RCW 43.105.291 Technology services board security subcommittee.

(1) The technology services board security subcommittee is created within the board. The membership of the technology services board security subcommittee is comprised of a subset of members appointed to the board, as determined by the chair of the technology services board. The chair may make additional appointments to the technology services board security subcommittee to ensure that relevant technology sectors are represented.

(2) The technology services board security subcommittee has the following powers and duties related to cybersecurity:

(a) Review emergent cyberattacks and threats to critical infrastructure sectors in order to identify existing gaps in state agency cybersecurity policies;

(b) Assess emerging risks to state agency information technology;

(c) Recommend a reporting and information sharing system to notify state agencies of new risks, risk treatment opportunities, and projected shortfalls in response and recovery;

(d) Recommend tabletop cybersecurity exercises, including data breach simulation exercises;

(e) Assist the office of cybersecurity created in RCW 43.105.450 in developing cybersecurity best practice recommendations for state agencies;

(f) Review the proposed policies and standards developed by the office of cybersecurity and recommend their approval to the full board;

(g) Review information relating to cybersecurity incidents and ransomware incidents to determine commonalities and develop best practice recommendations for public agencies; and

(h) Assist the agency and the military department in creating the state of cybersecurity report required in subsection (6) of this section.

(3) In providing staff support to the board, the agency shall work with the national institute of standards and technology and other federal agencies, private sector businesses, and private cybersecurity experts and bring their perspectives and guidance to the board for consideration in fulfilling its duties to ensure a holistic approach to cybersecurity in state government.

(4) To discuss sensitive security topics and information, the technology services board security subcommittee may hold a portion of its agenda in executive session closed to the public.

(5) The technology services board security subcommittee must meet quarterly. The technology services board security subcommittee must hold a joint meeting once a year with the cybersecurity advisory committee created in RCW 38.52.040(4).

(6) By December 1, 2023, and each December 1st thereafter, the military department and the agency are jointly responsible for providing a state of cybersecurity report to the governor and the appropriate committees of the legislature, consistent with RCW 43.01.036, specifying recommendations considered necessary to address cybersecurity in the state. The technology services board security subcommittee shall coordinate the implementation of any recommendations contained in the state of cybersecurity report. The technology services board security subcommittee may identify as confidential, and not subject to public disclosure, those portions of the report as the technology services board security subcommittee

deems necessary to protect the security of public and private cyber systems.

(7) In fulfilling its duties under this section, the agency and the technology services board security subcommittee shall collaborate with the military department and the cybersecurity advisory committee created in RCW 38.52.040(4).

(8) The reports produced and information compiled pursuant to this section are confidential and may not be disclosed under chapter 42.56 RCW. [2023 c 124 s 3.]