



101ST GENERAL ASSEMBLY

State of Illinois

2019 and 2020

SB3518

Introduced 2/14/2020, by Sen. Elgie R. Sims, Jr.

SYNOPSIS AS INTRODUCED:

5 ILCS 140/7	from Ch. 116, par. 207
20 ILCS 1370/1-65 new	
20 ILCS 1370/1-70 new	
20 ILCS 1370/1-75 new	
20 ILCS 1375/5-25	
20 ILCS 1375/5-30 new	
30 ILCS 105/5.930 new	
30 ILCS 500/55-25 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. Authorizes the Department of Innovation and Technology to accept grants and donations. Creates the Technology, Education, and Cybersecurity Fund as a special fund in the State treasury to be used by the Department of Innovation and Technology to promote and effectuate information technology activities. 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. Amends the State Finance Act to provide for the Technology, Education, and Cybersecurity Fund.

LRB101 20683 RJF 70347 b

FISCAL NOTE ACT
MAY APPLY

A BILL FOR

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 disclosure
10 under this Section, but also contains information that is not
11 exempt from disclosure, the public body may elect to redact the
12 information that is exempt. The public body shall make the
13 remaining information available for inspection and copying.
14 Subject to this requirement, the following shall be exempt from
15 inspection and copying:

16 (a) Information specifically prohibited from
17 disclosure by federal or State law or rules and regulations
18 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 more
2 law enforcement agencies regarding the physical or mental
3 status of one or more individual subjects.

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

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

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

25 (ii) interfere with active administrative
26 enforcement proceedings conducted by the public body

1 that is the recipient of the request;

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

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

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

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

26 (vii) obstruct an ongoing criminal investigation

1 by the agency that is the recipient of the request.

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

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

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

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

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

1 through an administrative request to the Department of
2 Corrections or Department of Human Services Division of
3 Mental Health.

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

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

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

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

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

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

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

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

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

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

1 purpose of the request is to access and disseminate
2 information regarding the health, safety, welfare, or
3 legal rights of the general public.

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

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

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

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

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

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

1 airport facilities, sport stadiums, convention centers,
2 and all government owned, operated, or occupied buildings,
3 but only to the extent that disclosure would compromise
4 security.

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

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

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

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

1 computerized systems, employee manuals, and any other
2 information that, if disclosed, would jeopardize the
3 security of the system or its data or the security of
4 materials exempt under this Section.

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

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

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

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

1 Insurance or self insurance (including any
2 intergovernmental risk management association or self
3 insurance pool) claims, loss or risk management
4 information, records, data, advice or communications.

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

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

17 (v) Vulnerability assessments, security measures, and
18 response policies or plans that are designed to identify,
19 prevent, or respond to potential attacks upon a community's
20 population or systems, facilities, or installations, ~~the~~
21 ~~destruction or contamination of which would constitute a~~
22 ~~clear and present danger to the health or safety of the~~
23 ~~community,~~ but only to the extent that disclosure could
24 reasonably be expected to expose the vulnerability or
25 jeopardize the effectiveness of the measures, policies, or
26 plans, or the safety of the personnel who implement them or

1 the public. Information exempt under this item may include
2 such things as details pertaining to the mobilization or
3 deployment of personnel or equipment, to the operation of
4 communication systems or protocols, to cybersecurity
5 vulnerabilities, or to tactical operations.

6 (w) (Blank).

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

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

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

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

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

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

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

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

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

25 (gg) Confidential information described in Section
26 1-100 of the Illinois Independent Tax Tribunal Act of 2012.

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

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

16 (jj) Confidential information described in Section
17 5-535 of the Civil Administrative Code of Illinois.

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

24 (ll) ~~(kk)~~ Records concerning the work of the threat
25 assessment team of a school district.

26 (1.5) Any information exempt from disclosure under the

1 Judicial Privacy Act shall be redacted from public records
2 prior to disclosure under this Act.

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

10 (3) This Section does not authorize withholding of
11 information or limit the availability of records to the public,
12 except as stated in this Section or otherwise provided in this
13 Act.

14 (Source: P.A. 100-26, eff. 8-4-17; 100-201, eff. 8-18-17;
15 100-732, eff. 8-3-18; 101-434, eff. 1-1-20; 101-452, eff.
16 1-1-20; 101-455, eff. 8-23-19; revised 9-27-19.)

17 Section 10. The Department of Innovation and Technology Act
18 is amended by adding Sections 1-65, 1-70, and 1-75 as follows:

19 (20 ILCS 1370/1-65 new)

20 Sec. 1-65. Technology, Education, and Cybersecurity Fund.
21 The Technology, Education, and Cybersecurity Fund is hereby
22 created as a special fund in the State treasury, and may be
23 used by the Department, subject to appropriation, to promote
24 and effectuate information technology activities.

1 (20 ILCS 1370/1-70 new)

2 Sec. 1-70. Authority to accept grants and donations.

3 (a) The Department may accept offers of services,
4 equipment, supplies, materials, or funds via grant or donation
5 from the federal government, its agencies, or officers, or from
6 any person, firm, or corporation for the purposes of promoting
7 information technology or information technology education.
8 The funds shall be expended by the Department for purposes as
9 indicated by the grantor or donor, or, in the case of funds
10 provided for no specific purpose, for any purpose deemed
11 appropriate by the Secretary in administering the
12 responsibilities of the Department. The Illinois Procurement
13 Code shall not apply to expenditures for activities paid for
14 exclusively by donations or private grants to the Department.

15 (b) Any funds received by the Department from donations
16 shall be deposited in the Technology, Education, and
17 Cybersecurity Fund and used by the Department to promote and
18 effectuate information technology activities.

