall mandate that no default
20 access is provided to any national ALPR database and law
21 enforcement agency or government entity captured plate data,
22 is by default, not accessible to any other law enforcement
23 agency, government entity, or foreign entity.

24 (b) It is unlawful to access, share, transfer, or
25 otherwise provide locally collected captured plate data

1 unless:

2 (1) the law enforcement agency or government entity in
3 receipt of the request is authorized to access, share,
4 transfer, or otherwise provide the captured plate data
5 under this Act;

6 (2) the captured plate data requested is authorized
7 under subsection (b) or (d) of Section 10; and

8 (3) the requester is:

9 (A) an in-state law enforcement agency, in
10 compliance with this Act, the requesting agency is in
11 receipt of a valid written declaration as required
12 under Section 2-130 of the Illinois Vehicle Code, and
13 the request is accompanied by a valid and current case
14 file number that is linked to a downloadable detailed
15 file or report;

16 (B) making the request pursuant to a valid
17 criminal warrant issued upon a judicial determination
18 of probable cause, and in compliance with the
19 requirements of the Fourth Amendment to the U.S.
20 Constitution and Article I, Section 6 of the Illinois
21 Constitution; or

22 (C) making the request pursuant to a disclosure
23 order authorized under Section 35.

24 Section 30. Requirements for use.

25 (a) Prior to using, operating, maintaining, or accessing

1 any ALPR, ALPR system, or captured plate data, a law
2 enforcement agency or government entity shall:

3 (1) Provide a presentation that includes a meaningful
4 opportunity for public comment at a regularly scheduled
5 public meeting of the governing body of the law
6 enforcement agency or government entity.

7 (A) Before a decision is made to use an ALPR, ALPR
8 system, or captured plate data, the law enforcement
9 agency or government entity shall provide a public
10 presentation that includes (i) information about the
11 ALPR, including information on the technology,
12 equipment, tools, and associated vendors, (ii)
13 authorized uses under this Act, and (iii) where, why,
14 and how it may be used. The presentation must provide a
15 meaningful opportunity for the public to comment, ask
16 questions, give feedback, and raise concerns.

17 (B) If use of an ALPR system was approved and
18 implemented before the effective date of this Act, the
19 law enforcement agency or government entity shall
20 provide a public presentation, prior to the effective
21 date of this Act, that includes (i) information about
22 the ALPR systems, including information on the
23 technology, equipment, tools, and vendors used, (ii)
24 where, why, and how they have been used, (iii) the
25 types and description of information collected,
26 shared, and received, and (iv) any changes that will

1 be made to comply with this Act. The presentation must
2 provide a meaningful opportunity for the public to
3 comment, ask questions, give feedback, and raise
4 concerns. If the presentation is not made before the
5 effective date of this Act, the law enforcement agency
6 or government entity shall be prohibited from
7 continuing to operate, use or access any ALPR, ALPR
8 system or captured plate data until a presentation
9 that meets the requirements under this subsection is
10 completed.

11 (2) Adopt, implement, disclose, and maintain an ALPR
12 usage and privacy policy that ensures that the collection,
13 access, use, sharing, retention and deletion of ALPR
14 captured plate data is authorized under this Act and
15 consistent with respect for individuals' privacy, civil
16 liberties, and civil rights, including prohibiting
17 non-essential data collection and sharing, and protecting
18 the security of data collected. The ALPR usage and privacy
19 policy shall be made available to the public in writing
20 and shall be conspicuously posted or linked to its
21 Internet website in a manner that is easily accessible to
22 individuals. The usage and privacy policy shall, at a
23 minimum, include the following information:

24 (A) authorized uses of ALPRs, ALPR systems, and
25 captured plate data;

26 (B) authorized purposes for collecting, accessing,

1 and using captured plate data;

2 (C) the purposes, process, and restrictions
3 related to the sharing or transfer of captured plate
4 data with other law enforcement agencies, government
5 entities, or foreign entities;

6 (D) a description of the measures that will be
7 used to ensure the accuracy of captured plate data and
8 correct data errors;

9 (E) the length of time captured plate data will be
10 retained, including the maximum data retention period
11 for non-hit data and data collected and used as
12 authorized by Sections 10 and 15;

13 (F) a description of the job title or other
14 designation of the employees and independent
15 contractors who are authorized to access and use
16 captured plate data. The policy shall identify the
17 screening and training requirements necessary for
18 those authorized employees and independent
19 contractors;

20 (G) a description of how ALPRs, ALPR systems, and
21 captured plate data will be monitored to ensure the
22 security of the information accessed or used,
23 compliance with all applicable privacy laws, and a
24 process for periodic system audits; and

25 (H) a description of the range of disciplinary
26 actions available for violation of the usage and

1 privacy policies.

2 (3) Adopt, implement, and maintain reasonable security
3 procedures and practices, including operational,
4 administrative, technical, and physical safeguards, to
5 protect captured plate data from unauthorized access,
6 destruction, use, modification, or disclosure, including,
7 but not limited to:

8 (A) safeguards for managing which employees can
9 see the data from its systems, including requiring
10 supervisory approval, robust authentication protocols
11 for establishing an account to access an ALPR system
12 and tracking searches of captured plate data made by
13 employees;

14 (B) requiring data security training and data
15 privacy training for all employees that access
16 captured plate data; and

17 (C) an audit process to ensure that captured plate
18 data obtained through the use of an ALPR or ALPR system
19 is used only for authorized purposes, including audits
20 of requests made by individual law enforcement
21 agencies or government entities.

22 (b) Any ALPR operator that accesses or provides access to
23 captured plate data under this Act shall maintain a record of
24 when captured plate data is accessed that shall include, at a
25 minimum:

26 (1) the date and time the information is accessed;

1 (2) the license plate number or other data elements
2 used to query the ALPR system;

3 (3) the username of the person who accesses the
4 information, and, as applicable, the organization or
5 entity with whom the person is affiliated;

6 (4) the purpose for accessing the information; and

7 (5) the justification for the search, a linked copy of
8 the justification saved and linked to the search query,
9 and whether access was authorized by (i) a case file
10 number, accompanied by a detailed case file or report,
11 (ii) a criminal warrant issued upon a judicial
12 determination of probable cause, and in compliance with
13 the requirements of the Fourth Amendment to the U.S.
14 Constitution and Article I, Section 6 of the Illinois
15 Constitution, or (iii) a written declaration as required
16 under Section 2-130 of the Illinois Vehicle Code.

17 Section 35. Preservation and disclosure.

18 (a) Upon the written request of a law enforcement agency,
19 government entity, or a defendant in a criminal case, a law
20 enforcement agency or government entity that uses, operates,
21 or accesses an ALPR, ALPR system, or captured plate data shall
22 take all necessary steps to preserve specified captured plate
23 data in its possession for 30 days pending the issuance of a
24 court order sought pursuant to subsection (b) if the
25 requesting law enforcement agency, government entity or

1 defendant in a criminal case makes a retention request and
2 specifies in a written, sworn statement:

3 (1) the specific camera or cameras for which captured
4 data must be preserved, or the specific license plate for
5 which captured plate data must be preserved;

6 (2) the date or dates and timeframes for which
7 captured plate data must be preserved; and

8 (3) that a court order for the retention and
9 disclosure of captured plate data will be sought, pursuant
10 to subsection (b), in a court of competent jurisdiction
11 within 5 days of the transmission of the preservation
12 request.

13 (b) A law enforcement agency, government entity or
14 defendant in a criminal case may apply for a court order for
15 the extended retention and disclosure of captured plate data,
16 which shall be issued by any court of competent jurisdiction,
17 if the law enforcement agency, government entity, or defendant
18 in a criminal case offers specific and articulable facts
19 showing there is probable cause to believe that captured plate
20 data is relevant and material to an ongoing felony criminal or
21 missing persons investigation, prosecution, or defense.

