HB1631

LRB104 07727 BDA 17772 b

104TH GENERAL ASSEMBLY

State of Illinois

2025 and 2026

HB1631

Introduced 1/28/2025, by Rep. Abdelnasser Rashid

SYNOPSIS AS INTRODUCED:

20 ILCS 1370/1-5
20 ILCS 1370/1-10
20 ILCS 1370/1-15
20 ILCS 1370/1-25
20 ILCS 1370/1-75 rep.
20 ILCS 1375/5-5
20 ILCS 1375/5-15
20 ILCS 1375/5-25
20 ILCS 1375/5-35 new

Amends the Department of Innovation and Technology Act. Repeals the definition of "client agency" and makes changes in the definitions of "dedicated unit", "State agency", and "transferring agency". Replaces references to "transferring agency" with references to "transferred agency". Makes changes in provisions concerning the powers and duties of the Department of Innovation and Technology, including changes in the scope of services provided by the Department and in the classes of persons to whom those services are to be provided. Authorizes the Department to charge fees for service to all State agencies under the jurisdiction of the Governor (rather than only client agencies). Repeals from the Department of Innovation and Technology Act and adds to the Illinois Information Security Improvement Act a provision requiring the principal executive officer of specified units of local government to designate a local official or employee as the primary point of contact for local cybersecurity issues. Requires the name and contact information for the specified individual to be provided to the Statewide Chief Information Security Officer. Further amends the Illinois Information Security Improvement Act. Makes changes concerning the duties of the Office of the Statewide Chief Information Security Officer and the Secretary of Innovation and Technology. Changes the definition of "State agency".

LRB104 07727 BDA 17772 b

A BILL FOR

AN ACT concerning State government.

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

Section 5. The Department of Innovation and Technology Act is amended by changing Sections 1-5, 1-10, 1-15, and 1-25 as follows:

(20 ILCS 1370/1-5)

Sec. 1-5. Definitions. In this Act:

~~"Client agency" means each transferring agency, or its successor, and any other public agency to which the Department provides service to the extent specified in an interagency agreement with the public agency.~~

"Dedicated unit" means the dedicated bureau, division, office, or other unit within a transferred ~~transferring~~ agency that is responsible for the information technology functions of the transferred ~~transferring~~ agency.

"Department" means the Department of Innovation and Technology.

"Information technology" means technology, infrastructure, equipment, systems, software, networks, and processes used to create, send, receive, and store electronic or digital information, including, without limitation, computer systems and telecommunication services and systems.

"Information technology" shall be construed broadly to incorporate future technologies that change or supplant those in effect as of the effective date of this Act.

"Information technology functions" means the development, procurement, installation, retention, maintenance, operation, possession, storage, and related functions of all information technology.

"Secretary" means the Secretary of Innovation and Technology.

"State agency" means each State agency, department, board, and commission under the jurisdiction of the Governor to which the Department provides services.

"Transferred ~~Transferring~~ agency" means the Department on Aging; the Departments of Agriculture, Central Management Services, Children and Family Services, Commerce and Economic Opportunity, Corrections, Employment Security, Financial and Professional Regulation, Healthcare and Family Services, Human Rights, Human Services, Insurance, Juvenile Justice, Labor, Lottery, Military Affairs, Natural Resources, Public Health, Revenue, Transportation, and Veterans' Affairs; the Illinois State Police; the Capital Development Board; the Deaf and Hard of Hearing Commission; the Environmental Protection Agency; the Governor's Office of Management and Budget; the Guardianship and Advocacy Commission; the Abraham Lincoln Presidential Library and Museum; the Illinois Arts Council; the Illinois Council on Developmental Disabilities; the

Illinois Emergency Management Agency; the Illinois Gaming Board; the Illinois Liquor Control Commission; the Office of the State Fire Marshal; the Prisoner Review Board; and the Department of Early Childhood.

(Source: P.A. 102-376, eff. 1-1-22; 102-538, eff. 8-20-21; 102-813, eff. 5-13-22; 102-870, eff. 1-1-23; 103-588, eff. 6-5-24.)

(20 ILCS 1370/1-10)

Sec. 1-10. Transfer of functions. On and after March 25, 2016 (the effective date of Executive Order 2016-001):

(a) (Blank).

