

# VIRGINIA ACTS OF ASSEMBLY -- 2018 SESSION

## CHAPTER 52

*An Act to amend and reenact § 2.2-3705.2 of the Code of Virginia, relating to the Virginia Freedom of Information Act; exclusions from mandatory disclosure; Rail Fixed Guideway Systems Safety Oversight agency.*

[H 727]

Approved February 28, 2018

**Be it enacted by the General Assembly of Virginia:**

**1. That § 2.2-3705.2 of the Code of Virginia is amended and reenacted as follows:**

**§ 2.2-3705.2. Exclusions to application of chapter; records relating to public safety.**

The following information contained in a public record is excluded from the mandatory disclosure provisions of this chapter but may be disclosed by the custodian in his discretion, except where such disclosure is prohibited by law. Redaction of information excluded under this section from a public record shall be conducted in accordance with § 2.2-3704.01.

1. Confidential information, including victim identity, provided to or obtained by staff in a rape crisis center or a program for battered spouses.

2. Information that describes the design, function, operation, or access control features of any security system, whether manual or automated, which is used to control access to or use of any automated data processing or telecommunications system.

3. Information that would disclose the security aspects of a system safety program plan adopted pursuant to ~~49 C.F.R. Part 659~~ *Federal Transit Administration regulations* by the Commonwealth's designated Rail Fixed Guideway Systems Safety Oversight agency; and information in the possession of such agency, the release of which would jeopardize the success of an ongoing investigation of a rail accident or other incident threatening railway safety.

4. Information concerning security plans and specific assessment components of school safety audits, as provided in § 22.1-279.8.

Nothing in this subdivision shall be construed to prevent the disclosure of information relating to the effectiveness of security plans after (i) any school building or property has been subjected to fire, explosion, natural disaster, or other catastrophic event or (ii) any person on school property has suffered or been threatened with any personal injury.

5. Information concerning the mental health assessment of an individual subject to commitment as a sexually violent predator under Chapter 9 (§ 37.2-900 et seq.) of Title 37.2 held by the Commitment Review Committee; except that in no case shall information identifying the victims of a sexually violent predator be disclosed.

6. Subscriber data provided directly or indirectly by a communications services provider to a public body that operates a 911 or E-911 emergency dispatch system or an emergency notification or reverse 911 system if the data is in a form not made available by the communications services provider to the public generally. Nothing in this subdivision shall prevent the disclosure of subscriber data generated in connection with specific calls to a 911 emergency system, where the requester is seeking to obtain public records about the use of the system in response to a specific crime, emergency or other event as to which a citizen has initiated a 911 call.

For the purposes of this subdivision:

"Communications services provider" means the same as that term is defined in § 58.1-647.

"Subscriber data" means the name, address, telephone number, and any other information identifying a subscriber of a communications services provider.

7. Subscriber data collected by a local governing body in accordance with the Enhanced Public Safety Telephone Services Act (§ 56-484.12 et seq.) and other identifying information of a personal, medical, or financial nature provided to a local governing body in connection with a 911 or E-911 emergency dispatch system or an emergency notification or reverse 911 system if such records are not otherwise publicly available.

Nothing in this subdivision shall prevent the disclosure of subscriber data generated in connection with specific calls to a 911 emergency system, where the requester is seeking to obtain public records about the use of the system in response to a specific crime, emergency or other event as to which a citizen has initiated a 911 call.

For the purposes of this subdivision:

"Communications services provider" means the same as that term is defined in § 58.1-647.

"Subscriber data" means the name, address, telephone number, and any other information identifying a subscriber of a communications services provider.

8. Information held by the Virginia Military Advisory Council or any commission created by

executive order for the purpose of studying and making recommendations regarding preventing closure or realignment of federal military and national security installations and facilities located in Virginia and relocation of such facilities to Virginia, or a local or regional military affairs organization appointed by a local governing body, that would (i) reveal strategies under consideration or development by the Council or such commission or organizations to prevent the closure or realignment of federal military installations located in Virginia or the relocation of national security facilities located in Virginia, to limit the adverse economic effect of such realignment, closure, or relocation, or to seek additional tenant activity growth from the Department of Defense or federal government or (ii) disclose trade secrets, as defined in the Uniform Trade Secrets Act (§ 59.1-336 et seq.), provided to the Council or such commission or organizations in connection with their work.

In order to invoke the trade secret protection provided by clause (ii), the submitting entity shall, in writing and at the time of submission (a) invoke this exclusion, (b) identify with specificity the information for which such protection is sought, and (c) state the reason why such protection is necessary. Nothing in this subdivision shall be construed to prevent the disclosure of all or part of any record, other than a trade secret that has been specifically identified as required by this subdivision, after the Department of Defense or federal agency has issued a final, unappealable decision, or in the event of litigation, a court of competent jurisdiction has entered a final, unappealable order concerning the closure, realignment, or expansion of the military installation or tenant activities, or the relocation of the national security facility, for which records are sought.