22 (c) Captured plate data held by a law enforcement agency
23 or government entity for more than 30 days pursuant to
24 subsection (b) preservation request shall be destroyed within
25 24 hours if:

26 (1) an application for the court order is not made

1 within five days of the preservation request; or

2 (2) the application for the court order made pursuant
3 to subsection (b) is denied.

4 (d) Notice of a data deletion triggering event as
5 enumerated in paragraph (1) or (2) of subsection (c), shall be
6 provided within 24 hours of its occurrence by the person,
7 agency, or entity who made the preservation request authorized
8 by subsection (a) to the recipient of that request.

9 Section 40. Required data collection. Any law enforcement
10 agency or government entity that uses, operates, or accesses
11 ALPRs, ALPR systems, or captured plate data shall, at a
12 minimum, collect information related to following categories
13 for reporting purposes:

14 (1) ALPR and ALPR systems and vendors, including:

15 (A) the total number of ALPRs operated, or otherwise
16 accessed, including the specific number of fixed, mobile
17 and portable devices, and mobile applications;

18 (B) a complete list of all other ALPR systems used,
19 operated, or otherwise accessed;

20 (C) the specific number of ALPRs and ALPR systems
21 owned or leased but not in use at any time during the
22 reporting period and reasons why they were not
23 operational; and

24 (D) a complete list of ALPR related vendors, including
25 the vendor services used and length of the contract term

1 for each vendor.

2 (2) Captured plate data collection and uses, including:

3 (A) the total number of license plates scanned for
4 uses authorized under subsection (c) of Section 10;

5 (B) the total number of manually entered license
6 plates, and the specific number of manually entered
7 license plates for each offense category authorized under
8 subsection (b) of Section 10, and the number of confirmed
9 matches for each category;

10 (C) the total number of arrests directly attributed to
11 ALPR hot list detections authorized under subsection (b)
12 of Section 10 and the specific number by each enumerated
13 category;

14 (D) the total number of convictions directly
15 attributed to ALPR hot list detections authorized under
16 subsection (b) of Section 10 and the specific number by
17 each enumerated category;

18 (E) the total number of license plates scanned for the
19 purposes authorized by subsection (d) of Section 10 and
20 the specific number by each enumerated category;

21 (F) the total number of investigations conducted as
22 authorized under subsection (d) of Section 10 and the
23 specific number by each enumerated category;

24 (G) the total number of investigations that resulted
25 in a finding of unlawful conduct under subsection (d) of
26 Section 10 and the specific number by each enumerated

1 category; and

2 (H) the total number of investigations authorized
3 under paragraph (5) of subsection (d) of Section 10 that
4 resulted in a referral to the Illinois Accountability
5 Commission.

6 (3) Requests for captured plate data, including:

7 (A) the total number of requests received;

8 (B) the total number of requests that resulted in the
9 release of information and the authorization used to
10 release the information;

11 (C) the total number of in-state requests, and for
12 each in-state requester, (i) the specific number of
13 requests that resulted in the release of information, (ii)
14 the authorization used to release the information, and
15 (iii) the name and municipality of the requester;

16 (D) the total number of out-of-state requests, and for
17 each out-of-state requester, (i) the specific number of
18 requests that resulted in a release of information, (ii)
19 the authorization used to release the information, and
20 (iii) the name and state of the requester;

21 (E) the total number of federal requests, and for each
22 federal requester, (i) the specific number of requests
23 that resulted in a release of information, (ii) the
24 authorization used to release the information, and (iii)
25 the name and associated agency of the requester;

26 (F) the total number of valid written declarations

1 entered into as required under subsection (c) of Section
2 2-130 of the Illinois Vehicle Code, and for each written
3 declaration:

4 (i) the name and state of each law enforcement
5 agency that submitted a written declaration;

6 (ii) the length of the sharing authorized under
7 the written declaration and whether sharing is still
8 authorized as of the reporting period; and

9 (iii) whether there have been any instances of
10 non-compliance with the data requirements outlined in
11 Section 2-130 of the Illinois Vehicle Code during the
12 reporting period;

13 (G) the total number and kind of any other data
14 sharing practices or agreements entered into with any
15 other ALPR user, and for each of the data sharing
16 practices or agreements:

17 (i) the name, state, and type of ALPR user;

18 (ii) the authorization for data sharing and
19 whether the agreement allows data sharing only, data
20 receiving only, or data sharing and receiving;

21 (iii) the length of sharing authorized under the
22 data sharing practice or agreement and whether sharing
23 is still authorized as of the reporting period; and

24 (iv) whether there have been any instances of
25 non-compliance with the data sharing practice or
26 agreement during the reporting period;

1 (4) Protections and transparency, including:

2 (A) the number of unauthorized uses of any ALPR, ALPR
3 system, or captured plate data;

4 (B) the number of data breaches of the ALPR system or
5 captured plate data; and

6 (C) a list of internal or external audits that were
7 completed and by whom.

8 Section 45. Reporting.

9 (a) All law enforcement agencies and government entities
10 shall publicly disclose whether they operate, use, or
11 otherwise access an ALPR, ALPR system, or captured plate data
12 on or before April 1 of each year. The reporting requirements
13 under this subsection shall begin on the first April after the
14 effective date of this Act and annually thereafter.

15 (1) Any law enforcement agency or government entity
16 that operates, uses, or otherwise accesses any ALPR system
17 shall report in writing, and publish on its publicly
18 available website, a report that includes the required
19 data collected under Section 40 from February 1 of the
20 previous calendar year through January 31 of the reporting
21 year. The report shall also contain a copy of, or link to,
22 the agency's latest ALPR policy as required under Section
23 30 as of March 1 of the reporting year.

24 (2) Any law enforcement agency or government entity
25 that does not own, operate, or otherwise access an ALPR,

1 ALPR system, or captured plate data shall report in
2 writing, and publish on its publicly available website,
3 that it did not own or use an ALPR, ALPR system, or
4 captured plate data between February 1 of the previous
5 calendar year through January 31 of the reporting year.

6 (b) All law enforcement agencies or government entities
7 shall report to the Secretary of State, and any local body that
8 governs that agency or entity, whether they own, operate, or
9 otherwise access an ALPR, ALPR system, or captured plate data
10 on or before April 1 of each year, beginning after the
11 effective date of this Act.

12 (1) Any law enforcement agency or government entity
13 that owns, operates, or otherwise accesses an ALPR, ALPR
14 system, or captured plate data, shall submit the report
15 required under subsection (a) and certify in writing that
16 it is in compliance with the provisions of this Act.

17 (2) Any law enforcement agency or government entity
18 that does not own or use an ALPR, ALPR system, or captured
19 data shall report in writing that it was not in possession
20 of any ALPR, ALPR system, or captured plate data between
21 February 1 of the previous calendar year through January
22 31 of the reporting year.