(b) (Blank).

(c) The personnel of each transferred ~~transferring~~ agency designated by the Governor are transferred to the Department. The status and rights of the employees and the State of Illinois or its transferred ~~transferring~~ agencies under the Personnel Code, the Illinois Public Labor Relations Act, and applicable collective bargaining agreements or under any pension, retirement, or annuity plan shall not be affected by this Act. Under the direction of the Governor, the Secretary, in consultation with the transferred ~~transferring~~ agencies and labor organizations representing the affected employees, shall identify each position and employee who is engaged in the performance of functions transferred to the Department, or engaged in the administration of a law the administration of

which is transferred to the Department, to be transferred to the Department. An employee engaged primarily in providing administrative support for information technology functions may be considered engaged in the performance of functions transferred to the Department.

(d) All books, records, papers, documents, property (real and personal), contracts, causes of action, and pending business pertaining to the powers, duties, rights, and responsibilities relating to dedicated units and information technology functions transferred under this Act to the Department, including, but not limited to, material in electronic or magnetic format and necessary computer hardware and software, shall be transferred to the Department.

(e) All unexpended appropriations and balances and other funds available for use relating to dedicated units and information technology functions transferred under this Act shall be transferred for use by the Department at the direction of the Governor. Unexpended balances so transferred shall be expended only for the purpose for which the appropriations were originally made.

(f) The powers, duties, rights, and responsibilities relating to dedicated units and information technology functions transferred by this Act shall be vested in and shall be exercised by the Department.

(g) Whenever reports or notices are now required to be made or given or papers or documents furnished or served by any

person to or upon each dedicated unit in connection with any of the powers, duties, rights, and responsibilities relating to information technology functions transferred by this Act, the same shall be made, given, furnished, or served in the same manner to or upon the Department.

(h) This Act does not affect any act done, ratified, or canceled or any right occurring or established or any action or proceeding had or commenced in an administrative, civil, or criminal cause by each dedicated unit relating to information technology functions before the transfer of responsibilities under this Act; such actions or proceedings may be prosecuted and continued by the Department.

(i) (Blank).

(j) (Blank).

(Source: P.A. 102-376, eff. 1-1-22.)

(20 ILCS 1370/1-15)

Sec. 1-15. Powers and duties.

(a) The head officer of the Department is the Secretary, who shall be the chief information officer for the State and the steward of State data with respect to those <u>transferred</u> agencies under the jurisdiction of the Governor. The Secretary shall be appointed by the Governor, with the advice and consent of the Senate. The Department may employ or retain other persons to assist in the discharge of its functions, subject to the Personnel Code.

(b) The Department shall promote best-in-class innovation and technology to transferred ~~client~~ agencies to foster collaboration among ~~client~~ agencies, empower ~~client~~ agencies to provide better service to residents of Illinois, and maximize the value of taxpayer resources. The Department shall be responsible for information technology functions on behalf of transferred ~~client~~ agencies.

(c) When requested and when in the best interest of the State, the ~~The~~ Department may ~~shall~~ provide for and assist with ~~coordinate~~ information technology for non-transferred State agencies, ~~and, when requested and when in the best interests of the State,~~ for State constitutional offices, units of federal or local governments, and public and not-for-profit institutions of primary, secondary, and higher education, or other parties not associated with State government. The Department shall establish charges for information technology for State agencies, ~~and, when requested,~~ for State constitutional offices, units of federal or local government, and public and not-for-profit institutions of primary, secondary, or higher education and for use by other parties not associated with State government for any services requested or provided. Entities charged for these services shall make payment to the Department. The Department may instruct ~~all~~ State agencies to report their usage of information technology regularly to the Department in the manner the Secretary may prescribe.

(d) The Department shall establish principles ~~develop~~ and ~~implement~~ standards for the protection of~~, policies, and procedures to protect the~~ security and interoperability of State data with respect to State ~~those~~ agencies ~~under the jurisdiction of the Governor~~, including in particular data that are confidential, sensitive, or protected from disclosure by privacy or other laws, while recognizing and balancing the need for collaboration and public transparency.

