ESSB 6528 - H COMM AMD
By Committee on General Government & Information Technology

ADOPTED 03/03/2016

Strike everything after the enacting clause and insert the following:

"NEW SECTION. **Sec. 1.** (1) Communication and information resources in the various state agencies are strategic and vital assets belonging to the people of Washington and are an important component of maintaining a vibrant economy. Coordinated efforts and a sense of urgency are necessary to protect these assets against unauthorized access, disclosure, use, and modification or destruction, whether accidental or deliberate, as well as to assure the confidentiality, integrity, and availability of information.

(2) State government has a duty to Washington citizens to ensure that the information entrusted to state agencies is safe, secure, and protected from unauthorized access, unauthorized use, or destruction.

(3) Securing the state's communication and information resources is a statewide imperative requiring a coordinated and shared effort from all departments, agencies, and political subdivisions of the state and a long-term commitment to state funding that ensures the success of such efforts.

(4) Risks to communication and information resources must be managed, and the integrity of data and the source, destination, and processes applied to data must be assured.

(5) Information security standards, policies, and guidelines must be adopted and implemented throughout state agencies to ensure the development and maintenance of minimum information security controls to protect communication and information resources that support the operations and assets of those agencies.

(6) Washington state must build upon its existing expertise in information technology including research and development facilities and workforce to become a national leader in cybersecurity.

Sec. 2. RCW 43.105.020 and 2015 3rd sp.s. c 1 s 102 are each reenacted and amended to read as follows:

The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Agency" means the consolidated technology services agency.

(2) "Board" means the technology services board.

(3) "Customer agencies" means all entities that purchase or use information technology resources, telecommunications, or services from the consolidated technology services agency.

(4) "Director" means the state chief information officer, who is the director of the consolidated technology services agency.

(5) "Enterprise architecture" means an ongoing activity for translating business vision and strategy into effective enterprise change. It is a continuous activity. Enterprise architecture creates, communicates, and improves the key principles and models that describe the enterprise's future state and enable its evolution.

(6) "Equipment" means the machines, devices, and transmission facilities used in information processing, including but not limited to computers, terminals, telephones, wireless communications system facilities, cables, and any physical facility necessary for the operation of such equipment.

(7) "Information" includes, but is not limited to, data, text, voice, and video.

(8) "Information security" means the protection of communication and information resources from unauthorized access, use, disclosure, disruption, modification, or destruction in order to:

(a) Prevent improper information modification or destruction;

(b) Preserve authorized restrictions on information access and disclosure;

(c) Ensure timely and reliable access to and use of information; and

(d) Maintain the confidentiality, integrity, and availability of information.

(9) "Information technology" includes, but is not limited to, all electronic technology systems and services, automated information handling, system design and analysis, conversion of data, computer programming, information storage and retrieval, telecommunications, requisite system controls, simulation, electronic commerce, radio technologies, and all related interactions between people and machines.

((~~(9)~~)) (10) "Information technology portfolio" or "portfolio" means a strategic management process documenting relationships

between agency missions and information technology and telecommunications investments.

((~~(10)~~)) (11) "K-20 network" means the network established in RCW 43.41.391.

((~~(11)~~)) (12) "Local governments" includes all municipal and quasi-municipal corporations and political subdivisions, and all agencies of such corporations and subdivisions authorized to contract separately.

((~~(12)~~)) (13) "Office" means the office of the state chief information officer within the consolidated technology services agency.

((~~(13)~~)) (14) "Oversight" means a process of comprehensive risk analysis and management designed to ensure optimum use of information technology resources and telecommunications.

((~~(14)~~)) (15) "Proprietary software" means that software offered for sale or license.

((~~(15)~~)) (16) "Public agency" means any agency of this state or another state; any political subdivision or unit of local government of this state or another state including, but not limited to, municipal corporations, quasi-municipal corporations, special purpose districts, and local service districts; any public benefit nonprofit corporation; any agency of the United States; and any Indian tribe recognized as such by the federal government.

((~~(16)~~)) (17) "Public benefit nonprofit corporation" means a public benefit nonprofit corporation as defined in RCW 24.03.005 that is receiving local, state, or federal funds either directly or through a public agency other than an Indian tribe or political subdivision of another state.

((~~(17)~~)) (18) "Public record" has the definitions in RCW 42.56.010 and chapter 40.14 RCW and includes legislative records and court records that are available for public inspection.

((~~(18)~~)) (19) "Security incident" means an accidental or deliberative event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources.

(20) "State agency" means every state office, department, division, bureau, board, commission, or other state agency, including offices headed by a statewide elected official.

((~~(19)~~)) (21) "Telecommunications" includes, but is not limited to, wireless or wired systems for transport of voice, video, and data communications, network systems, requisite facilities, equipment, system controls, simulation, electronic commerce, and all related interactions between people and machines.