23 (c) On or before May 1 of each year, beginning after the
24 effective date of this Act, the Secretary of State shall
25 publish on its publicly available website a report, or link to
26 a report that includes:

1 (1) the total number of ALPRs operated in the State by
2 law enforcement agencies and by governmental entities;

3 (2) the total number of law enforcement agencies and
4 total number of governmental entities that own, operate,
5 or otherwise access ALPR systems or captured plate data
6 between February 1 of the previous calendar year through
7 January 31 of the reporting year, and for each law
8 enforcement agency or government entity, a list, separated
9 by county and municipality:

10 (A) the number and kinds of ALPRs or ALPR systems,
11 including the specific number of fixed, mobile and
12 portable devices, and mobile applications; and

13 (B) the list of vendors, and related services
14 provided by each vendor;

15 (3) the total number of law enforcement agencies with
16 valid written declaration as required under subsection (c)
17 of Section 2-130 of the Illinois Vehicle Code, and for
18 each law enforcement agency:

19 (A) the name and state of the out-of-state law
20 enforcement agencies that submitted a written
21 declaration;

22 (B) the length of the sharing authorized under the
23 written declaration and whether sharing is still
24 authorized, as of the reporting period; and

25 (C) whether there have been any instances of
26 non-compliance with the data requirements outlined in

1 Section 2-130 of the Illinois Vehicle Code by the
2 out-of-state law enforcement agency during the
3 reporting period;

4 (4) the total number and kind of any other data
5 sharing practices or agreements entered into by law
6 enforcement and by governmental entities with any other
7 ALPR user, and for each of those entities:

8 (A) the name, state, and type of ALPR user;

9 (B) the authorization for data sharing and whether
10 the agreement allows data sharing, data receiving or
11 both sharing and receiving;

12 (C) the length of the sharing authorized under the
13 data sharing practice or agreement and whether sharing
14 is still authorized, as of the reporting period; and

15 (D) whether there have been any instances of
16 non-compliance with the data sharing practice or
17 agreement during the reporting period;

18 (5) the total number of requests made to law
19 enforcement agencies, and the number of requests that
20 resulted in the release of information, including the
21 specific number of:

22 (A) in-state requests, and in-state requests that
23 resulted in the release of information;

24 (B) out-of-state requests, and out-of-state
25 requests that resulted in the release of information;
26 and

1 (C) federal requests, and federal requests that
2 resulted in the release of information;

3 (6) the total number of requests made to governmental
4 entities, and the number of requests that resulted in the
5 release of information, including the specific number of:

6 (A) in-state requests and in-state requests that
7 resulted in the release of information;

8 (B) out-of-state requests and out-of-state
9 requests that resulted in the release of information;
10 and

11 (C) federal requests and federal requests that
12 resulted in the release of information;

13 (7) the number of unauthorized uses of any ALPR, ALPR
14 system, or captured plate data;

15 (8) the number of data breaches of the ALPR system or
16 captured plate data;

17 (9) a list of, and a link to, any audits completed by
18 the Secretary of State;

19 (10) a list of law enforcement agencies and a list of
20 government entities that did not own, operate, or
21 otherwise access any ALPR, ALPR system, or captured plate
22 data in the previous calendar year, as reported to the
23 Secretary of State under subsection (b); and

24 (11) a direct link to the publicly available report
25 submitted by each law enforcement agency or government
26 entity as required under subsection (a).

1 Section 50. Admissibility.

2 (a) If a court finds by a preponderance of the evidence
3 that captured plate data was gathered, stored, used, or
4 disclosed in violation of this Act, then that information
5 shall be presumed to be inadmissible in any judicial or
6 administrative proceeding. The State may overcome this
7 presumption by proving the applicability of a judicially
8 recognized exception to the exclusionary rule of the Fourth
9 Amendment to the U.S. Constitution or Article I, Section 6 of
10 the Illinois Constitution, or by a preponderance of the
11 evidence that the individual, partnership, corporation,
12 association, or the law enforcement officer was acting in good
13 faith and reasonably believed that one or more of the
14 exceptions identified in subsection (b), (c), or (d) of
15 Section 10 existed at the time that the captured plate
16 information was gathered, stored, used, or disclosed.

17 (b) No captured plate data and no evidence derived
18 therefrom may be received in evidence in any trial, hearing,
19 or other proceeding in or before any court, grand jury,
20 department, officer, agency, regulatory body, legislative
21 committee, or other authority of the State, or a political
22 subdivision thereof, if the disclosure of that information
23 would be in violation of this Act.

24 Section 55. Privacy.

1 (a) Captured plate data is not considered a public record
2 for the purposes of Section 7 of the Freedom of Information Act
3 and may only be disclosed to the person to whom the vehicle is
4 registered, or with the prior written consent of the person to
5 whom the vehicle is registered.

6 (b) Upon the presentation to an appropriate governmental
7 entity of a valid, outstanding protection order protecting the
8 driver of a vehicle jointly registered with or registered
9 solely in the name of the individual against whom the order was
10 issued, captured plate data may not be disclosed except
11 pursuant to a disclosure order under Section 35 or as the
12 result of a match pursuant to Section 10.

13 Section 60. Penalties.

14 (a) An officer or employee of a law enforcement agency or
15 employee of a government entity, who intentionally fails to
16 perform any act required by this Act is guilty of official
17 misconduct and may be punished in accordance with Section 33-3
18 of the Criminal Code of 2012.

19 (b) The knowing and intentional violation of Section 10,
20 15, 20, 25, 30, 35, 40, or 45 by an officer or employee of any
21 law enforcement agency or employee of a government entity
22 shall constitute a cause for discipline, including termination
23 of employment.

24 (c) Any law enforcement agency or government entity that
25 fails to use, operate, maintain, or access an ALPR, an ALPR

1 system, or captured plate data in full compliance with the
2 requirements set forth in this Act shall trigger a 3-month use
3 prohibition for the first offense and a 6-month use
4 prohibition for each subsequent offense.

5 (d) Any violation of the requirements under this Act made
6 by or the result of the actions or inactions of a vendor shall
7 render the contract null and void and without legal force or
8 effect.

9 Section 65. Private right of action.

10 (a) Notwithstanding any other provision of law, any person
11 who violates the provisions of this Act is subject to legal
12 action for damages, to be brought by any other person claiming
13 that a violation of this Act has injured the person's
14 business, the person, or the person's reputation. A person so
15 injured is entitled to actual damages, including mental pain
16 and suffering endured by the person on account of violation of
17 the provisions of this Act, or liquidated damages, and
18 reasonable attorney's fees, and other costs of litigation.

19 (b) Any person aggrieved by a violation of this Act shall
20 have a right of action in a State circuit court or as a
21 supplemental claim in federal district court against an
22 offending party. A prevailing party may recover for each
23 violation:

24 (1) against any offending party that negligently
25 violates a provision of this Act, liquidated damages of

1 \$1,000 or actual damages, whichever is greater;

2 (2) against any offending party that intentionally or

3 recklessly violates a provision of this Act, liquidated

4 damages of \$5,000 or actual damages, whichever is greater;

5 (3) reasonable attorney's fees and costs, including

6 expert witness fees and other litigation expenses; and

7 (4) other relief, including an injunction, as the

8 State or federal court may deem appropriate.

9 (c) Any law enforcement agency or government entity

10 aggrieved by a vendor's violation of this Act may file suit in

11 any court of competent jurisdiction for injuries sustained as

12 a result of the vendor's violation. Each individual search or

13 share of information constitutes a separate violation. If such

14 violation is found to occur, the court may assess a civil

15 penalty of \$10,000 per violation, injunctive relief, and

16 reasonable attorney's fees and costs. This subsection shall

17 not constitute a limitation on any other private right of

18 action.

19 Section 900. The Freedom of Information Act is amended by

20 changing Section 7 as follows:

21 (5 ILCS 140/7)

22 (Text of Section before amendment by P.A. 104-300)

23 Sec. 7. Exemptions.

24 (1) When a request is made to inspect or copy a public

1 record that contains information that is exempt from
2 disclosure under this Section, but also contains information
3 that is not exempt from disclosure, the public body may elect
4 to redact the information that is exempt. The public body
5 shall make the remaining information available for inspection
6 and copying. Subject to this requirement, the following shall
7 be exempt from inspection and copying:

8 (a) Information specifically prohibited from
9 disclosure by federal or State law or rules and
10 regulations implementing federal or State law.

11 (b) Private information, unless disclosure is required
12 by another provision of this Act, a State or federal law,
13 or a court order.

14 (b-5) Files, documents, and other data or databases
15 maintained by one or more law enforcement agencies and
16 specifically designed to provide information to one or
17 more law enforcement agencies regarding the physical or
18 mental status of one or more individual subjects.

