S-3640.1

SENATE BILL 5957

State of Washington 68th Legislature 2024 Regular Session

By Senator Boehnke

Prefiled 01/03/24.

AN ACT Relating to requiring the office of privacy and data protection to develop guidelines for the use of artificial intelligence; and amending RCW 43.105.020 and 43.105.369.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

Sec. 1. RCW 43.105.020 and 2023 c 124 s 1 are each 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) "Artificial intelligence" means:

(a) A branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement; or

(b) The capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement.

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

((~~(3)~~)) (4) "Cloud computing" has the same meaning as provided by the special publication 800-145 issued by the national institute of

standards and technology of the United States department of commerce as of September 2011 or its successor publications.

((~~(4)~~)) (5) "Customer agencies" means all entities that purchase or use information technology resources, telecommunications, or services from the consolidated technology services agency.

((~~(5)~~)) (6) "Director" means the state chief information officer, who is the director of the consolidated technology services agency.

((~~(6)~~)) (7) "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.

((~~(7)~~)) (8) "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.

((~~(8)~~)) (9) "Information" includes, but is not limited to, data, text, voice, and video.

((~~(9)~~)) (10) "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.

((~~(10)~~)) (11) "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.

((~~(11)~~)) (12) "Information technology portfolio" or "portfolio" means a strategic management process documenting relationships

between agency missions and information technology and telecommunications investments.

((~~(12)~~)) (13) "K-20 network" means the network established in RCW 43.41.391.

((~~(13)~~)) (14) "Local governments" includes all municipal and quasi-municipal corporations and political subdivisions, and all agencies of such corporations and subdivisions authorized to contract separately.

((~~(14)~~)) (15) "Office" means the office of the state chief information officer within the consolidated technology services agency.

((~~(15)~~)) (16) "Oversight" means a process of comprehensive risk analysis and management designed to ensure optimum use of information technology resources and telecommunications.

((~~(16)~~)) (17) "Proprietary software" means that software offered for sale or license.

((~~(17)~~)) (18) "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.

((~~(18)~~)) (19) "Public benefit nonprofit corporation" means a public benefit nonprofit corporation as defined in RCW 24.03A.245 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.

((~~(19)~~)) (20) "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.

((~~(20)~~)) (21) "Public safety" refers to any entity or services that ensure the welfare and protection of the public.

((~~(21)~~)) (22) "Ransomware" means a type of malware that attempts to deny a user or organization access to data or systems, usually through encryption, until a sum of money or other currency is paid or the user or organization is forced to take a specific action.

((~~(22)~~)) (23) "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.

((~~(23)~~)) (24) "State agency" means every state office, department, division, bureau, board, commission, or other state agency, including offices headed by a statewide elected official.

((~~(24)~~)) (25) "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.

((~~(25)~~)) (26) "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. 2. RCW 43.105.369 and 2016 c 195 s 2 are each amended to read as follows:

(1) The office of privacy and data protection is created within the office of the state chief information officer. The purpose of the office of privacy and data protection is to serve as a central point of contact for state agencies on policy matters involving data privacy and data protection.

(2) The director shall appoint the chief privacy officer, who is the director of the office of privacy and data protection.

(3) The primary duties of the office of privacy and data protection with respect to state agencies are:

(a) To conduct an annual privacy review;

(b) To conduct an annual privacy training for state agencies and employees;

(c) To articulate privacy principles and best practices;

(d) To develop guidelines for the use of artificial intelligence to ensure the ethical, transparent, accountable, and responsible implementation of the technology, and protection of personally identifiable information;

(e) To coordinate data protection in cooperation with the agency; and

((~~(e)~~)) (f) To participate with the office of the state chief information officer in the review of major state agency projects involving personally identifiable information.

(4) The office of privacy and data protection must serve as a resource to local governments and the public on data privacy and protection concerns by:

(a) Developing and promoting the dissemination of best practices for the collection and storage of personally identifiable information, including establishing and conducting a training program or programs for local governments; and

(b) Educating consumers about the use of personally identifiable information on mobile and digital networks and measures that can help protect this information.

(5) By December 1, 2016, and every four years thereafter, the office of privacy and data protection must prepare and submit to the legislature a report evaluating its performance. The office of privacy and data protection must establish performance measures in its 2016 report to the legislature and, in each report thereafter, demonstrate the extent to which performance results have been achieved. These performance measures must include, but are not limited to, the following:

(a) The number of state agencies and employees who have participated in the annual privacy training;

(b) A report on the extent of the office of privacy and data protection's coordination with international and national experts in the fields of data privacy, data protection, and access equity;

(c) A report on the implementation of data protection measures by state agencies attributable in whole or in part to the office of privacy and data protection's coordination of efforts; and

(d) A report on consumer education efforts, including but not limited to the number of consumers educated through public outreach efforts, as indicated by how frequently educational documents were accessed, the office of privacy and data protection's participation in outreach events, and inquiries received back from consumers via telephone or other media.

(6) Within one year of June 9, 2016, the office of privacy and data protection must submit to the joint legislative audit and review committee for review and comment the performance measures developed under subsection (5) of this section and a data collection plan.

(7) The office of privacy and data protection shall submit a report to the legislature on the: (a) Extent to which telecommunications providers in the state are deploying advanced telecommunications capability; and (b) existence of any inequality in

access to advanced telecommunications infrastructure experienced by residents of tribal lands, rural areas, and economically distressed communities. The report may be submitted at a time within the discretion of the office of privacy and data protection, at least once every four years, and only to the extent the office of privacy and data protection is able to gather and present the information within existing resources.

--- END ---