

VIRGINIA ACTS OF ASSEMBLY — CHAPTER

An Act to amend and reenact § 2.2-3705.2 of the Code of Virginia, relating to the Virginia Freedom of Information Act; record exemption for public safety; cybersecurity.

[S 1129]

Approved

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 records are excluded from the provisions of this chapter but may be disclosed by the custodian in his discretion, except where such disclosure is prohibited by law:

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

2. Those portions of engineering and construction drawings and plans submitted for the sole purpose of complying with the Building Code in obtaining a building permit that would identify specific trade secrets or other information, the disclosure of which would be harmful to the competitive position of the owner or lessee. However, such information shall be exempt only until the building is completed. Information relating to the safety or environmental soundness of any building shall not be exempt from disclosure.

Those portions of engineering and construction drawings and plans that reveal critical structural components, security equipment and systems, ventilation systems, fire protection equipment, mandatory building emergency equipment or systems, elevators, electrical systems, telecommunications equipment and systems, and other utility equipment and systems submitted for the purpose of complying with the Uniform Statewide Building Code (§ 36-97 et seq.) or the Statewide Fire Prevention Code (§ 27-94 et seq.), the disclosure of which would jeopardize the safety or security of any public or private commercial office, multifamily residential or retail building or its occupants in the event of terrorism or other threat to public safety, to the extent that the owner or lessee of such property, equipment or system in writing (i) invokes the protections of this paragraph; (ii) identifies the drawings, plans, or other materials to be protected; and (iii) states the reasons why protection is necessary.

Nothing in this subdivision shall prevent the disclosure of information relating to any building in connection with an inquiry into the performance of that building after it has been subjected to fire, explosion, natural disaster or other catastrophic event.

3. Documentation or other 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.

4. Plans and information to prevent or respond to terrorist activity *or cyber attacks*, the disclosure of which would jeopardize the safety of any person, including (i) critical infrastructure sector or structural components; (ii) vulnerability assessments, operational, procedural, transportation, and tactical planning or training manuals, and staff meeting minutes or other records; ~~and~~ (iii) engineering or architectural records, or records containing information derived from such records, to the extent such records reveal the location or operation of security equipment and systems, elevators, ventilation, fire protection, emergency, electrical, telecommunications or utility equipment and systems of any public building, structure or information storage facility, or telecommunications or utility equipment or systems; *and (iv) 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.* The same categories of records of any ~~governmental or nongovernmental~~ 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 *or cybersecurity* planning or protection. Such statement shall be a public record and shall be disclosed upon request. Nothing in this subdivision shall be construed to prohibit the disclosure of records relating to the structural or environmental soundness of any building, nor shall it prevent the disclosure of information relating to any building in connection with an inquiry into the performance of that building after it has been subjected to fire, explosion, natural disaster or other catastrophic event.

5. Information that would disclose the security aspects of a system safety program plan adopted

ENROLLED

SB1129ER

57 pursuant to 49 C.F.R. Part 659 by the Commonwealth's designated Rail Fixed Guideway Systems Safety
58 Oversight agency; and information in the possession of such agency, the release of which would
59 jeopardize the success of an ongoing investigation of a rail accident or other incident threatening railway
60 safety.

61 6. Engineering and architectural drawings, operational, procedural, tactical planning or training
62 manuals, or staff meeting minutes or other records, the disclosure of which would reveal surveillance
63 techniques, personnel deployments, alarm or security systems or technologies, or operational and
64 transportation plans or protocols, to the extent such disclosure would jeopardize the security of any
65 governmental facility, building or structure or the safety of persons using such facility, building or
66 structure.

67 7. Security plans and specific assessment components of school safety audits, as provided in
68 § 22.1-279.8.

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

73 8. [Expired.]

74 9. Records of the Commitment Review Committee concerning the mental health assessment of an
75 individual subject to commitment as a sexually violent predator under Chapter 9 (§ 37.2-900 et seq.) of
76 Title 37.2; except that in no case shall records identifying the victims of a sexually violent predator be
77 disclosed.