19 (c) Personal information contained within public
20 records, the disclosure of which would constitute a
21 clearly unwarranted invasion of personal privacy, unless
22 the disclosure is consented to in writing by the
23 individual subjects of the information. "Unwarranted
24 invasion of personal privacy" means the disclosure of
25 information that is highly personal or objectionable to a
26 reasonable person and in which the subject's right to

1 privacy outweighs any legitimate public interest in
2 obtaining the information. The disclosure of information
3 that bears on the public duties of public employees and
4 officials shall not be considered an invasion of personal
5 privacy.

6 (d) Records in the possession of any public body
7 created in the course of administrative enforcement
8 proceedings, and any law enforcement or correctional
9 agency for law enforcement purposes, but only to the
10 extent that disclosure would:

11 (i) interfere with pending or actually and
12 reasonably contemplated law enforcement proceedings
13 conducted by any law enforcement or correctional
14 agency that is the recipient of the request;

15 (ii) interfere with active administrative
16 enforcement proceedings conducted by the public body
17 that is the recipient of the request;

18 (iii) create a substantial likelihood that a
19 person will be deprived of a fair trial or an impartial
20 hearing;

21 (iv) unavoidably disclose the identity of a
22 confidential source, confidential information
23 furnished only by the confidential source, or persons
24 who file complaints with or provide information to
25 administrative, investigative, law enforcement, or
26 penal agencies; except that the identities of

1 witnesses to traffic crashes, traffic crash reports,
2 and rescue reports shall be provided by agencies of
3 local government, except when disclosure would
4 interfere with an active criminal investigation
5 conducted by the agency that is the recipient of the
6 request;

7 (v) disclose unique or specialized investigative
8 techniques other than those generally used and known
9 or disclose internal documents of correctional
10 agencies related to detection, observation, or
11 investigation of incidents of crime or misconduct, and
12 disclosure would result in demonstrable harm to the
13 agency or public body that is the recipient of the
14 request;

15 (vi) endanger the life or physical safety of law
16 enforcement personnel or any other person; or

17 (vii) obstruct an ongoing criminal investigation
18 by the agency that is the recipient of the request.

19 (d-5) A law enforcement record created for law
20 enforcement purposes and contained in a shared electronic
21 record management system if the law enforcement agency or
22 criminal justice agency that is the recipient of the
23 request did not create the record, did not participate in
24 or have a role in any of the events which are the subject
25 of the record, and only has access to the record through
26 the shared electronic record management system. As used in

1 this subsection (d-5), "criminal justice agency" means the
2 Illinois Criminal Justice Information Authority or the
3 Illinois Sentencing Policy Advisory Council.

4 (d-6) Records contained in the Officer Professional
5 Conduct Database under Section 9.2 of the Illinois Police
6 Training Act, except to the extent authorized under that
7 Section. This includes the documents supplied to the
8 Illinois Law Enforcement Training Standards Board from the
9 Illinois State Police and Illinois State Police Merit
10 Board.

11 (d-7) Information gathered or records created from the
12 use of automatic license plate readers in connection with
13 Section 2-130 of the Illinois Vehicle Code.

14 (e) Records that relate to or affect the security of
15 correctional institutions and detention facilities.

16 (e-5) Records requested by persons committed to the
17 Department of Corrections, Department of Human Services
18 Division of Mental Health, or a county jail if those
19 materials are available in the library of the correctional
20 institution or facility or jail where the inmate is
21 confined.

22 (e-6) Records requested by persons committed to the
23 Department of Corrections, Department of Human Services
24 Division of Mental Health, or a county jail if those
25 materials include records from staff members' personnel
26 files, staff rosters, or other staffing assignment

1 information.

2 (e-7) Records requested by persons committed to the
3 Department of Corrections or Department of Human Services
4 Division of Mental Health if those materials are available
5 through an administrative request to the Department of
6 Corrections or Department of Human Services Division of
7 Mental Health.

8 (e-8) Records requested by a person committed to the
9 Department of Corrections, Department of Human Services
10 Division of Mental Health, or a county jail, the
11 disclosure of which would result in the risk of harm to any
12 person or the risk of an escape from a jail or correctional
13 institution or facility.

14 (e-9) Records requested by a person in a county jail
15 or committed to the Department of Corrections or
16 Department of Human Services Division of Mental Health,
17 containing personal information pertaining to the person's
18 victim or the victim's family, including, but not limited
19 to, a victim's home address, home telephone number, work
20 or school address, work telephone number, social security
21 number, or any other identifying information, except as
22 may be relevant to a requester's current or potential case
23 or claim.

24 (e-10) Law enforcement records of other persons
25 requested by a person committed to the Department of
26 Corrections, Department of Human Services Division of

1 Mental Health, or a county jail, including, but not
2 limited to, arrest and booking records, mug shots, and
3 crime scene photographs, except as these records may be
4 relevant to the requester's current or potential case or
5 claim.

6 (f) Preliminary drafts, notes, recommendations,
7 memoranda, and other records in which opinions are
8 expressed, or policies or actions are formulated, except
9 that a specific record or relevant portion of a record
10 shall not be exempt when the record is publicly cited and
11 identified by the head of the public body. The exemption
12 provided in this paragraph (f) extends to all those
13 records of officers and agencies of the General Assembly
14 that pertain to the preparation of legislative documents.

15 (g) Trade secrets and commercial or financial
16 information obtained from a person or business where the
17 trade secrets or commercial or financial information are
18 furnished under a claim that they are proprietary,
19 privileged, or confidential, and that disclosure of the
20 trade secrets or commercial or financial information would
21 cause competitive harm to the person or business, and only
22 insofar as the claim directly applies to the records
23 requested.

24 The information included under this exemption includes
25 all trade secrets and commercial or financial information
26 obtained by a public body, including a public pension

1 fund, from a private equity fund or a privately held
2 company within the investment portfolio of a private
3 equity fund as a result of either investing or evaluating
4 a potential investment of public funds in a private equity
5 fund. The exemption contained in this item does not apply
6 to the aggregate financial performance information of a
7 private equity fund, nor to the identity of the fund's
8 managers or general partners. The exemption contained in
9 this item does not apply to the identity of a privately
10 held company within the investment portfolio of a private
11 equity fund, unless the disclosure of the identity of a
12 privately held company may cause competitive harm.

13 Nothing contained in this paragraph (g) shall be
14 construed to prevent a person or business from consenting
15 to disclosure.

16 (h) Proposals and bids for any contract, grant, or
17 agreement, including information which if it were
18 disclosed would frustrate procurement or give an advantage
19 to any person proposing to enter into a contractor
20 agreement with the body, until an award or final selection
21 is made. Information prepared by or for the body in
22 preparation of a bid solicitation shall be exempt until an
23 award or final selection is made.

24 (i) Valuable formulae, computer geographic systems,
25 designs, drawings, and research data obtained or produced
26 by any public body when disclosure could reasonably be

1 expected to produce private gain or public loss. The
2 exemption for "computer geographic systems" provided in
3 this paragraph (i) does not extend to requests made by
4 news media as defined in Section 2 of this Act when the
5 requested information is not otherwise exempt and the only
6 purpose of the request is to access and disseminate
7 information regarding the health, safety, welfare, or
8 legal rights of the general public.

9 (j) The following information pertaining to
10 educational matters:

11 (i) test questions, scoring keys, and other
12 examination data used to administer an academic
13 examination;

14 (ii) information received by a primary or
15 secondary school, college, or university under its
16 procedures for the evaluation of faculty members by
17 their academic peers;

18 (iii) information concerning a school or
19 university's adjudication of student disciplinary
20 cases, but only to the extent that disclosure would
21 unavoidably reveal the identity of the student; and

22 (iv) course materials or research materials used
23 by faculty members.

