20 ILCS 1375/5-15

Statutes current with legislation through P.A. 103-585 of the 2024 Regular Session of the 103rd General Assembly.

Illinois Compiled Statutes Annotated > Chapter 20 EXECUTIVE BRANCH (§§ 5/1-1 — 100-90) > DEPARTMENT OF INNOVATION AND TECHNOLOGY (§§ 1370/1-1 — 1375/99-99) > Illinois Information Security Improvement (§§ 1375/5-1 — 1375/99-99)

20 ILCS 1375/5-15 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 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 agency or of a contractor of the agency.

(5) manage the response to information security and information security incidents involving 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 information systems;

(8) monitor and report compliance of each State 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 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.

History

2018 P.A. 100-611, § 5-15, effective July 20, 2018.

End of Document