19 (20 ILCS 1370/1-75 new)

20 Sec. 1-75. Local government cybersecurity designee. The
21 principal executive officer, or his or her designee, of each
22 municipality with a population of 35,000 or greater and of each
23 county shall designate a local official or employee as the
24 primary point of contact for local cybersecurity issues. Each

1 jurisdiction must provide the name and contact information of
2 the cybersecurity designee to the Department and update the
3 information as necessary.

4 Section 15. The Illinois Information Security Improvement
5 Act is amended by changing Section 5-25 and by adding Section
6 5-30 as follows:

7 (20 ILCS 1375/5-25)

8 Sec. 5-25. Responsibilities.

9 (a) The Secretary shall:

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

12 (2) provide the Office with the staffing and resources
13 deemed necessary by the Secretary to fulfill the
14 responsibilities of the Office;

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

17 (A) directing and overseeing the development,
18 implementation, and communication of statewide
19 information security policies, standards, and
20 guidelines;

21 (B) overseeing the education of State agency
22 personnel regarding the requirement to identify and
23 provide information security protections commensurate
24 with the risk and magnitude of the harm resulting from

1 the unauthorized access, use, disclosure, disruption,
2 modification, or destruction of information in a
3 critical information system;

4 (C) overseeing the development and implementation
5 of a statewide information security risk management
6 program;

7 (D) overseeing State agency compliance with the
8 requirements of this Section;

9 (E) coordinating Information Security policies and
10 practices with related information and personnel
11 resources management policies and procedures; and

12 (F) providing an effective and efficient process
13 to assist State agencies with complying with the
14 requirements of this Act; ~~and-~~

15 (4) subject to appropriation, establish a
16 cybersecurity liaison program to advise and assist units of
17 local government and school districts in identifying cyber
18 threats, performing risk assessments, sharing best
19 practices, and responding to cyber incidents.

20 (b) The Statewide Chief Information Security Officer
21 shall:

22 (1) serve as the head of the Office and ensure the
23 execution of the responsibilities of the Office as set
24 forth in subsection (c) of Section 5-15, the Statewide
25 Chief Information Security Officer shall also oversee
26 State agency personnel with significant responsibilities

1 for information security and ensure a competent workforce
2 that keeps pace with the changing information security
3 environment;

4 (2) develop and recommend information security
5 policies, standards, procedures, and guidelines to the
6 Secretary for statewide adoption and monitor compliance
7 with these policies, standards, guidelines, and procedures
8 through periodic testing;

9 (3) develop and maintain risk-based, cost-effective
10 information security programs and control techniques to
11 address all applicable security and compliance
12 requirements throughout the life cycle of State agency
13 information systems;

14 (4) establish the procedures, processes, and
15 technologies to rapidly and effectively identify threats,
16 risks, and vulnerabilities to State information systems,
17 and ensure the prioritization of the remediation of
18 vulnerabilities that pose risk to the State;

19 (5) develop and implement capabilities and procedures
20 for detecting, reporting, and responding to information
21 security incidents;

22 (6) establish and direct a statewide information
23 security risk management program to identify information
24 security risks in State agencies and deploy risk mitigation
25 strategies, processes, and procedures;

26 (7) establish the State's capability to sufficiently

1 protect the security of data through effective information
2 system security planning, secure system development,
3 acquisition, and deployment, the application of protective
4 technologies and information system certification,
5 accreditation, and assessments;

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

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

11 (A) the ongoing communication of risk and risk
12 reduction strategies,

13 (B) effective implementation of information
14 security policies and practices, and

15 (C) the incorporation of and compliance with
16 information security policies, standards, and
17 guidelines into the policies and procedures of the
18 agencies;

19 (10) provide operational and technical assistance to
20 State agencies in implementing policies, principles,
21 standards, and guidelines on information security,
22 including implementation of standards promulgated under
23 subparagraph (A) of paragraph (3) of subsection (a) of this
24 Section, and provide assistance and effective and
25 efficient means for State agencies to comply with the State
26 agency requirements under this Act;

1 (11) in coordination and consultation with the
2 Secretary and the Governor's Office of Management and
3 Budget, review State agency budget requests related to
4 Information Security systems and provide recommendations
5 to the Governor's Office of Management and Budget;

6 (12) ensure the preparation and maintenance of plans
7 and procedures to provide cyber resilience and continuity
8 of operations for critical information systems that
9 support the operations of the State; and

10 (13) take such other actions as the Secretary may
11 direct.

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

13 (20 ILCS 1375/5-30 new)

14 Sec. 5-30. Local government and school district employee
15 cybersecurity training. Every employee of a county,
16 municipality, and school district shall annually complete a
17 cybersecurity training program. The training shall include,
18 but need not be limited to, detecting phishing scams,
19 preventing spyware infections and identity theft, and
20 preventing and responding to data breaches. The Department
21 shall make available to each county, municipality, and school
22 district a training program for employees that complies with
23 the content requirements of this Section. A county,
24 municipality, or school district may create its own
25 cybersecurity training program.

1 Section 20. The State Finance Act is amended by adding
2 Section 5.930 as follows:

3 (30 ILCS 105/5.930 new)

4 Sec. 5.930. The Technology, Education, and Cybersecurity
5 Fund.

6 Section 25. The Illinois Procurement Code is amended by
7 adding Section 55-25 as follows:

8 (30 ILCS 500/55-25 new)

9 Sec. 55-25. Cybersecurity prohibited products. State
10 agencies are prohibited from purchasing any products that, due
11 to cybersecurity risks, are prohibited for purchase by federal
12 agencies pursuant to a United States Department of Homeland
13 Security Binding Operational Directive.