

2-C-19 | SECURITY SYSTEM INFORMATION AND BLUEPRINTS**a. Blueprints**

Section 119.071(3)(b)1., F.S., exempts building plans, blueprints, schematic drawings, and diagrams which depict the internal layout and structural elements of a building, arena, stadium, water treatment facility, or other structure owned or operated by an agency. Exempt information may be disclosed to another governmental entity, to a licensed professional performing work on the structure, or upon a showing of good cause to a court. Section 119.071(3)(b)3., F.S. Exempt documents may also be released in order to comply with competitive bidding requirements. AGO 02-74. However, the entities or persons receiving such information must maintain its exempt status. Id. And see 119.071(3)(e), F.S. (exemption for records which depict structural elements of 911, E911 or public safety radio communications system infrastructure, structures, or facilities owned and operated by an agency; and geographical maps indicating actual or proposed locations of such infrastructure, structures, or facilities).

Section 119.071(3)(c)1., F.S., exempts building plans, blueprints, schematic drawings and diagrams which depict the internal layout or structural elements of various attractions, retail, resort, office, health care facilities, and industrial complexes and developments when the records are held by an agency. The exemption afforded by this statute, however, does not apply to comprehensive plans or site plans, or amendments thereto, which are submitted for approval or which have been approved under local land development regulations, local zoning regulations, or development of regional impact review. Section 119.071(3)(c)4., F.S. And see s. 119.071(3)(d) (information relating to the National Public Safety Broadband Network deemed confidential if disclosure would reveal information set forth in the exemption)

b. Security System Records

Information relating to the security or fire-safety systems for property owned by or leased to the state or any of its political subdivisions is confidential and exempt from disclosure. Section 281.301, F.S. Exempt information includes all records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations,



or consultations or portions thereof relating directly to or revealing such security systems or information. Id.

The exemption extends to information relating to or revealing the security or fire-safety systems for property owned or leased by the state or its political subdivisions, and also to such information concerning privately owned or leased property which is in the possession of an agency. AGOs 01-75 and 93-86, and Inf. Op. to Sherman, July 2, 2018. See also ss. 331.22, F.S. (airport security plans); s. 311.13, F.S. (seaport security plans); and 1004.0962(2), F.S. (campus emergency response of postsecondary education institution).

Section 119.071(3)(a), F.S., provides a similar exemption from disclosure for a security or fire-safety system plan of a private or public entity that is held by an agency. The information may be disclosed to the property owner or leaseholder; in furtherance of the official duties and responsibilities of the agency holding the information; to another local, state or federal agency in furtherance of that agency's official duties and responsibilities; or upon a showing of good cause before a court.

The term "security or fire-safety system plan" includes: records relating directly to the physical security or fire-safety of the facility or revealing security or fire-safety systems; threat assessments conducted by an agency or private entity; threat response plans; emergency evacuation plans; sheltering arrangements; or security or fire-safety manuals. Id. Cf. *Marino v. University of Florida*, 107 So. 3d 1231 (Fla. 1st DCA 2013), in which the court rejected a university's contention that it could withhold the location of animal research facilities based on a determination that the nature of the public activities occurring at the facility subjects them to physical threats.

(1) Security System (Alarm) Permits and Applications

Sections 281.301 and 119.071(3)(a), F.S., prohibit public disclosure of the name and address of applicants for security system permits, of persons cited for violations of alarm ordinances, and of individuals who are the subject of law enforcement dispatch reports for verified or false alarms "because disclosure would imperil the safety of persons and property." Critical

Intervention Services, Inc. v. City of Clearwater, 908 So. 2d 1195, 1197 (Fla. 2d DCA 2005). Accord AGO 04-28.

(2) Surveillance Video Recordings

The term “security or fire-safety system plan” as used in s. 119.071(3)(a)1., F.S., includes “audio and visual presentations... relating directly to the physical security or fire-safety of the facility or revealing security or fire-safety systems.” Video footage captured by city bus cameras “directly relates to and reveals information about a security system” and thus was determined to be confidential and exempt from disclosure by ss. 281.301 and 119.071(3)(a), F.S. Central Florida Regional Transportation Authority v. Post-Newsweek Stations, Orlando, Inc., 157 So. 3d 401 (Fla. 5th DCA 2015). The videos “reveal the capabilities—and as a corollary, the vulnerabilities” of the security system. *Id.* at 405. And see AGO 15-06, relying on Central Florida Regional Transportation Authority, and applying the exemption to surveillance tapes from a security system for a public transit authority building. Cf. Gonzalez v. State, 240 So. 3d 99 (Fla. 2d DCA 2018) (in the absence of an in camera inspection of the requested records [CDs] the circuit court could not conclude that the contents were exempt from disclosure under s. 119.071(3)(a)2., or s. 281.301; nor could it determine whether redaction was possible); and City of Miami v. Blanco, 336 So. 3d 1268 (Fla. 3d DCA 2022) (trial court departed from essential requirements of law by failing to conduct in camera review before granting defendant’s motion to compel and/or for a subpoena for video camera recordings taken at police station following his arrest; without an in camera inspection, the judge could not determine whether the video recordings fell within the security plan exemption).

