SB3939

LRB10222761RJF31907b

102ND GENERAL ASSEMBLY

State of Illinois

2021 and 2022

SB3939

Introduced 1/21/2022, by Sen. Elgie R. Sims, 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 22761 RJF 31907 b

A BILL FOR

AN ACT concerning cybersecurity.

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

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

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

Sec. 7. Exemptions.

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

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

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

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

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

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

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

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

(ii) interfere with active administrative

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

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

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

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

(vi) endanger the life or physical safety of law

enforcement personnel or any other person; or

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

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

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

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

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

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

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

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

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

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

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

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

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

insofar as the claim directly applies to the records requested.

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

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

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

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

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

(j) The following information pertaining to educational matters:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(w) (Blank).

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

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

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

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

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

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

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

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

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

districts, forest preserve districts, conservation districts, recreation agencies, and special recreation associations.

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

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

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

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

Corrections.

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

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

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

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

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

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

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

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

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

(20 ILCS 1370/1-75 new)

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

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

(20 ILCS 1375/5-25)

Sec. 5-25. Responsibilities.

(a) The Secretary shall:

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

(2) provide the Office with the staffing and resources

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

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

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

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

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

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

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

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

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

(b) The Statewide Chief Information Security Officer shall:

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

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

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

(4) establish the procedures, processes, and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(20 ILCS 1375/5-30 new)

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

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

(30 ILCS 500/25-90 new)

Sec. 25-90. Cybersecurity prohibited products. 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.