20 ILCS 1375/5-25

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 1375/5-25 Responsibilities.

(a) The Secretary shall:

(1) appoint a Statewide Chief Information Security Officer pursuant to Section 5-20 [20 ILCS 1375/5-20];

(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 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 [20 ILCS 1375/5-15], 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.

History

2018 P.A. 100-611, § 5-25, effective July 20, 2018; 2019 P.A. 101-81, § 135, effective July 12, 2019; 2022 P.A. 102-753, § 15, effective January 1, 2023.

End of Document