Video footage from surveillance cameras at a high school “relates directly” to the security system at the school, including both its capabilities and its vulnerabilities, and thus is confidential and exempt from disclosure unless one of the exceptions to the exemption applies. State Attorney’s Office of the Seventeenth Judicial Circuit v. Cable News Network, Inc., 251 So. 3d 205 (Fla. 4th DCA 2018). As previously discussed on pages 153-154,



there are several exceptions to this confidentiality provision, including a court order issued upon a showing of good cause. In State Attorney's Office, the appellate court affirmed the trial judge's order mandating release of surveillance video from a school shooting where 17 students and staff were killed. The court found that the media had established good cause because the footage revealed the conduct of public servants in the discharge of their duties and also provided "insight" into the high school's security "net" that failed to protect the students and staff. Id. at 215.

By contrast, the First District overturned the trial court's determination that a news organization had shown good cause to obtain security footage from two correctional institutions. *Florida Department of Corrections v. Miami Herald Media Company*, 278 So. 3d 786 (Fla. 1st DCA 2019). At the hearing, the Miami Herald advised that it no longer needed the video recordings as they were no longer newsworthy. Nevertheless the court still found that the Herald had satisfied the statutory exception to confidentiality, noting the awards the journalist received for her reporting on prison issues, and that this fact, combined with the "extremely important right of freedom of the press" constituted good cause. The appellate court reversed, finding that the Herald "extinguished any claim to good cause when it unambiguously renounced its need for the video footage." 278 So. 3d at 790.

c. Cybersecurity

Section 119.01(2)(a), F.S., states that agencies "must provide reasonable public access to records electronically maintained and must ensure that exempt or confidential records are not disclosed except as otherwise permitted by law." Cf. AGO 19-08 (pension board authorized to release nonpublic personnel information pursuant to a confidentiality agreement with a vendor conducting cybersecurity testing of the board's electronic data storage systems).

Accordingly, an agency is not required to provide direct access to the agency's electronic records through a hard drive provided by a requester, but must otherwise allow inspection and copying of such records in a manner which will accommodate the request, but protect from disclosure exempt or



confidential materials. AGO 13-07. And see *Rea v. Sansbury*, 504 So. 2d 1315, 1317-1318 (Fla. 4th DCA 1987), review denied, 513 So. 2d 1063 (Fla. 1987) (while county possesses statutory authority to facilitate inspection of public records by electronic means, this “does not mean that every means adopted by the county to facilitate the work of county employees ipso facto requires that the public be allowed to participate therein”).

Section 119.0725(2), F.S., provides that the following information held by an agency is confidential: coverage limits and deductible or self-insurance amounts of insurance or other risk mitigation coverages acquired for the protection of information technology systems, operational technology systems, or data of an agency; information relating to critical infrastructure; cybersecurity incident information reported pursuant to s. 282.318 or 282.3185, F.S.; network schematics, hardware and software configurations, or encryption information or information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, including suspected or confirmed breaches, if the disclosure of such information would facilitate unauthorized access to or unauthorized modification, disclosure, or destruction of data or information or information technology resources. Key terms used in this exemption such as “information technology” and “incident” are defined in s. 119.0725(1), F.S. Section 119.0725(5)(a), F.S., specifies agencies authorized to receive confidential information.

There are other exemptions which address cybersecurity issues. For example, s. 282.318(4), F.S., requires state agencies, as defined in the statute, to conduct risk assessments, and internal audits, as well as to develop policies and procedures to address cybersecurity issues. This section also contains exemptions for records relating to these functions. See s. 282.318(4)(d), (e), and (g), and (5), F.S. And see s. 119.0713(5)(a), F.S. (records relating to security of information technology systems of local government owned or operated utilities); s. 627.352 (Citizens Property Insurance Corporation) and s. 1004.055(1), F.S. (state postsecondary education institutions). Secure login credentials held by the Department of Highway Safety and Motor Vehicles are exempt, as are Internet protocol addresses, geolocation data, and other information from which a user



accesses a public facing portal. Section 119.0712(2)(f), F.S. And see the discussion of the exemptions from the Sunshine Law for cybersecurity meetings found on pages 36-37.

d. School System Security

Section 943.082(1), F.S., requires the Florida Department of Law Enforcement to acquire a mobile suspicious activity reporting tool that allows students and the community to relay information anonymously concerning unsafe, potentially harmful, dangerous, violent, or criminal activities, or the threat of these activities to appropriate public safety agencies and school officials. The identity of the reporting party received through the reporting tool and held by the department, law enforcement agencies, or school officials is confidential and exempt. Section 943.082(6), F.S. Any other information received through the reporting tool and held by the above agencies is exempt. *Id.* And see ss. 1004.0962(2), F.S. (campus emergency response held by a public postsecondary institution or specified agencies is exempt from disclosure); and 1004.055(1) (certain security incident information records held by state postsecondary education institution).

Any information that would identify whether an individual has been appointed as a safe school officer pursuant to s. 1006.12, F.S., held by a law enforcement agency, school district, or charter school is exempt. Section 1006.12(8), F.S. See also s. 119.071(3)(a), F.S., providing an exemption for agency security system plans, discussed on pages 155-156.

(Florida Office of the Attorney General // © March 9, 2023)