RCW 43.105.450 Office of cybersecurity—State chief information security officer—State agency information technology security. (1) The office of cybersecurity is created within the office of the chief information officer.

(2) The director shall appoint a state chief information security officer, who is the director of the office of cybersecurity.

(3) The primary duties of the office of cybersecurity are:

(a) To establish security standards and policies to protect the state's information technology systems and infrastructure, to provide appropriate governance and application of the standards and policies across information technology resources used by the state, and to ensure the confidentiality, availability, and integrity of the information transacted, stored, or processed in the state's information technology systems and infrastructure;

(b) To develop a centralized cybersecurity protocol for protecting and managing state information technology assets and infrastructure;

(c) To detect and respond to security incidents consistent with information security standards and policies;

(d) To create a model incident response plan for agency adoption, with the office of cybersecurity as the incident response coordinator for incidents that: (i) Impact multiple agencies; (ii) impact more than 10,000 citizens; (iii) involve a nation state actor; or (iv) are likely to be in the public domain;

(e) To ensure the continuity of state business and information resources that support the operations and assets of state agencies in the event of a security incident;

(f) To provide formal guidance to agencies on leading practices and applicable standards to ensure a whole government approach to cybersecurity, which shall include, but not be limited to, guidance regarding: (i) The configuration and architecture of agencies' information technology systems, infrastructure, and assets; (ii) governance, compliance, and oversight; and (iii) incident investigation and response;

(g) To serve as a resource for local and municipal governments in Washington in the area of cybersecurity;

(h) To develop a service catalog of cybersecurity services to be offered to state and local governments;

(i) To collaborate with state agencies in developing standards, functions, and services in order to ensure state agency regulatory environments are understood and considered as part of an enterprise cybersecurity response;

(j) To define core services that must be managed by agency information technology security programs; and

(k) To perform all other matters and things necessary to carry out the purposes of this chapter.

(4) In performing its duties, the office of cybersecurity must address the highest levels of security required to protect confidential information transacted, stored, or processed in the state's information technology systems and infrastructure that is specifically protected from disclosure by state or federal law and for which strict handling requirements are required.

(5) In executing its duties under subsection (3) of this section, the office of cybersecurity shall use or rely upon existing, industry standard, widely adopted cybersecurity standards, with a preference for United States federal standards.

(6) Each state agency, institution of higher education, the legislature, and the judiciary must develop an information technology security program consistent with the office of cybersecurity's standards and policies.

(7)(a) Each state agency information technology security program must adhere to the office of cybersecurity's security standards and policies. Each state agency must review and update its program annually, certify to the office of cybersecurity that its program is in compliance with the office of cybersecurity's security standards and policies, and provide the office of cybersecurity with a list of the agency's cybersecurity business needs and agency program metrics.

(b) The office of cybersecurity shall require a state agency to obtain an independent compliance audit of its information technology security program and controls at least once every three years to determine whether the state agency's information technology security program is in compliance with the standards and policies established by the agency and that security controls identified by the state agency in its security program are operating efficiently.

(c) If a review or an audit conducted under (a) or (b) of this subsection identifies any failure to comply with the standards and policies of the office of cybersecurity or any other material cybersecurity risk, the office of cybersecurity must require the state agency to formulate and implement a plan to resolve the failure or risk. On an annual basis, the office of cybersecurity must provide a confidential report to the governor and appropriate committees of the legislature identifying and describing the cybersecurity risk or failure to comply with the office of cybersecurity's security policy or implementing cybersecurity standards and policies, as well as the agency's plan to resolve such failure or risk. Risks that are not mitigated are to be tracked by the office of cybersecurity and reviewed with the governor and the chair and ranking member of the appropriate committees of the legislature on a quarterly basis.

(d) The reports produced, and information compiled, pursuant to this subsection (7) are confidential and may not be disclosed under chapter 42.56 RCW.

(8) In the case of institutions of higher education, the judiciary, and the legislature, each information technology security program must be comparable to the intended outcomes of the office of cybersecurity's security standards and policies. [2021 c 291 § 1.]