9. Information, as determined by the State Comptroller, that describes the design, function, operation, or implementation of internal controls over the Commonwealth's financial processes and systems, and the assessment of risks and vulnerabilities of those controls, including the annual assessment of internal controls mandated by the State Comptroller, if disclosure of such information would jeopardize the security of the Commonwealth's financial assets. However, records relating to the investigation of and findings concerning the soundness of any fiscal process shall be disclosed in a form that does not compromise internal controls. Nothing in this subdivision shall be construed to prohibit the Auditor of Public Accounts or the Joint Legislative Audit and Review Commission from reporting internal control deficiencies discovered during the course of an audit.

10. Information relating to the Statewide Agencies Radio System (STARS) or any other similar local or regional public safety communications system that (i) describes the design, function, programming, operation, or access control features of the overall system, components, structures, individual networks, and subsystems of the STARS or any other similar local or regional communications system or (ii) relates to radio frequencies assigned to or utilized by STARS or any other similar local or regional communications system, code plugs, circuit routing, addressing schemes, talk groups, fleet maps, encryption, or programming maintained by or utilized by STARS or any other similar local or regional public safety communications system.

11. Information concerning a salaried or volunteer Fire/EMS company or Fire/EMS department if disclosure of such information would reveal the telephone numbers for cellular telephones, pagers, or comparable portable communication devices provided to its personnel for use in the performance of their official duties.

12. Information concerning the disaster recovery plans or the evacuation plans in the event of fire, explosion, natural disaster, or other catastrophic event for hospitals and nursing homes regulated by the Board of Health pursuant to Chapter 5 (§ 32.1-123 et seq.) of Title 32.1 provided to the Department of Health. Nothing in this subdivision shall be construed to prevent the disclosure of information relating to the effectiveness of executed evacuation plans after the occurrence of fire, explosion, natural disaster, or other catastrophic event.

13. Records received by the Department of Criminal Justice Services pursuant to §§ 9.1-184, 22.1-79.4, and 22.1-279.8 or for purposes of evaluating threat assessment teams established by a public institution of higher education pursuant to § 23.1-805 or by a private nonprofit institution of higher education, to the extent such records reveal security plans, walk-through checklists, or vulnerability and threat assessment components.

14. Information contained in (i) engineering, architectural, or construction drawings; (ii) operational, procedural, tactical planning, or training manuals; (iii) staff meeting minutes; or (iv) other records that reveal any of the following, the disclosure of which would jeopardize the safety or security of any person; governmental facility, building, or structure or persons using such facility, building, or structure; or public or private commercial office, multifamily residential, or retail building or its occupants:

a. Critical infrastructure information or the location or operation of security equipment and systems of any public building, structure, or information storage facility, including ventilation systems, fire protection equipment, mandatory building emergency equipment or systems, elevators, electrical systems, telecommunications equipment and systems, or utility equipment and systems;

b. Vulnerability assessments, information not lawfully available to the public regarding specific cybersecurity threats or vulnerabilities, or security plans and measures of an entity, facility, building structure, information technology system, or software program;

c. Surveillance techniques, personnel deployments, alarm or security systems or technologies, or

operational or transportation plans or protocols; or

d. Interconnectivity, network monitoring, network operation centers, master sites, or systems related to the Statewide Agencies Radio System (STARS) or any other similar local or regional public safety communications system.

The same categories of records of any person or entity submitted to a public body for the purpose of antiterrorism response planning or cybersecurity planning or protection may be withheld from disclosure if such person or entity in writing (a) invokes the protections of this subdivision, (b) identifies with specificity the records or portions thereof for which protection is sought, and (c) states with reasonable particularity why the protection of such records from public disclosure is necessary to meet the objective of antiterrorism, cybersecurity planning or protection, or critical infrastructure information security and resilience. Such statement shall be a public record and shall be disclosed upon request.

Any public body receiving a request for records excluded under clauses (a) and (b) of this subdivision 14 shall notify the Secretary of Public Safety and Homeland Security or his designee of such request and the response made by the public body in accordance with § 2.2-3704.

Nothing in this subdivision 14 shall prevent the disclosure of records relating to (1) the structural or environmental soundness of any such facility, building, or structure or (2) an inquiry into the performance of such facility, building, or structure after it has been subjected to fire, explosion, natural disaster, or other catastrophic event.

As used in this subdivision, "critical infrastructure information" means the same as that term is defined in 6 U.S.C. § 131.