RCW 42.56.420 Security. The following information relating to security is exempt from disclosure under this chapter:

(1) Those portions of records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts, which are acts that significantly disrupt the conduct of government or of the general civilian population of the state or the United States and that manifest an extreme indifference to human life, the public disclosure of which would have a substantial likelihood of threatening public safety, consisting of:

(a) Specific and unique vulnerability assessments or specific and unique response or deployment plans, including compiled underlying data collected in preparation of or essential to the assessments, or to the response or deployment plans; and

(b) Records not subject to public disclosure under federal law that are shared by federal or international agencies, and information prepared from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism;

(2) Those portions of records containing specific and unique vulnerability assessments or specific and unique emergency and escape response plans at a city, county, or state adult or juvenile correctional facility, or secure facility for persons civilly confined under chapter 71.09 RCW, the public disclosure of which would have a substantial likelihood of threatening the security of a city, county, or state adult or juvenile correctional facility, secure facility for persons civilly confined under chapter 71.09 RCW, or any individual's safety;

(3) Information compiled by school districts or schools in the development of their comprehensive safe school plans under RCW 28A.320.125, to the extent that they identify specific vulnerabilities of school districts and each individual school;

(4) Information regarding the public and private infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities, and other such information the release of which may increase risk to the confidentiality, integrity, or availability of security, information technology infrastructure, or assets;

(5) The system security and emergency preparedness plan required under RCW 35.21.228, 35A.21.300, 36.01.210, 36.57.120, 36.57A.170, and 81.112.180; and

(6) Personally identifiable information of employees, and other security information, of a private cloud service provider that has entered into a criminal justice information services agreement as contemplated by the United States department of justice criminal justice information services security policy, as authorized by 28 C.F.R. Part 20. [2023 c 404 § 3; 2022 c 140 § 1; 2021 c 26 § 1; 2017 c 149 § 1; 2016 c 153 § 1; 2013 2nd sp.s. c 33 § 9; 2009 c 67 § 1; 2005 c 274 § 422.]

Findings—Intent—2023 c 404: See note following RCW 29A.08.105.

Application—2022 c 140 §§ 1 and 2: See note following RCW 29A.04.260.

Effective date—2022 c 140: See note following RCW 29A.04.260.

Application—2021 c 26: "The exemptions in this act apply to any public records requests made prior to April 14, 2021, for which the disclosure of records has not already occurred." [2021 c 26 § 2.]

Effective date—2021 c 26: "This act is necessary for the immediate preservation of the public peace, health, or safety, or support of the state government and its existing public institutions, and takes effect immediately [April 14, 2021]." [2021 c 26 § 3.]