(e) The Department shall be responsible for providing the Governor with timely, comprehensive, and meaningful information pertinent to the formulation and execution of fiscal policy. In performing this responsibility, the Department shall have the power to do the following:

(1) Control the procurement, retention, installation, maintenance, and operation, as specified by the Department, of information technology equipment used by State ~~client~~ agencies in such a manner as to achieve maximum economy and provide appropriate assistance in the development of information suitable for management analysis.

(2) Establish principles and standards for the implementation of information technology-related reporting by State ~~client~~ agencies and priorities for completion of research by those agencies in accordance with the requirements for management analysis specified by the Department. State agencies shall work with the

Department to follow the principles and standards developed by the Department.

(3) Establish charges for information technology and related services requested by transferred ~~client~~ agencies and rendered by the Department. The Department is likewise empowered to establish prices or charges for all information technology reports purchased by State agencies and governmental entities ~~individuals~~ not connected with State government using the Department's services.

(4) Instruct all State ~~client~~ agencies to report regularly to the Department, in the manner the Department may prescribe, their usage of information technology, the cost incurred, the information produced, and the procedures followed in obtaining the information. All State ~~client~~ agencies shall request from the Department assistance and consultation in securing any necessary information technology to support their requirements.

(5) Examine the accounts and information technology-related data of any organization, body, or agency receiving appropriations from the General Assembly, except for a State constitutional office, the Office of the Executive Inspector General, or any office of the legislative or judicial branches of State government. For a State constitutional office, the Office of the Executive Inspector General, or any office of the legislative or judicial branches of State government, the Department

shall have the power to examine the accounts and information technology-related data of the State constitutional office, the Office of the Executive Inspector General, or any office of the legislative or judicial branches of State government when requested by those offices.

(6) Install and operate a modern information technology system for State agencies using equipment adequate to satisfy the requirements for analysis and review as specified by the Department. Expenditures for information technology and related services rendered shall be reimbursed by the recipients. The reimbursement shall be determined by the Department as amounts sufficient to reimburse the Technology Management Revolving Fund for expenditures incurred in rendering the services.

(f) In addition to the other powers and duties listed in subsection (e), the Department shall analyze the present and future aims, needs, and requirements of information technology, research, and planning for State agencies ~~in order~~ to provide for the formulation of overall policy relative to the use of information technology and related equipment by the State of Illinois. In making this analysis, the Department shall formulate a master plan for information technology, using information technology most advantageously, and advising whether information technology should be leased or purchased by the State. The Department shall prepare and submit interim

reports of meaningful developments and proposals for legislation to the Governor on or before January 30 each year. The Department shall engage in a continuing analysis and evaluation of the master plan so developed, and it shall be the responsibility of the Department to recommend from time to time any needed amendments and modifications of any master plan enacted by the General Assembly.

(g) The Department may make information technology and the use of information technology available to units of local government, elected State officials, State educational institutions, the judicial branch, the legislative branch, and all other governmental units of the State requesting them. The Department shall establish prices and charges for the information technology so furnished and for the use of the information technology. The prices and charges shall be sufficient to reimburse the cost of furnishing the services and use of information technology.

(h) The Department may establish <u>principles and</u> standards to provide consistency in the operation and use of information technology <u>by State agencies</u>. <u>State agencies shall work with the Department to follow the principles and standards developed by the Department.</u>

(i) The Department may adopt rules under the Illinois Administrative Procedure Act necessary to carry out its responsibilities under this Act.

(Source: P.A. 102-376, eff. 1-1-22.)

(20 ILCS 1370/1-25)

Sec. 1-25. Charges for services; non-State funding. The Department may establish charges for services rendered by the Department to State ~~client~~ agencies from funds provided directly to the State ~~client~~ agency by appropriation or otherwise. In establishing charges, the Department shall consult with State ~~client~~ agencies to make charges transparent and clear and seek to minimize or avoid charges for costs for which the Department has other funding sources available.

State ~~Client~~ agencies shall continue to apply for and otherwise seek federal funds and other capital and operational resources for technology for which the agencies are eligible and, subject to compliance with applicable laws, regulations, and grant terms, make those funds available for use by the Department.

(Source: P.A. 102-870, eff. 1-1-23.)

(20 ILCS 1370/1-75 rep.)

Section 10. The Department of Innovation and Technology Act is amended by repealing Section 1-75.

