

## SENATE COMMITTEE SUBSTITUTE

FOR

SENATE BILL NO. 166

AN ACT

To repeal sections 386.480 and 610.021, RSMo, and to enact in lieu thereof two new sections relating to records submitted to the public service commission, with existing penalty provisions.

---

---

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF MISSOURI,  
AS FOLLOWS:

Section A. Sections 386.480 and 610.021, RSMo, are repealed and two new sections enacted in lieu thereof, to be known as sections 386.480 and 610.021, to read as follows:

386.480. 1. No information furnished to the commission by a corporation, person or public utility, except such matters as are specifically required to be open to public inspection by the provisions of this chapter, or chapter 610, shall be open to public inspection or made public except on order of the commission, or by the commission or a commissioner in the course of a hearing or proceeding. The public counsel shall have full and complete access to public service commission files and records, except as limited by this section. Any officer or employee of the commission or the public counsel or any employee of the public counsel who, in violation of the provisions of this section, divulges any such information shall be guilty of a misdemeanor.

2. Records under subdivision (25) of section 610.021 shall not be made available to the public counsel if doing so would

threaten public health or safety, as determined by the commission after consultation with the entity submitting the records.  
However, such records related to critical infrastructure or protected systems may be released to the director of the Missouri Information Analysis Center (MIAC) or his or her designee.

610.021. Except to the extent disclosure is otherwise required by law, a public governmental body is authorized to close meetings, records and votes, to the extent they relate to the following:

(1) Legal actions, causes of action or litigation involving a public governmental body and any confidential or privileged communications between a public governmental body or its representatives and its attorneys. However, any minutes, vote or settlement agreement relating to legal actions, causes of action or litigation involving a public governmental body or any agent or entity representing its interests or acting on its behalf or with its authority, including any insurance company acting on behalf of a public government body as its insured, shall be made public upon final disposition of the matter voted upon or upon the signing by the parties of the settlement agreement, unless, prior to final disposition, the settlement agreement is ordered closed by a court after a written finding that the adverse impact to a plaintiff or plaintiffs to the action clearly outweighs the public policy considerations of section 610.011, however, the amount of any moneys paid by, or on behalf of, the public governmental body shall be disclosed; provided, however, in matters involving the exercise of the power of eminent domain, the vote shall be announced or become public immediately

following the action on the motion to authorize institution of such a legal action. Legal work product shall be considered a closed record;

(2) Leasing, purchase or sale of real estate by a public governmental body where public knowledge of the transaction might adversely affect the legal consideration therefor. However, any minutes, vote or public record approving a contract relating to the leasing, purchase or sale of real estate by a public governmental body shall be made public upon execution of the lease, purchase or sale of the real estate;

(3) Hiring, firing, disciplining or promoting of particular employees by a public governmental body when personal information about the employee is discussed or recorded. However, any vote on a final decision, when taken by a public governmental body, to hire, fire, promote or discipline an employee of a public governmental body shall be made available with a record of how each member voted to the public within seventy-two hours of the close of the meeting where such action occurs; provided, however, that any employee so affected shall be entitled to prompt notice of such decision during the seventy-two-hour period before such decision is made available to the public. As used in this subdivision, the term "personal information" means information relating to the performance or merit of individual employees;

(4) The state militia or national guard or any part thereof;

(5) Nonjudicial mental or physical health proceedings involving identifiable persons, including medical, psychiatric, psychological, or alcoholism or drug dependency diagnosis or

treatment;

(6) Scholastic probation, expulsion, or graduation of identifiable individuals, including records of individual test or examination scores; however, personally identifiable student records maintained by public educational institutions shall be open for inspection by the parents, guardian or other custodian of students under the age of eighteen years and by the parents, guardian or other custodian and the student if the student is over the age of eighteen years;

(7) Testing and examination materials, before the test or examination is given or, if it is to be given again, before so given again;

(8) Welfare cases of identifiable individuals;

(9) Preparation, including any discussions or work product, on behalf of a public governmental body or its representatives for negotiations with employee groups;

(10) Software codes for electronic data processing and documentation thereof;

(11) Specifications for competitive bidding, until either the specifications are officially approved by the public governmental body or the specifications are published for bid;

(12) Sealed bids and related documents, until the bids are opened; and sealed proposals and related documents or any documents related to a negotiated contract until a contract is executed, or all proposals are rejected;

