



102ND GENERAL ASSEMBLY

State of Illinois

2021 and 2022

HB5165

Introduced 1/27/2022, by Rep. Lamont J. Robinson, Jr.

SYNOPSIS AS INTRODUCED:

5 ILCS 140/7 from Ch. 116, par. 207
20 ILCS 1370/1-75 new
20 ILCS 1375/5-25
20 ILCS 1375/5-30 new
30 ILCS 500/25-90 new

Amends the Freedom of Information Act. Modifies the exemptions from inspection and copying concerning cybersecurity vulnerabilities. Amends the Department of Innovation and Technology Act. Requires a local government official or employee to be chosen to act as the primary point of contact for local cybersecurity issues. Amends the Illinois Information Security Improvement Act. Requires the Secretary of Innovation and Technology to establish a cybersecurity liaison program to advise and assist units of local government and school districts concerning specified cybersecurity issues. Provides for cybersecurity training for employees of counties, municipalities, and school districts. Amends the Illinois Procurement Code. Provides that State agencies are prohibited from purchasing any products that, due to cybersecurity risks, are prohibited for purchase by federal agencies pursuant to a United States Department of Homeland Security Binding Operational Directive.

LRB102 22762 RJF 31908 b

1 AN ACT concerning cybersecurity.

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

4 Section 5. The Freedom of Information Act is amended by
5 changing Section 7 as follows:

6 (5 ILCS 140/7) (from Ch. 116, par. 207)

7 Sec. 7. Exemptions.

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

16 (a) Information specifically prohibited from
17 disclosure by federal or State law or rules and
18 regulations implementing federal or State law.

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

22 (b-5) Files, documents, and other data or databases
23 maintained by one or more law enforcement agencies and

1 specifically designed to provide information to one or
2 more law enforcement agencies regarding the physical or
3 mental status of one or more individual subjects.

4 (c) Personal information contained within public
5 records, the disclosure of which would constitute a
6 clearly unwarranted invasion of personal privacy, unless
7 the disclosure is consented to in writing by the
8 individual subjects of the information. "Unwarranted
9 invasion of personal privacy" means the disclosure of
10 information that is highly personal or objectionable to a
11 reasonable person and in which the subject's right to
12 privacy outweighs any legitimate public interest in
13 obtaining the information. The disclosure of information
14 that bears on the public duties of public employees and
15 officials shall not be considered an invasion of personal
16 privacy.

17 (d) Records in the possession of any public body
18 created in the course of administrative enforcement
19 proceedings, and any law enforcement or correctional
20 agency for law enforcement purposes, but only to the
21 extent that disclosure would:

22 (i) interfere with pending or actually and
23 reasonably contemplated law enforcement proceedings
24 conducted by any law enforcement or correctional
25 agency that is the recipient of the request;

26 (ii) interfere with active administrative

1 enforcement proceedings conducted by the public body
2 that is the recipient of the request;

3 (iii) create a substantial likelihood that a
4 person will be deprived of a fair trial or an impartial
5 hearing;

6 (iv) unavoidably disclose the identity of a
7 confidential source, confidential information
8 furnished only by the confidential source, or persons
9 who file complaints with or provide information to
10 administrative, investigative, law enforcement, or
11 penal agencies; except that the identities of
12 witnesses to traffic accidents, traffic accident
13 reports, and rescue reports shall be provided by
14 agencies of local government, except when disclosure
15 would interfere with an active criminal investigation
16 conducted by the agency that is the recipient of the
17 request;

18 (v) disclose unique or specialized investigative
19 techniques other than those generally used and known
20 or disclose internal documents of correctional
21 agencies related to detection, observation or
22 investigation of incidents of crime or misconduct, and
23 disclosure would result in demonstrable harm to the
24 agency or public body that is the recipient of the
25 request;

26 (vi) endanger the life or physical safety of law

1 enforcement personnel or any other person; or

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

4 (d-5) A law enforcement record created for law
5 enforcement purposes and contained in a shared electronic
6 record management system if the law enforcement agency
7 that is the recipient of the request did not create the
8 record, did not participate in or have a role in any of the
9 events which are the subject of the record, and only has
10 access to the record through the shared electronic record
11 management system.