Section 15. The Illinois Information Security Improvement Act is amended by changing Sections 5-5, 5-15, and 5-25 and by adding Section 5-35 as follows:

(20 ILCS 1375/5-5)

Sec. 5-5. Definitions. As used in this Act:

"Critical information system" means any information system (including any telecommunications system) used or operated by a State agency or by a contractor of a State agency or other organization or entity on behalf of a State agency: that contains health insurance information, medical information, or personal information as defined in the Personal Information Protection Act; where the unauthorized disclosure, modification, destruction of information in the information system could be expected to have a serious, severe, or catastrophic adverse effect on State agency operations, assets, or individuals; or where the disruption of access to or use of the information or information system could be expected to have a serious, severe, or catastrophic adverse effect on State operations, assets, or individuals.

"Department" means the Department of Innovation and Technology.

"Information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and

proprietary information; and availability, which means ensuring timely and reliable access to and use of information.

"Incident" means an occurrence that: actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies or standard security practices.

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information created or maintained by or for the State of Illinois.

"Office" means the Office of the Statewide Chief Information Security Officer.

"Secretary" means the Secretary of Innovation and Technology.

"Security controls" means the management, operational, and technical controls (including safeguards and countermeasures) for an information system that protect the confidentiality, integrity, and availability of the system and its information.

"State agency" means any State agency, department, board, and commission under the jurisdiction of the Governor to which the Department provides services.

(Source: P.A. 100-611, eff. 7-20-18.)

(20 ILCS 1375/5-15)

Sec. 5-15. Office of the Statewide Chief Information Security Officer.

(a) The Office of the Statewide Chief Information Security Officer is established within the Department of Innovation and Technology. The Office is directly subordinate to the Secretary of Innovation and Technology.

(b) The Office shall:

(1) serve as the strategic planning, facilitation, and coordination office for information technology security in this State and as the lead and central coordinating entity to guide and oversee the information security functions of State agencies;

(2) provide information security services to support the secure delivery of State agency services that utilize information systems and to assist State agencies with fulfilling their responsibilities under this Act;

(3) conduct information and cybersecurity strategic, operational, and resource planning and facilitating an effective enterprise information security architecture capable of protecting the State;

(4) identify information security risks to each State agency, to third-party providers, and to key supply chain partners, including an assessment of the extent to which information resources or processes are vulnerable to

unauthorized access or harm, including the extent to which the State agency's or contractor's electronically stored information is vulnerable to unauthorized access, use, disclosure, disruption, modification, or destruction, and recommend risk mitigation strategies, methods, and procedures to reduce those risks. These assessments shall also include, but not be limited to, assessments of information systems, computers, printers, software, computer networks, interfaces to computer systems, mobile and peripheral device sensors, and other devices or systems which access the State's network, computer software, and information processing or operational procedures of the State agency or of a contractor of the State agency.

(5) manage the response to information security and information security incidents involving State agency ~~State of Illinois~~ information systems and ensure the completeness of information system security plans for critical information systems;

(6) conduct pre-deployment information security assessments for critical information systems and submit findings and recommendations to the Secretary and State agency heads;

(7) develop and conduct targeted operational evaluations, including threat and vulnerability assessments on State agency information systems;

(8) monitor and report ~~compliance of each~~ State agency's compliance ~~agency~~ with State information security policies, standards, and procedures;

(9) coordinate statewide information security awareness and training programs; and

(10) develop and execute other strategies as necessary to protect State agency's ~~this State's~~ information technology infrastructure and the data stored on or transmitted by such infrastructure.

(c) The Office may temporarily suspend operation of an information system or information technology infrastructure that is owned, leased, outsourced, or shared by one or more State agencies ~~in order~~ to isolate the source of, or stop the spread of, an information security breach or other similar information security incident. State agencies shall comply with directives to temporarily discontinue or suspend operations of information systems or information technology infrastructure.

(Source: P.A. 100-611, eff. 7-20-18.)

(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 for State agencies, 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 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 for State agencies 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 State 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 State 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. 101-81, eff. 7-12-19; 102-753, eff. 1-1-23.)

(20 ILCS 1375/5-35 new)

Sec. 5-35. 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 Statewide Chief Information Security Officer and update the information as necessary.