(13) Individually identifiable personnel records, performance ratings or records pertaining to employees or applicants for employment, except that this exemption shall not

apply to the names, positions, salaries and lengths of service of officers and employees of public agencies once they are employed as such, and the names of private sources donating or contributing money to the salary of a chancellor or president at all public colleges and universities in the state of Missouri and the amount of money contributed by the source;

(14) Records which are protected from disclosure by law;

(15) Meetings and public records relating to scientific and technological innovations in which the owner has a proprietary interest;

(16) Records relating to municipal hotlines established for the reporting of abuse and wrongdoing;

(17) Confidential or privileged communications between a public governmental body and its auditor, including all auditor work product; however, all final audit reports issued by the auditor are to be considered open records pursuant to this chapter;

(18) Operational guidelines, policies and specific response plans developed, adopted, or maintained by any public agency responsible for law enforcement, public safety, first response, or public health for use in responding to or preventing any critical incident which is or appears to be terrorist in nature and which has the potential to endanger individual or public safety or health. Financial records related to the procurement of or expenditures relating to operational guidelines, policies or plans purchased with public funds shall be open. When seeking to close information pursuant to this exception, the public governmental body shall affirmatively state in writing that

disclosure would impair the public governmental body's ability to protect the security or safety of persons or real property, and shall in the same writing state that the public interest in nondisclosure outweighs the public interest in disclosure of the records;

(19) Existing or proposed security systems and structural plans of real property owned or leased by a public governmental body, and information that is voluntarily submitted by a nonpublic entity owning or operating an infrastructure to any public governmental body for use by that body to devise plans for protection of that infrastructure, the public disclosure of which would threaten public safety:

(a) Records related to the procurement of or expenditures relating to security systems purchased with public funds shall be open;

(b) When seeking to close information pursuant to this exception, the public governmental body shall affirmatively state in writing that disclosure would impair the public governmental body's ability to protect the security or safety of persons or real property, and shall in the same writing state that the public interest in nondisclosure outweighs the public interest in disclosure of the records;

(c) Records that are voluntarily submitted by a nonpublic entity shall be reviewed by the receiving agency within ninety days of submission to determine if retention of the document is necessary in furtherance of a state security interest. If retention is not necessary, the documents shall be returned to the nonpublic governmental body or destroyed;

(20) The portion of a record that identifies security systems or access codes or authorization codes for security systems of real property;

(21) Records that identify the configuration of components or the operation of a computer, computer system, computer network, or telecommunications network, and would allow unauthorized access to or unlawful disruption of a computer, computer system, computer network, or telecommunications network of a public governmental body. This exception shall not be used to limit or deny access to otherwise public records in a file, document, data file or database containing public records. Records related to the procurement of or expenditures relating to such computer, computer system, computer network, or telecommunications network, including the amount of moneys paid by, or on behalf of, a public governmental body for such computer, computer system, computer network, or telecommunications network shall be open;

(22) Credit card numbers, personal identification numbers, digital certificates, physical and virtual keys, access codes or authorization codes that are used to protect the security of electronic transactions between a public governmental body and a person or entity doing business with a public governmental body. Nothing in this section shall be deemed to close the record of a person or entity using a credit card held in the name of a public governmental body or any record of a transaction made by a person using a credit card or other method of payment for which reimbursement is made by a public governmental body;

(23) Records submitted by an individual, corporation, or

other business entity to a public institution of higher education in connection with a proposal to license intellectual property or perform sponsored research and which contains sales projections or other business plan information the disclosure of which may endanger the competitiveness of a business; [and]

(24) Records relating to foster home or kinship placements of children in foster care under section 210.498; and

(25) (a) Critical infrastructure or protected system records submitted by a person, corporation, public utility, or other entity to the public service commission that are not customarily in the public domain and are related to:

a. Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of that infrastructure or system by either physical or computer based attack or other similar conduct, including the misuse of or unauthorized access to all types of communications and data transmission systems, that threatens public health or safety;

b. The ability of that infrastructure or system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of vulnerabilities, security testing, risk evaluation, risk management planning, or risk audit; or

c. Any planned or past operational problem or solution, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation of that infrastructure or system.

(b) As used in this subdivision, the term "critical infrastructure" means systems and assets, whether physical or



virtual, so vital locally, regionally, or nationally that the incapacity or destruction of such systems and assets would have a debilitating impact on: local, regional, or national security; local, regional, or national economic security; local, regional, or national public health or safety; or, any combination of those matters;

(c) As used in this subdivision, the term "protected system" means:

a. Any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and

b. Includes any physical infrastructure, computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage;.