12 (d-6) Records contained in the Officer Professional
13 Conduct Database under Section 9.2 ~~9.4~~ of the Illinois
14 Police Training Act, except to the extent authorized under
15 that Section. This includes the documents supplied to the
16 Illinois Law Enforcement Training Standards Board from the
17 Illinois State Police and Illinois State Police Merit
18 Board.

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

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

1 (e-6) Records requested by persons committed to the
2 Department of Corrections, Department of Human Services
3 Division of Mental Health, or a county jail if those
4 materials include records from staff members' personnel
5 files, staff rosters, or other staffing assignment
6 information.

7 (e-7) Records requested by persons committed to the
8 Department of Corrections or Department of Human Services
9 Division of Mental Health if those materials are available
10 through an administrative request to the Department of
11 Corrections or Department of Human Services Division of
12 Mental Health.

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

19 (e-9) Records requested by a person in a county jail
20 or committed to the Department of Corrections or
21 Department of Human Services Division of Mental Health,
22 containing personal information pertaining to the person's
23 victim or the victim's family, including, but not limited
24 to, a victim's home address, home telephone number, work
25 or school address, work telephone number, social security
26 number, or any other identifying information, except as

1 may be relevant to a requester's current or potential case
2 or claim.

3 (e-10) Law enforcement records of other persons
4 requested by a person committed to the Department of
5 Corrections, Department of Human Services Division of
6 Mental Health, or a county jail, including, but not
7 limited to, arrest and booking records, mug shots, and
8 crime scene photographs, except as these records may be
9 relevant to the requester's current or potential case or
10 claim.

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

20 (g) Trade secrets and commercial or financial
21 information obtained from a person or business where the
22 trade secrets or commercial or financial information are
23 furnished under a claim that they are proprietary,
24 privileged, or confidential, and that disclosure of the
25 trade secrets or commercial or financial information would
26 cause competitive harm to the person or business, and only

1 insofar as the claim directly applies to the records
2 requested.

3 The information included under this exemption includes
4 all trade secrets and commercial or financial information
5 obtained by a public body, including a public pension
6 fund, from a private equity fund or a privately held
7 company within the investment portfolio of a private
8 equity fund as a result of either investing or evaluating
9 a potential investment of public funds in a private equity
10 fund. The exemption contained in this item does not apply
11 to the aggregate financial performance information of a
12 private equity fund, nor to the identity of the fund's
13 managers or general partners. The exemption contained in
14 this item does not apply to the identity of a privately
15 held company within the investment portfolio of a private
16 equity fund, unless the disclosure of the identity of a
17 privately held company may cause competitive harm.

18 Nothing contained in this paragraph (g) shall be
19 construed to prevent a person or business from consenting
20 to disclosure.

21 (h) Proposals and bids for any contract, grant, or
22 agreement, including information which if it were
23 disclosed would frustrate procurement or give an advantage
24 to any person proposing to enter into a contractor
25 agreement with the body, until an award or final selection
26 is made. Information prepared by or for the body in

1 preparation of a bid solicitation shall be exempt until an
2 award or final selection is made.

3 (i) Valuable formulae, computer geographic systems,
4 designs, drawings and research data obtained or produced
5 by any public body when disclosure could reasonably be
6 expected to produce private gain or public loss. The
7 exemption for "computer geographic systems" provided in
8 this paragraph (i) does not extend to requests made by
9 news media as defined in Section 2 of this Act when the
10 requested information is not otherwise exempt and the only
11 purpose of the request is to access and disseminate
12 information regarding the health, safety, welfare, or
13 legal rights of the general public.