24 (k) Architects' plans, engineers' technical
25 submissions, and other construction related technical
26 documents for projects not constructed or developed in

1 whole or in part with public funds and the same for
2 projects constructed or developed with public funds,
3 including, but not limited to, power generating and
4 distribution stations and other transmission and
5 distribution facilities, water treatment facilities,
6 airport facilities, sport stadiums, convention centers,
7 and all government owned, operated, or occupied buildings,
8 but only to the extent that disclosure would compromise
9 security.

10 (l) Minutes of meetings of public bodies closed to the
11 public as provided in the Open Meetings Act until the
12 public body makes the minutes available to the public
13 under Section 2.06 of the Open Meetings Act.

14 (m) Communications between a public body and an
15 attorney or auditor representing the public body that
16 would not be subject to discovery in litigation, and
17 materials prepared or compiled by or for a public body in
18 anticipation of a criminal, civil, or administrative
19 proceeding upon the request of an attorney advising the
20 public body, and materials prepared or compiled with
21 respect to internal audits of public bodies.

22 (n) Records relating to a public body's adjudication
23 of employee grievances or disciplinary cases; however,
24 this exemption shall not extend to the final outcome of
25 cases in which discipline is imposed.

26 (o) Administrative or technical information associated

1 with automated data processing operations, including, but
2 not limited to, software, operating protocols, computer
3 program abstracts, file layouts, source listings, object
4 modules, load modules, user guides, documentation
5 pertaining to all logical and physical design of
6 computerized systems, employee manuals, and any other
7 information that, if disclosed, would jeopardize the
8 security of the system or its data or the security of
9 materials exempt under this Section.

10 (p) Records relating to collective negotiating matters
11 between public bodies and their employees or
12 representatives, except that any final contract or
13 agreement shall be subject to inspection and copying.

14 (q) Test questions, scoring keys, and other
15 examination data used to determine the qualifications of
16 an applicant for a license or employment.

17 (r) The records, documents, and information relating
18 to real estate purchase negotiations until those
19 negotiations have been completed or otherwise terminated.
20 With regard to a parcel involved in a pending or actually
21 and reasonably contemplated eminent domain proceeding
22 under the Eminent Domain Act, records, documents, and
23 information relating to that parcel shall be exempt except
24 as may be allowed under discovery rules adopted by the
25 Illinois Supreme Court. The records, documents, and
26 information relating to a real estate sale shall be exempt

1 until a sale is consummated.

2 (s) Any and all proprietary information and records
3 related to the operation of an intergovernmental risk
4 management association or self-insurance pool or jointly
5 self-administered health and accident cooperative or pool.
6 Insurance or self-insurance (including any
7 intergovernmental risk management association or
8 self-insurance pool) claims, loss or risk management
9 information, records, data, advice, or communications.

10 (t) Information contained in or related to
11 examination, operating, or condition reports prepared by,
12 on behalf of, or for the use of a public body responsible
13 for the regulation or supervision of financial
14 institutions, insurance companies, or pharmacy benefit
15 managers, unless disclosure is otherwise required by State
16 law.

17 (u) Information that would disclose or might lead to
18 the disclosure of secret or confidential information,
19 codes, algorithms, programs, or private keys intended to
20 be used to create electronic signatures under the Uniform
21 Electronic Transactions Act.

22 (v) Vulnerability assessments, security measures, and
23 response policies or plans that are designed to identify,
24 prevent, or respond to potential attacks upon a
25 community's population or systems, facilities, or
26 installations, but only to the extent that disclosure

1 could reasonably be expected to expose the vulnerability
2 or jeopardize the effectiveness of the measures, policies,
3 or plans, or the safety of the personnel who implement
4 them or the public. Information exempt under this item may
5 include such things as details pertaining to the
6 mobilization or deployment of personnel or equipment, to
7 the operation of communication systems or protocols, to
8 cybersecurity vulnerabilities, or to tactical operations.

9 (w) (Blank).

10 (x) Maps and other records regarding the location or
11 security of generation, transmission, distribution,
12 storage, gathering, treatment, or switching facilities
13 owned by a utility, by a power generator, or by the
14 Illinois Power Agency.

15 (y) Information contained in or related to proposals,
16 bids, or negotiations related to electric power
17 procurement under Section 1-75 of the Illinois Power
18 Agency Act and Section 16-111.5 of the Public Utilities
19 Act that is determined to be confidential and proprietary
20 by the Illinois Power Agency or by the Illinois Commerce
21 Commission.

22 (z) Information about students exempted from
23 disclosure under Section 10-20.38 or 34-18.29 of the
24 School Code, and information about undergraduate students
25 enrolled at an institution of higher education exempted
26 from disclosure under Section 25 of the Illinois Credit

1 Card Marketing Act of 2009.

2 (aa) Information the disclosure of which is exempted
3 under the Viatical Settlements Act of 2009.

4 (bb) Records and information provided to a mortality
5 review team and records maintained by a mortality review
6 team appointed under the Department of Juvenile Justice
7 Mortality Review Team Act.

8 (cc) Information regarding interments, entombments, or
9 inurnments of human remains that are submitted to the
10 Cemetery Oversight Database under the Cemetery Care Act or
11 the Cemetery Oversight Act, whichever is applicable.

12 (dd) Correspondence and records (i) that may not be
13 disclosed under Section 11-9 of the Illinois Public Aid
14 Code or (ii) that pertain to appeals under Section 11-8 of
15 the Illinois Public Aid Code.

16 (ee) The names, addresses, or other personal
17 information of persons who are minors and are also
18 participants and registrants in programs of park
19 districts, forest preserve districts, conservation
20 districts, recreation agencies, and special recreation
21 associations.

22 (ff) The names, addresses, or other personal
23 information of participants and registrants in programs of
24 park districts, forest preserve districts, conservation
25 districts, recreation agencies, and special recreation
26 associations where such programs are targeted primarily to

1 minors.

2 (gg) Confidential information described in Section
3 1-100 of the Illinois Independent Tax Tribunal Act of
4 2012.

5 (hh) The report submitted to the State Board of
6 Education by the School Security and Standards Task Force
7 under item (8) of subsection (d) of Section 2-3.160 of the
8 School Code and any information contained in that report.

9 (ii) Records requested by persons committed to or
10 detained by the Department of Human Services under the
11 Sexually Violent Persons Commitment Act or committed to
12 the Department of Corrections under the Sexually Dangerous
13 Persons Act if those materials: (i) are available in the
14 library of the facility where the individual is confined;
15 (ii) include records from staff members' personnel files,
16 staff rosters, or other staffing assignment information;
17 or (iii) are available through an administrative request
18 to the Department of Human Services or the Department of
19 Corrections.

20 (jj) Confidential information described in Section
21 5-535 of the Civil Administrative Code of Illinois.

22 (kk) The public body's credit card numbers, debit card
23 numbers, bank account numbers, Federal Employer
24 Identification Number, security code numbers, passwords,
25 and similar account information, the disclosure of which
26 could result in identity theft or impersonation or defrauding

1 of a governmental entity or a person.

2 (ll) Records concerning the work of the threat
3 assessment team of a school district, including, but not
4 limited to, any threat assessment procedure under the
5 School Safety Drill Act and any information contained in
6 the procedure.

7 (mm) Information prohibited from being disclosed under
8 subsections (a) and (b) of Section 15 of the Student
9 Confidential Reporting Act.

10 (nn) Proprietary information submitted to the
11 Environmental Protection Agency under the Drug Take-Back
12 Act.

13 (oo) Records described in subsection (f) of Section
14 3-5-1 of the Unified Code of Corrections.

15 (pp) Any and all information regarding burials,
16 interments, or entombments of human remains as required to
17 be reported to the Department of Natural Resources
18 pursuant either to the Archaeological and Paleontological
19 Resources Protection Act or the Human Remains Protection
20 Act.

21 (qq) Reports described in subsection (e) of Section
22 16-15 of the Abortion Care Clinical Training Program Act.