78 10. Subscriber data, which for the purposes of this subdivision, means the name, address, telephone
79 number, and any other information identifying a subscriber of a telecommunications carrier, provided
80 directly or indirectly by a telecommunications carrier to a public body that operates a 911 or E-911
81 emergency dispatch system or an emergency notification or reverse 911 system, if the data is in a form
82 not made available by the telecommunications carrier to the public generally. Nothing in this subdivision
83 shall prevent the release of subscriber data generated in connection with specific calls to a 911
84 emergency system, where the requester is seeking to obtain public records about the use of the system
85 in response to a specific crime, emergency or other event as to which a citizen has initiated a 911 call.

86 11. Subscriber data, which for the purposes of this subdivision, means the name, address, telephone
87 number, and any other information identifying a subscriber of a telecommunications carrier, collected by
88 a local governing body in accordance with the Enhanced Public Safety Telephone Services Act
89 (§ 56-484.12 et seq.), and other identifying information of a personal, medical, or financial nature
90 provided to a local governing body in connection with a 911 or E-911 emergency dispatch system or an
91 emergency notification or reverse 911 system, if such records are not otherwise publicly available.
92 Nothing in this subdivision shall prevent the release of subscriber data generated in connection with
93 specific calls to a 911 emergency system, where the requester is seeking to obtain public records about
94 the use of the system in response to a specific crime, emergency or other event as to which a citizen has
95 initiated a 911 call.

96 12. Records of the Virginia Military Advisory Council or any commission created by executive order
97 for the purpose of studying and making recommendations regarding preventing closure or realignment of
98 federal military and national security installations and facilities located in Virginia and relocation of such
99 facilities to Virginia, or a local or regional military affairs organization appointed by a local governing
100 body, to the extent such records (i) contain information relating to strategies under consideration or
101 development by the Council or such commission or organizations to prevent the closure or realignment
102 of federal military installations located in Virginia or the relocation of national security facilities located
103 in Virginia, to limit the adverse economic effect of such realignment, closure, or relocation, or to seek
104 additional tenant activity growth from the Department of Defense or federal government or (ii) disclose
105 trade secrets, as defined in the Uniform Trade Secrets Act (§ 59.1-336 et seq.), provided to the Council
106 or such commission or organizations in connection with their work. In order to invoke the trade secret
107 protection provided by clause (ii), the submitting entity shall, in writing and at the time of submission
108 (a) invoke this exclusion, (b) identify with specificity the information for which such protection is
109 sought, and (c) state the reason why such protection is necessary. Nothing in this subdivision shall be
110 construed to authorize the withholding of all or part of any record, other than a trade secret that has
111 been specifically identified as required by this subdivision, after the Department of Defense or federal
112 agency has issued a final, unappealable decision, or in the event of litigation, a court of competent
113 jurisdiction has entered a final, unappealable order concerning the closure, realignment, or expansion of
114 the military installation or tenant activities, or the relocation of the national security facility, for which
115 records are sought.

116 13. Documentation or other information as determined by the State Comptroller that describes the
117 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, the disclosure of which 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.

14. Documentation or other 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, programming maintained by or utilized by STARS or any other similar local or regional public safety communications system; those portions of engineering and construction drawings and plans that reveal critical structural components, interconnectivity, security equipment and systems, network monitoring, network operation center, master sites, ventilation systems, fire protection equipment, mandatory building emergency equipment, electrical systems, and other utility equipment and systems related to STARS or any other similar local or regional public safety communications system; and special event plans, operational plans, storm plans, or other pre-arranged programming, the disclosure of which would reveal surveillance techniques, personnel deployments, alarm or security systems or technologies, or operational and transportation plans or protocols, to the extent such disclosure would jeopardize the security of any governmental facility, building, or structure or the safety of any person.

15. Records of a salaried or volunteer Fire/EMS company or Fire/EMS department, to the extent that the records disclose 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.

16. Records of 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, to the extent such records reveal the disaster recovery plans or the evacuation plans for such facilities in the event of fire, explosion, natural disaster, or other catastrophic event. Nothing in this subdivision shall be construed to prohibit the disclosure of records relating to the effectiveness of executed evacuation plans after the occurrence of fire, explosion, natural disaster, or other catastrophic event.

2. That an emergency exists and this act is in force from its passage.