14 (j) The following information pertaining to
15 educational matters:

16 (i) test questions, scoring keys and other
17 examination data used to administer an academic
18 examination;

19 (ii) information received by a primary or
20 secondary school, college, or university under its
21 procedures for the evaluation of faculty members by
22 their academic peers;

23 (iii) information concerning a school or
24 university's adjudication of student disciplinary
25 cases, but only to the extent that disclosure would
26 unavoidably reveal the identity of the student; and

1 (iv) course materials or research materials used
2 by faculty members.

3 (k) Architects' plans, engineers' technical
4 submissions, and other construction related technical
5 documents for projects not constructed or developed in
6 whole or in part with public funds and the same for
7 projects constructed or developed with public funds,
8 including, but not limited to, power generating and
9 distribution stations and other transmission and
10 distribution facilities, water treatment facilities,
11 airport facilities, sport stadiums, convention centers,
12 and all government owned, operated, or occupied buildings,
13 but only to the extent that disclosure would compromise
14 security.

15 (l) Minutes of meetings of public bodies closed to the
16 public as provided in the Open Meetings Act until the
17 public body makes the minutes available to the public
18 under Section 2.06 of the Open Meetings Act.

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

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

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

15 (p) Records relating to collective negotiating matters
16 between public bodies and their employees or
17 representatives, except that any final contract or
18 agreement shall be subject to inspection and copying.

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

22 (r) The records, documents, and information relating
23 to real estate purchase negotiations until those
24 negotiations have been completed or otherwise terminated.
25 With regard to a parcel involved in a pending or actually
26 and reasonably contemplated eminent domain proceeding

1 under the Eminent Domain Act, records, documents, and
2 information relating to that parcel shall be exempt except
3 as may be allowed under discovery rules adopted by the
4 Illinois Supreme Court. The records, documents, and
5 information relating to a real estate sale shall be exempt
6 until a sale is consummated.

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

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

22 (u) Information that would disclose or might lead to
23 the disclosure of secret or confidential information,
24 codes, algorithms, programs, or private keys intended to
25 be used to create electronic signatures under the Uniform
26 Electronic Transactions Act.

1 (v) Vulnerability assessments, security measures, and
2 response policies or plans that are designed to identify,
3 prevent, or respond to potential attacks upon a
4 community's population or systems, facilities, or
5 installations, ~~the destruction or contamination of which~~
6 ~~would constitute a clear and present danger to the health~~
7 ~~or safety of the community,~~ but only to the extent that
8 disclosure could reasonably be expected to expose the
9 vulnerability or jeopardize the effectiveness of the
10 measures, policies, or plans, or the safety of the
11 personnel who implement them or the public. Information
12 exempt under this item may include such things as details
13 pertaining to the mobilization or deployment of personnel
14 or equipment, to the operation of communication systems or
15 protocols, to cybersecurity vulnerabilities, or to
16 tactical operations.

17 (w) (Blank).

18 (x) Maps and other records regarding the location or
19 security of generation, transmission, distribution,
20 storage, gathering, treatment, or switching facilities
21 owned by a utility, by a power generator, or by the
22 Illinois Power Agency.

23 (y) Information contained in or related to proposals,
24 bids, or negotiations related to electric power
25 procurement under Section 1-75 of the Illinois Power
26 Agency Act and Section 16-111.5 of the Public Utilities

1 Act that is determined to be confidential and proprietary
2 by the Illinois Power Agency or by the Illinois Commerce
3 Commission.

4 (z) Information about students exempted from
5 disclosure under Sections 10-20.38 or 34-18.29 of the
6 School Code, and information about undergraduate students
7 enrolled at an institution of higher education exempted
8 from disclosure under Section 25 of the Illinois Credit
9 Card Marketing Act of 2009.

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

12 (bb) Records and information provided to a mortality
13 review team and records maintained by a mortality review
14 team appointed under the Department of Juvenile Justice
15 Mortality Review Team Act.

16 (cc) Information regarding interments, entombments, or
17 inurnments of human remains that are submitted to the
18 Cemetery Oversight Database under the Cemetery Care Act or
19 the Cemetery Oversight Act, whichever is applicable.