23 (rr) Information obtained by a certified local health
24 department under the Access to Public Health Data Act.

25 (ss) For a request directed to a public body that is
26 also a HIPAA-covered entity, all information that is

1 protected health information, including demographic
2 information, that may be contained within or extracted
3 from any record held by the public body in compliance with
4 State and federal medical privacy laws and regulations,
5 including, but not limited to, the Health Insurance
6 Portability and Accountability Act and its regulations, 45
7 CFR Parts 160 and 164. As used in this paragraph,
8 "HIPAA-covered entity" has the meaning given to the term
9 "covered entity" in 45 CFR 160.103 and "protected health
10 information" has the meaning given to that term in 45 CFR
11 160.103.

12 (tt) Proposals or bids submitted by engineering
13 consultants in response to requests for proposal or other
14 competitive bidding requests by the Department of
15 Transportation or the Illinois Toll Highway Authority.

16 (uu) Documents that, pursuant to the State of
17 Illinois' 1987 Agreement with the U.S. Nuclear Regulatory
18 Commission and the corresponding requirement to maintain
19 compatibility with the National Materials Program, have
20 been determined to be security sensitive. These documents
21 include information classified as safeguards,
22 safeguards-modified, and sensitive unclassified
23 nonsafeguards information, as identified in U.S. Nuclear
24 Regulatory Commission regulatory information summaries,
25 security advisories, and other applicable communications
26 or regulations related to the control and distribution of

1 security sensitive information.

2 (vv) Any captured plate data under the Automated
3 License Plate Recognition System Act.

4 (1.5) Any information exempt from disclosure under the
5 Judicial Privacy Act shall be redacted from public records
6 prior to disclosure under this Act.

7 (1.6) Any information exempt from disclosure under the
8 Public Official Safety and Privacy Act shall be redacted from
9 public records prior to disclosure under this Act.

10 (1.7) Any information exempt from disclosure under
11 paragraph (3.5) of Section 9-15 of the Election Code shall be
12 redacted from public records prior to disclosure under this
13 Act.

14 (2) A public record that is not in the possession of a
15 public body but is in the possession of a party with whom the
16 agency has contracted to perform a governmental function on
17 behalf of the public body, and that directly relates to the
18 governmental function and is not otherwise exempt under this
19 Act, shall be considered a public record of the public body,
20 for purposes of this Act.

21 (3) This Section does not authorize withholding of
22 information or limit the availability of records to the
23 public, except as stated in this Section or otherwise provided
24 in this Act.

25 (Source: P.A. 103-154, eff. 6-30-23; 103-423, eff. 1-1-24;
26 103-446, eff. 8-4-23; 103-462, eff. 8-4-23; 103-540, eff.

1 1-1-24; 103-554, eff. 1-1-24; 103-605, eff. 7-1-24; 103-865,
2 eff. 1-1-25; 104-438, eff. 1-1-26; 104-443, eff. 1-1-26;
3 revised 1-7-26.)

4 (Text of Section after amendment by P.A. 104-300)

5 Sec. 7. Exemptions.

6 (1) When a request is made to inspect or copy a public
7 record that contains information that is exempt from
8 disclosure under this Section, but also contains information
9 that is not exempt from disclosure, the public body may elect
10 to redact the information that is exempt. The public body
11 shall make the remaining information available for inspection
12 and copying. Subject to this requirement, the following shall
13 be exempt from inspection and copying:

14 (a) Records created or compiled by a State public
15 defender agency or commission subject to the State Public
16 Defender Act that contain: individual client identity;
17 individual case file information; individual investigation
18 records and other records that are otherwise subject to
19 attorney-client privilege; records that would not be
20 discoverable in litigation; records under Section 2.15;
21 training materials; records related to attorney
22 consultation and representation strategy; or any of the
23 above concerning clients of county public defenders or
24 other defender agencies and firms. This exclusion does not
25 apply to deidentified, aggregated, administrative records,

1 such as general case processing and workload information.

2 (a-5) Information specifically prohibited from
3 disclosure by federal or State law or rules and
4 regulations implementing federal or State law.

5 (b) Private information, unless disclosure is required
6 by another provision of this Act, a State or federal law,
7 or a court order.

8 (b-5) Files, documents, and other data or databases
9 maintained by one or more law enforcement agencies and
10 specifically designed to provide information to one or
11 more law enforcement agencies regarding the physical or
12 mental status of one or more individual subjects.

13 (c) Personal information contained within public
14 records, the disclosure of which would constitute a
15 clearly unwarranted invasion of personal privacy, unless
16 the disclosure is consented to in writing by the
17 individual subjects of the information. "Unwarranted
18 invasion of personal privacy" means the disclosure of
19 information that is highly personal or objectionable to a
20 reasonable person and in which the subject's right to
21 privacy outweighs any legitimate public interest in
22 obtaining the information. The disclosure of information
23 that bears on the public duties of public employees and
24 officials shall not be considered an invasion of personal
25 privacy.

26 (d) Records in the possession of any public body

1 created in the course of administrative enforcement
2 proceedings, and any law enforcement or correctional
3 agency for law enforcement purposes, but only to the
4 extent that disclosure would:

5 (i) interfere with pending or actually and
6 reasonably contemplated law enforcement proceedings
7 conducted by any law enforcement or correctional
8 agency that is the recipient of the request;

9 (ii) interfere with active administrative
10 enforcement proceedings conducted by the public body
11 that is the recipient of the request;

12 (iii) create a substantial likelihood that a
13 person will be deprived of a fair trial or an impartial
14 hearing;

15 (iv) unavoidably disclose the identity of a
16 confidential source, confidential information
17 furnished only by the confidential source, or persons
18 who file complaints with or provide information to
19 administrative, investigative, law enforcement, or
20 penal agencies; except that the identities of
21 witnesses to traffic crashes, traffic crash reports,
22 and rescue reports shall be provided by agencies of
23 local government, except when disclosure would
24 interfere with an active criminal investigation
25 conducted by the agency that is the recipient of the
26 request;

1 (v) disclose unique or specialized investigative
2 techniques other than those generally used and known
3 or disclose internal documents of correctional
4 agencies related to detection, observation, or
5 investigation of incidents of crime or misconduct, and
6 disclosure would result in demonstrable harm to the
7 agency or public body that is the recipient of the
8 request;

9 (vi) endanger the life or physical safety of law
10 enforcement personnel or any other person; or

11 (vii) obstruct an ongoing criminal investigation
12 by the agency that is the recipient of the request.

13 (d-5) A law enforcement record created for law
14 enforcement purposes and contained in a shared electronic
15 record management system if the law enforcement agency or
16 criminal justice agency that is the recipient of the
17 request did not create the record, did not participate in
18 or have a role in any of the events which are the subject
19 of the record, and only has access to the record through
20 the shared electronic record management system. As used in
21 this subsection (d-5), "criminal justice agency" means the
22 Illinois Criminal Justice Information Authority or the
23 Illinois Sentencing Policy Advisory Council.

24 (d-6) Records contained in the Officer Professional
25 Conduct Database under Section 9.2 of the Illinois Police
26 Training Act, except to the extent authorized under that

1 Section. This includes the documents supplied to the
2 Illinois Law Enforcement Training Standards Board from the
3 Illinois State Police and Illinois State Police Merit
4 Board.

5 (d-7) Information gathered or records created from the
6 use of automatic license plate readers in connection with
7 Section 2-130 of the Illinois Vehicle Code.

8 (e) Records that relate to or affect the security of
9 correctional institutions and detention facilities.

10 (e-5) Records requested by persons committed to the
11 Department of Corrections, Department of Human Services
12 Division of Mental Health, or a county jail if those
13 materials are available in the library of the correctional
14 institution or facility or jail where the inmate is
15 confined.

16 (e-6) Records requested by persons committed to the
17 Department of Corrections, Department of Human Services
18 Division of Mental Health, or a county jail if those
19 materials include records from staff members' personnel
20 files, staff rosters, or other staffing assignment
21 information.