((~~(20)~~)) (22) "Utility-based infrastructure services" includes personal computer and portable device support, servers and server administration, security administration, network administration, telephony, email, and other information technology services commonly used by state agencies.

Sec. 3. RCW 43.105.054 and 2015 3rd sp.s. c 1 s 108 are each amended to read as follows:

(1) The director shall establish standards and policies to govern information technology in the state of Washington.

(2) The office shall have the following powers and duties related to information services:

(a) To develop statewide standards and policies governing the:

(i) Acquisition of equipment, software, and technology-related services;

(ii) Disposition of equipment;

(iii) Licensing of the radio spectrum by or on behalf of state agencies; and

(iv) Confidentiality of computerized data;

(b) To develop statewide and interagency technical policies, standards, and procedures;

(c) To review and approve standards and common specifications for new or expanded telecommunications networks proposed by agencies, public postsecondary education institutions, educational service districts, or statewide or regional providers of K-12 information technology services;

(d) With input from the legislature and the judiciary, ((~~[to]~~)) to provide direction concerning strategic planning goals and objectives for the state;

(e) To establish policies for the periodic review by the director of state agency performance which may include but are not limited to analysis of:

(i) Planning, management, control, and use of information services;

(ii) Training and education;

(iii) Project management; and

(iv) Cybersecurity;

(f) To coordinate with state agencies with an annual information technology expenditure that exceeds ten million dollars to implement a technology business management program to identify opportunities for savings and efficiencies in information technology expenditures and to monitor ongoing financial performance of technology investments; ((~~and~~))

(g) In conjunction with the consolidated technology services agency, to develop statewide standards for agency purchases of technology networking equipment and services;

(h) To implement a process for detecting, reporting, and responding to security incidents consistent with the information security standards, policies, and guidelines adopted by the director;

(i) To develop plans and procedures to ensure the continuity of commerce for information resources that support the operations and assets of state agencies in the event of a security incident; and

(j) To work with the department of commerce and other economic development stakeholders to facilitate the development of a strategy that includes key local, state, and federal assets that will create Washington as a national leader in cybersecurity. The office shall collaborate with, including but not limited to, community colleges, universities, the national guard, the department of defense, the department of energy, and national laboratories to develop the strategy.

(3) Statewide technical standards to promote and facilitate electronic information sharing and access are an essential component of acceptable and reliable public access service and complement content-related standards designed to meet those goals. The office shall:

(a) Establish technical standards to facilitate electronic access to government information and interoperability of information systems, including wireless communications systems; and

(b) Require agencies to include an evaluation of electronic public access needs when planning new information systems or major upgrades of systems.

In developing these standards, the office is encouraged to include the state library, state archives, and appropriate representatives of state and local government.

NEW SECTION. **Sec. 4.** A new section is added to chapter 43.105 RCW to read as follows:

(1) The office must evaluate the extent to which the state is building upon its existing expertise in information technology to become a national leader in cybersecurity, as described in section 1(6) of this act, by periodically evaluating the state's performance in achieving the following objectives:

(a) High levels of compliance with the state's information technology security policy and standards, as demonstrated by the attestation that state agencies make annually to the office in which they report their implementation of best practices identified by the office;

(b) Achieving recognition from the federal government as a leader in cybersecurity, as evidenced by federal dollars received for ongoing efforts or for piloting cybersecurity programs;

(c) Developing future leaders in cybersecurity, as evidenced by an increase in the number of students trained, and cybersecurity programs enlarged in educational settings from a January 1, 2016, baseline;

(d) Broad participation in cybersecurity trainings and exercises or outreach, as evidenced by the number of events and the number of participants;

(e) Full coverage and protection of state information technology assets by a centralized cybersecurity protocol; and

(f) Adherence by state agencies to recovery and resilience plans post cyber attack.

(2) The office is encouraged to collaborate with community colleges, universities, the department of commerce, and other stakeholders in obtaining the information necessary to measure its progress in achieving these objectives.

(3) Before December 1, 2020, the office must report to the legislature:

(a) Its performance in achieving the objectives described in subsection (1) of this section; and

(b) Its recommendations, if any, for additional or different metrics that would improve measurement of the effectiveness of the state's efforts to maintain leadership in cybersecurity.

(4) This section expires October 1, 2021.

NEW SECTION. **Sec. 5.** This act may be known and cited as the cybersecurity jobs act of 2016."

Correct the title.

EFFECT: Establishes performance metrics by which the Office of the Chief Information Officer (OCIO) must periodically measure the state's performance in achieving the Cybersecurity Jobs Act's goal of making Washington a national leader in cybersecurity, and requires the OCIO to report to the Legislature on the state's performance in achieving these metrics and any recommendations for different metrics by December 1, 2020. Provides that the act shall be known and cited as the Cybersecurity Jobs Act of 2016. Reverts reference to Washington technology solutions in definition of "Office" back to the consolidated technology services agency to remain consistent with other statutory references.

--- END ---