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

24 (ee) The names, addresses, or other personal
25 information of persons who are minors and are also
26 participants and registrants in programs of park

1 districts, forest preserve districts, conservation
2 districts, recreation agencies, and special recreation
3 associations.

4 (ff) The names, addresses, or other personal
5 information of participants and registrants in programs of
6 park districts, forest preserve districts, conservation
7 districts, recreation agencies, and special recreation
8 associations where such programs are targeted primarily to
9 minors.

10 (gg) Confidential information described in Section
11 1-100 of the Illinois Independent Tax Tribunal Act of
12 2012.

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

17 (ii) Records requested by persons committed to or
18 detained by the Department of Human Services under the
19 Sexually Violent Persons Commitment Act or committed to
20 the Department of Corrections under the Sexually Dangerous
21 Persons Act if those materials: (i) are available in the
22 library of the facility where the individual is confined;
23 (ii) include records from staff members' personnel files,
24 staff rosters, or other staffing assignment information;
25 or (iii) are available through an administrative request
26 to the Department of Human Services or the Department of

1 Corrections.

2 (jj) Confidential information described in Section
3 5-535 of the Civil Administrative Code of Illinois.

4 (kk) The public body's credit card numbers, debit card
5 numbers, bank account numbers, Federal Employer
6 Identification Number, security code numbers, passwords,
7 and similar account information, the disclosure of which
8 could result in identity theft or impersonation or defrauding
9 of a governmental entity or a person.

10 (ll) Records concerning the work of the threat
11 assessment team of a school district.

12 (1.5) Any information exempt from disclosure under the
13 Judicial Privacy Act shall be redacted from public records
14 prior to disclosure under this Act.

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

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

26 (Source: P.A. 101-434, eff. 1-1-20; 101-452, eff. 1-1-20;

1 101-455, eff. 8-23-19; 101-652, eff. 1-1-22; 102-38, eff.
2 6-25-21; 102-558, eff. 8-20-21; revised 11-22-21.)

3 Section 10. The Department of Innovation and Technology
4 Act is amended by adding Section 1-75 as follows:

5 (20 ILCS 1370/1-75 new)

6 Sec. 1-75. Local government cybersecurity designee. The
7 principal executive officer, or his or her designee, of each
8 municipality with a population of 35,000 or greater and of
9 each county shall designate a local official or employee as
10 the primary point of contact for local cybersecurity issues.
11 Each jurisdiction must provide the name and contact
12 information of the cybersecurity designee to the Department
13 and update the information as necessary.

14 Section 15. The Illinois Information Security Improvement
15 Act is amended by changing Section 5-25 and by adding Section
16 5-30 as follows:

17 (20 ILCS 1375/5-25)

18 Sec. 5-25. Responsibilities.

19 (a) The Secretary shall:

20 (1) appoint a Statewide Chief Information Security
21 Officer pursuant to Section 5-20;

22 (2) provide the Office with the staffing and resources

1 deemed necessary by the Secretary to fulfill the
2 responsibilities of the Office;

3 (3) oversee statewide information security policies
4 and practices, including:

5 (A) directing and overseeing the development,
6 implementation, and communication of statewide
7 information security policies, standards, and
8 guidelines;

9 (B) overseeing the education of State agency
10 personnel regarding the requirement to identify and
11 provide information security protections commensurate
12 with the risk and magnitude of the harm resulting from
13 the unauthorized access, use, disclosure, disruption,
14 modification, or destruction of information in a
15 critical information system;

16 (C) overseeing the development and implementation
17 of a statewide information security risk management
18 program;

19 (D) overseeing State agency compliance with the
20 requirements of this Section;

21 (E) coordinating Information Security policies and
22 practices with related information and personnel
23 resources management policies and procedures; and

24 (F) providing an effective and efficient process
25 to assist State agencies with complying with the
26 requirements of this Act; ~~and~~

1 (4) subject to appropriation, establish a
2 cybersecurity liaison program to advise and assist units
3 of local government and school districts in identifying
4 cyber threats, performing risk assessments, sharing best
5 practices, and responding to cyber incidents.