22 (e-7) Records requested by persons committed to the
23 Department of Corrections or Department of Human Services
24 Division of Mental Health if those materials are available
25 through an administrative request to the Department of
26 Corrections or Department of Human Services Division of

1 Mental Health.

2 (e-8) Records requested by a person committed to the
3 Department of Corrections, Department of Human Services
4 Division of Mental Health, or a county jail, the
5 disclosure of which would result in the risk of harm to any
6 person or the risk of an escape from a jail or correctional
7 institution or facility.

8 (e-9) Records requested by a person in a county jail
9 or committed to the Department of Corrections or
10 Department of Human Services Division of Mental Health,
11 containing personal information pertaining to the person's
12 victim or the victim's family, including, but not limited
13 to, a victim's home address, home telephone number, work
14 or school address, work telephone number, social security
15 number, or any other identifying information, except as
16 may be relevant to a requester's current or potential case
17 or claim.

18 (e-10) Law enforcement records of other persons
19 requested by a person committed to the Department of
20 Corrections, Department of Human Services Division of
21 Mental Health, or a county jail, including, but not
22 limited to, arrest and booking records, mug shots, and
23 crime scene photographs, except as these records may be
24 relevant to the requester's current or potential case or
25 claim.

26 (f) Preliminary drafts, notes, recommendations,

1 memoranda, and other records in which opinions are
2 expressed, or policies or actions are formulated, except
3 that a specific record or relevant portion of a record
4 shall not be exempt when the record is publicly cited and
5 identified by the head of the public body. The exemption
6 provided in this paragraph (f) extends to all those
7 records of officers and agencies of the General Assembly
8 that pertain to the preparation of legislative documents.

9 (g) Trade secrets and commercial or financial
10 information obtained from a person or business where the
11 trade secrets or commercial or financial information are
12 furnished under a claim that they are proprietary,
13 privileged, or confidential, and that disclosure of the
14 trade secrets or commercial or financial information would
15 cause competitive harm to the person or business, and only
16 insofar as the claim directly applies to the records
17 requested.

18 The information included under this exemption includes
19 all trade secrets and commercial or financial information
20 obtained by a public body, including a public pension
21 fund, from a private equity fund or a privately held
22 company within the investment portfolio of a private
23 equity fund as a result of either investing or evaluating
24 a potential investment of public funds in a private equity
25 fund. The exemption contained in this item does not apply
26 to the aggregate financial performance information of a

1 private equity fund, nor to the identity of the fund's
2 managers or general partners. The exemption contained in
3 this item does not apply to the identity of a privately
4 held company within the investment portfolio of a private
5 equity fund, unless the disclosure of the identity of a
6 privately held company may cause competitive harm.

7 Nothing contained in this paragraph (g) shall be
8 construed to prevent a person or business from consenting
9 to disclosure.

10 (h) Proposals and bids for any contract, grant, or
11 agreement, including information which if it were
12 disclosed would frustrate procurement or give an advantage
13 to any person proposing to enter into a contractor
14 agreement with the body, until an award or final selection
15 is made. Information prepared by or for the body in
16 preparation of a bid solicitation shall be exempt until an
17 award or final selection is made.

18 (i) Valuable formulae, computer geographic systems,
19 designs, drawings, and research data obtained or produced
20 by any public body when disclosure could reasonably be
21 expected to produce private gain or public loss. The
22 exemption for "computer geographic systems" provided in
23 this paragraph (i) does not extend to requests made by
24 news media as defined in Section 2 of this Act when the
25 requested information is not otherwise exempt and the only
26 purpose of the request is to access and disseminate

1 information regarding the health, safety, welfare, or
2 legal rights of the general public.

3 (j) The following information pertaining to
4 educational matters:

5 (i) test questions, scoring keys, and other
6 examination data used to administer an academic
7 examination;

8 (ii) information received by a primary or
9 secondary school, college, or university under its
10 procedures for the evaluation of faculty members by
11 their academic peers;

12 (iii) information concerning a school or
13 university's adjudication of student disciplinary
14 cases, but only to the extent that disclosure would
15 unavoidably reveal the identity of the student; and

16 (iv) course materials or research materials used
17 by faculty members.

18 (k) Architects' plans, engineers' technical
19 submissions, and other construction related technical
20 documents for projects not constructed or developed in
21 whole or in part with public funds and the same for
22 projects constructed or developed with public funds,
23 including, but not limited to, power generating and
24 distribution stations and other transmission and
25 distribution facilities, water treatment facilities,
26 airport facilities, sport stadiums, convention centers,

1 and all government owned, operated, or occupied buildings,
2 but only to the extent that disclosure would compromise
3 security.

4 (l) Minutes of meetings of public bodies closed to the
5 public as provided in the Open Meetings Act until the
6 public body makes the minutes available to the public
7 under Section 2.06 of the Open Meetings Act.

8 (m) Communications between a public body and an
9 attorney or auditor representing the public body that
10 would not be subject to discovery in litigation, and
11 materials prepared or compiled by or for a public body in
12 anticipation of a criminal, civil, or administrative
13 proceeding upon the request of an attorney advising the
14 public body, and materials prepared or compiled with
15 respect to internal audits of public bodies.

16 (n) Records relating to a public body's adjudication
17 of employee grievances or disciplinary cases; however,
18 this exemption shall not extend to the final outcome of
19 cases in which discipline is imposed.

20 (o) Administrative or technical information associated
21 with automated data processing operations, including, but
22 not limited to, software, operating protocols, computer
23 program abstracts, file layouts, source listings, object
24 modules, load modules, user guides, documentation
25 pertaining to all logical and physical design of
26 computerized systems, employee manuals, and any other

1 information that, if disclosed, would jeopardize the
2 security of the system or its data or the security of
3 materials exempt under this Section.

4 (p) Records relating to collective negotiating matters
5 between public bodies and their employees or
6 representatives, except that any final contract or
7 agreement shall be subject to inspection and copying.

8 (q) Test questions, scoring keys, and other
9 examination data used to determine the qualifications of
10 an applicant for a license or employment.

11 (r) The records, documents, and information relating
12 to real estate purchase negotiations until those
13 negotiations have been completed or otherwise terminated.
14 With regard to a parcel involved in a pending or actually
15 and reasonably contemplated eminent domain proceeding
16 under the Eminent Domain Act, records, documents, and
17 information relating to that parcel shall be exempt except
18 as may be allowed under discovery rules adopted by the
19 Illinois Supreme Court. The records, documents, and
20 information relating to a real estate sale shall be exempt
21 until a sale is consummated.

22 (s) Any and all proprietary information and records
23 related to the operation of an intergovernmental risk
24 management association or self-insurance pool or jointly
25 self-administered health and accident cooperative or pool.
26 Insurance or self-insurance (including any

1 intergovernmental risk management association or
2 self-insurance pool) claims, loss or risk management
3 information, records, data, advice, or communications.

4 (t) Information contained in or related to
5 examination, operating, or condition reports prepared by,
6 on behalf of, or for the use of a public body responsible
7 for the regulation or supervision of financial
8 institutions, insurance companies, or pharmacy benefit
9 managers, unless disclosure is otherwise required by State
10 law.

11 (u) Information that would disclose or might lead to
12 the disclosure of secret or confidential information,
13 codes, algorithms, programs, or private keys intended to
14 be used to create electronic signatures under the Uniform
15 Electronic Transactions Act.

16 (v) Vulnerability assessments, security measures, and
17 response policies or plans that are designed to identify,
18 prevent, or respond to potential attacks upon a
19 community's population or systems, facilities, or
20 installations, but only to the extent that disclosure
21 could reasonably be expected to expose the vulnerability
22 or jeopardize the effectiveness of the measures, policies,
23 or plans, or the safety of the personnel who implement
24 them or the public. Information exempt under this item may
25 include such things as details pertaining to the
26 mobilization or deployment of personnel or equipment, to

1 the operation of communication systems or protocols, to
2 cybersecurity vulnerabilities, or to tactical operations.

3 (w) (Blank).

4 (x) Maps and other records regarding the location or
5 security of generation, transmission, distribution,
6 storage, gathering, treatment, or switching facilities
7 owned by a utility, by a power generator, or by the
8 Illinois Power Agency.

9 (y) Information contained in or related to proposals,
10 bids, or negotiations related to electric power
11 procurement under Section 1-75 of the Illinois Power
12 Agency Act and Section 16-111.5 of the Public Utilities
13 Act that is determined to be confidential and proprietary
14 by the Illinois Power Agency or by the Illinois Commerce
15 Commission.

16 (z) Information about students exempted from
17 disclosure under Section 10-20.38 or 34-18.29 of the
18 School Code, and information about undergraduate students
19 enrolled at an institution of higher education exempted
20 from disclosure under Section 25 of the Illinois Credit
21 Card Marketing Act of 2009.

22 (aa) Information the disclosure of which is exempted
23 under the Viatical Settlements Act of 2009.

24 (bb) Records and information provided to a mortality
25 review team and records maintained by a mortality review
26 team appointed under the Department of Juvenile Justice

1 Mortality Review Team Act.

2 (cc) Information regarding interments, entombments, or
3 inurnments of human remains that are submitted to the
4 Cemetery Oversight Database under the Cemetery Care Act or
5 the Cemetery Oversight Act, whichever is applicable.

6 (dd) Correspondence and records (i) that may not be
7 disclosed under Section 11-9 of the Illinois Public Aid
8 Code or (ii) that pertain to appeals under Section 11-8 of
9 the Illinois Public Aid Code.

10 (ee) The names, addresses, or other personal
11 information of persons who are minors and are also
12 participants and registrants in programs of park
13 districts, forest preserve districts, conservation
14 districts, recreation agencies, and special recreation
15 associations.

16 (ff) The names, addresses, or other personal
17 information of participants and registrants in programs of
18 park districts, forest preserve districts, conservation
19 districts, recreation agencies, and special recreation
20 associations where such programs are targeted primarily to
21 minors.

22 (gg) Confidential information described in Section
23 1-100 of the Illinois Independent Tax Tribunal Act of
24 2012.

25 (hh) The report submitted to the State Board of
26 Education by the School Security and Standards Task Force

1 under item (8) of subsection (d) of Section 2-3.160 of the
2 School Code and any information contained in that report.

3 (ii) Records requested by persons committed to or
4 detained by the Department of Human Services under the
5 Sexually Violent Persons Commitment Act or committed to
6 the Department of Corrections under the Sexually Dangerous
7 Persons Act if those materials: (i) are available in the
8 library of the facility where the individual is confined;
9 (ii) include records from staff members' personnel files,
10 staff rosters, or other staffing assignment information;
11 or (iii) are available through an administrative request
12 to the Department of Human Services or the Department of
13 Corrections.

14 (jj) Confidential information described in Section
15 5-535 of the Civil Administrative Code of Illinois.

16 (kk) The public body's credit card numbers, debit card
17 numbers, bank account numbers, Federal Employer
18 Identification Number, security code numbers, passwords,
19 and similar account information, the disclosure of which
20 could result in identity theft or impersonation or defrauding
21 of a governmental entity or a person.

22 (ll) Records concerning the work of the threat
23 assessment team of a school district, including, but not
24 limited to, any threat assessment procedure under the
25 School Safety Drill Act and any information contained in
26 the procedure.

1 (mm) Information prohibited from being disclosed under
2 subsections (a) and (b) of Section 15 of the Student
3 Confidential Reporting Act.

4 (nn) Proprietary information submitted to the
5 Environmental Protection Agency under the Drug Take-Back
6 Act.

7 (oo) Records described in subsection (f) of Section
8 3-5-1 of the Unified Code of Corrections.

9 (pp) Any and all information regarding burials,
10 interments, or entombments of human remains as required to
11 be reported to the Department of Natural Resources
12 pursuant either to the Archaeological and Paleontological
13 Resources Protection Act or the Human Remains Protection
14 Act.

15 (qq) Reports described in subsection (e) of Section
16 16-15 of the Abortion Care Clinical Training Program Act.

17 (rr) Information obtained by a certified local health
18 department under the Access to Public Health Data Act.

19 (ss) For a request directed to a public body that is
20 also a HIPAA-covered entity, all information that is
21 protected health information, including demographic
22 information, that may be contained within or extracted
23 from any record held by the public body in compliance with
24 State and federal medical privacy laws and regulations,
25 including, but not limited to, the Health Insurance
26 Portability and Accountability Act and its regulations, 45

1 CFR Parts 160 and 164. As used in this paragraph,
2 "HIPAA-covered entity" has the meaning given to the term
3 "covered entity" in 45 CFR 160.103 and "protected health
4 information" has the meaning given to that term in 45 CFR
5 160.103.

6 (tt) Proposals or bids submitted by engineering
7 consultants in response to requests for proposal or other
8 competitive bidding requests by the Department of
9 Transportation or the Illinois Toll Highway Authority.

10 (uu) Documents that, pursuant to the State of
11 Illinois' 1987 Agreement with the U.S. Nuclear Regulatory
12 Commission and the corresponding requirement to maintain
13 compatibility with the National Materials Program, have
14 been determined to be security sensitive. These documents
15 include information classified as safeguards,
16 safeguards-modified, and sensitive unclassified
17 nonsafeguards information, as identified in U.S. Nuclear
18 Regulatory Commission regulatory information summaries,
19 security advisories, and other applicable communications
20 or regulations related to the control and distribution of
21 security sensitive information.

22 (vv) Any captured plate data under the Automated
23 License Plate Recognition System Act.

24 (1.5) Any information exempt from disclosure under the
25 Judicial Privacy Act shall be redacted from public records
26 prior to disclosure under this Act.

1 (1.6) Any information exempt from disclosure under the
2 Public Official Safety and Privacy Act shall be redacted from
3 public records prior to disclosure under this Act.

4 (1.7) Any information exempt from disclosure under
5 paragraph (3.5) of Section 9-15 of the Election Code shall be
6 redacted from public records prior to disclosure under this
7 Act.

8 (2) A public record that is not in the possession of a
9 public body but is in the possession of a party with whom the
10 agency has contracted to perform a governmental function on
11 behalf of the public body, and that directly relates to the
12 governmental function and is not otherwise exempt under this
13 Act, shall be considered a public record of the public body,
14 for purposes of this Act.

15 (3) This Section does not authorize withholding of
16 information or limit the availability of records to the
17 public, except as stated in this Section or otherwise provided
18 in this Act.

19 (Source: P.A. 103-154, eff. 6-30-23; 103-423, eff. 1-1-24;
20 103-446, eff. 8-4-23; 103-462, eff. 8-4-23; 103-540, eff.
21 1-1-24; 103-554, eff. 1-1-24; 103-605, eff. 7-1-24; 103-865,
22 eff. 1-1-25; 104-300, eff. 1-1-27; 104-438, eff. 1-1-26;
23 104-443, eff. 1-1-26; revised 1-7-26.)

24 Section 995. No acceleration or delay. Where this Act
25 makes changes in a statute that is represented in this Act by

1 text that is not yet or no longer in effect (for example, a
2 Section represented by multiple versions), the use of that
3 text does not accelerate or delay the taking effect of (i) the
4 changes made by this Act or (ii) provisions derived from any
5 other Public Act.

6 Section 997. Severability. The provisions of this Act are
7 severable under Section 1.31 of the Statute on Statutes.

8 Section 999. Effective date. This Act takes effect upon
9 becoming law.