6 (b) The Statewide Chief Information Security Officer
7 shall:

8 (1) serve as the head of the Office and ensure the
9 execution of the responsibilities of the Office as set
10 forth in subsection (c) of Section 5-15, the Statewide
11 Chief Information Security Officer shall also oversee
12 State agency personnel with significant responsibilities
13 for information security and ensure a competent workforce
14 that keeps pace with the changing information security
15 environment;

16 (2) develop and recommend information security
17 policies, standards, procedures, and guidelines to the
18 Secretary for statewide adoption and monitor compliance
19 with these policies, standards, guidelines, and procedures
20 through periodic testing;

21 (3) develop and maintain risk-based, cost-effective
22 information security programs and control techniques to
23 address all applicable security and compliance
24 requirements throughout the life cycle of State agency
25 information systems;

26 (4) establish the procedures, processes, and

1 technologies to rapidly and effectively identify threats,
2 risks, and vulnerabilities to State information systems,
3 and ensure the prioritization of the remediation of
4 vulnerabilities that pose risk to the State;

5 (5) develop and implement capabilities and procedures
6 for detecting, reporting, and responding to information
7 security incidents;

8 (6) establish and direct a statewide information
9 security risk management program to identify information
10 security risks in State agencies and deploy risk
11 mitigation strategies, processes, and procedures;

12 (7) establish the State's capability to sufficiently
13 protect the security of data through effective information
14 system security planning, secure system development,
15 acquisition, and deployment, the application of protective
16 technologies and information system certification,
17 accreditation, and assessments;

18 (8) ensure that State agency personnel, including
19 contractors, are appropriately screened and receive
20 information security awareness training;

21 (9) convene meetings with agency heads and other State
22 officials to help ensure:

23 (A) the ongoing communication of risk and risk
24 reduction strategies,

25 (B) effective implementation of information
26 security policies and practices, and

1 (C) the incorporation of and compliance with
2 information security policies, standards, and
3 guidelines into the policies and procedures of the
4 agencies;

5 (10) provide operational and technical assistance to
6 State agencies in implementing policies, principles,
7 standards, and guidelines on information security,
8 including implementation of standards promulgated under
9 subparagraph (A) of paragraph (3) of subsection (a) of
10 this Section, and provide assistance and effective and
11 efficient means for State agencies to comply with the
12 State agency requirements under this Act;

13 (11) in coordination and consultation with the
14 Secretary and the Governor's Office of Management and
15 Budget, review State agency budget requests related to
16 Information Security systems and provide recommendations
17 to the Governor's Office of Management and Budget;

18 (12) ensure the preparation and maintenance of plans
19 and procedures to provide cyber resilience and continuity
20 of operations for critical information systems that
21 support the operations of the State; and

22 (13) take such other actions as the Secretary may
23 direct.

24 (Source: P.A. 100-611, eff. 7-20-18; 101-81, eff. 7-12-19.)

25 (20 ILCS 1375/5-30 new)

1 Sec. 5-30. Local government and school district employee
2 cybersecurity training. Every employee of a county,
3 municipality, and school district shall annually complete a
4 cybersecurity training program. The training shall include,
5 but need not be limited to, detecting phishing scams,
6 preventing spyware infections and identity theft, and
7 preventing and responding to data breaches. The Department
8 shall make available to each county, municipality, and school
9 district a training program for employees that complies with
10 the content requirements of this Section. A county,
11 municipality, or school district may create its own
12 cybersecurity training program.

13 Section 20. The Illinois Procurement Code is amended by
14 adding Section 25-90 as follows:

15 (30 ILCS 500/25-90 new)

16 Sec. 25-90. Cybersecurity prohibited products. State
17 agencies are prohibited from purchasing any products that, due
18 to cybersecurity risks, are prohibited for purchase by federal
19 agencies pursuant to a United States Department of Homeland
20 Security Binding Operational Directive.