The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Rules

BILL:	CS/SB 442
INTRODUCER:	Rules Committee and Senator Yarborough
SUBJECT:	Return of Certain Search Warrants
DATE:	February 19, 2026 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Cellon	Stokes	CJ	**Favorable**
2.	Davis	Cibula	JU	**Favorable**
3.	Cellon	Kruse	RC	**Fav/CS**

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/SB 442 amends:

- Section 934.50(4)(b), F.S., to allow law enforcement to obtain a search warrant to search an area or areas, using a drone, where evidence that a crime was committed might reasonably be found.
- Section 933.02, F.S., to provide that recovering a dead body is a statutorily authorized reason to seek a search warrant from a court.
- Section 933.05, F.S., to alter the return of certain search warrants by:
  - Providing that a search warrant served on an out-of-state provider of electronic communications data as described in s. 934.23, F.S., must be returned within 20 days.
  - Providing that a warrant to search for and seize specimens from a specific person for DNA analysis and comparison, including blood and saliva samples, or to seize specimen pursuant to s. 943.325, F.S. for entry into the DNA database must be returned within 30 days.
  - Deleting the current 45 day return date and giving a law enforcement agency up to 365 days to return a search warrant to the court for a computer, a computer system, or an electronic device.
  - Specifying that if a search warrant is issued to search for and seize data or information contained in a computer, computer system, or electronic device, the warrant is considered timely executed if the computer, computer system, or electronic device is seized by a law enforcement agency within 10 days of the issuance of the search warrant, not including the date of issuance.

- Providing that a law enforcement agency is not required to complete the analysis or review of data or information contained in a computer, computer system, or electronic device within any specific time if such computer, computer system, or electronic device was timely seized by a law enforcement agency.

Section 933.07, F.S., is amended and s. 934.025, F.S., is created to provide that a judge may authorize a law enforcement officer to appear remotely using audio-video communication technology when seeking a search warrant from the judge.

The bill may have a fiscal impact. See Section V., Fiscal Impact Statement.

The bill becomes effective July 1, 2026.

II. Present Situation:

Search Warrant

A search warrant is a written order issued by a judge that authorizes a law enforcement officer to search a specific place and seize evidence. A warrant may not be issued unless the person seeking the warrant demonstrates in an affidavit that probable cause exists to believe that the evidence sought will aid in apprehending someone for a particular offense. The warrant must describe with particularity the place that is to be searched and the items to be seized.[1]

Section 933.04, F.S., states "The right of the people to be secure in their persons, houses, papers and effects against unreasonable seizures and searches shall not be violated and no search warrant shall be issued except upon probable cause, supported by oath or affirmation particularly describing the place to be searched and the person and thing to be seized."[2] Similarly, the State Constitution provides this same guarantee but adds the provision that this right extends to the people "against the unreasonable interception of private communications by any means."[3]

When proper affidavits are made, a search warrant may be issued under the provisions of ch. 933, F.S., upon any of the following grounds:

- When the property was stolen or embezzled in violation of law;
- When any property was used:
  - As a means to commit any crime;
  - In connection with gambling, gambling implements, and appliances; or
  - In violation of s. 847.011, F.S., or other laws in reference to obscene prints and literature;
- When any property constitutes evidence relevant to proving that a felony has been committed; and
- When any property is being held or possessed in violation of:
  - Any of the laws prohibiting the manufacture, sale, and transportation of intoxicating liquors;
  - The fish and game laws;

[1] Section 933.05, F.S., and 14A Fla. Jur 2d Criminal Law – Procedure: Pretrial Matters s. 657.
[2] Section 933.04, F.S. This section of the Florida Statutes is nearly identical to the Fourth Amendment of the U.S. Constitution, which must also be followed in matters related to search and seizure and privacy. See U.S. CONST. amend. IV.
[3] FLA. CONST. art. I, s. 12.

  - The laws relative to food and drug; or
  - The laws related to citrus disease pursuant to s. 581.184, F.S.; or
- When the laws in relation to cruelty to animals, as provided in ch. 828, F.S., have been or are violated in any building or place.

Section 933.02, F.S., applies to any papers or documents used as a means of or in aid of the commission of any offense against the laws of the state.[4]

A judge may electronically sign a search warrant if the requirements of subsections (1) or (2) of s. 933.07, F.S., are met and the judge, based on an examination of the application and proofs submitted, determines that the application:

- Bears the affiant's signature, or electronic signature if the application was submitted electronically.
- Is supported by an oath or affirmation administered by the judge or other person authorized by law to administer oaths.
- If submitted electronically, it is submitted by reliable electronic means.

A search warrant is considered issued by a judge at the time the judge affixes the judge's signature or electronic signature to the warrant. As used in this section, the term "electronic signature" has the same meaning as provided in s. 933.40, F.S.[5]

Although there are judicially recognized exceptions[6] to obtaining a search warrant before a search is conducted, the general preference is that a judge review the attesting officer's sworn application and warrant for the requisite probable cause for the seizure and the basis for it.[7]

Having found that probable cause for the search exists, the judge should then approve the warrant to be served, executed, and returned to the court by the law enforcement officer.[8, 9] Any search warrant must be returned within 10 days after it is issued; however, a search warrant issued for a computer, a computer system, or an electronic device, that is in the actual possession

[4] Section 933.02, F.S.
[5] Section 933.07(3), F.S.
[6] For example, the exigent circumstances exception "applies when the exigencies of the situation make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment." McNeely, 569 U.S. at 148-49, 133 S. Ct. at 1558 (quoting Kentucky v. King, 563 U.S. 452, 459, 131 S. Ct. 1849, 1856, 179 L. Ed. 2d 865 (2011)).
[7] " 'Probable cause exists where "the facts and circumstances within [an officer's] knowledge and of which [he] had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that" an offense has been or is being committed,' and that evidence bearing on that offense will be found in the place to be searched." Safford Unified Sch. Dist. # 1 v. Redding, 557 U.S. 364, 370, 129 S. Ct. 2633, 2639, 174 L. Ed. 2d 354 (2009) (alterations in original) (quoting Brinegar v. United States, 338 U.S. 160, 175-76, 69 S. Ct. 1302, 1310-11, 93 L. Ed. 1879 (1949)).
[8] Sections 933.07, 933.08, and 933.12, F.S.
[9] Upon the return of the warrant the officer shall attach thereto or thereon a true inventory of the property taken under the warrant, and at the foot of the inventory shall verify the same by affidavit taken before some officer authorized to administer oaths, or before the issuing officer, said verification to be to the following effect: I, A. B., the officer by whom the warrant was executed, do swear that the above inventory contains a true and detailed account of all the property taken by me on said warrant. Section 933.12, F.S.

of a law enforcement agency at the time the warrant is issued, must be returned to the court within 45 days after issuance thereof.[10]

Search Warrant Litigation and 2025 Legislation

A defendant was suspected of possessing child pornography in Manatee County in 2020. The sheriff's office seized his two mobile phones, a tablet, and a laptop. The detectives later applied for search warrants, one of which was for a forensic search of the devices. The circuit court issued the search warrant in July but one of the detectives working on the case admitted that the warrant was not executed until sometime in September, long past the 10 day period. The defendant moved to suppress the evidence but the circuit court rejected his argument finding that he had not been prejudiced by the time delay. On appeal, the Second District Court of Appeal noted that "the legislature has decided that ten days is a reasonable time" and that the language had been in place for over a century. The court reversed the judgment and sentences of the lower court and remanded the case for dismissal of the charges.[11]

Section 933.05, F.S., was amended by the Legislature during the 2025 Session to increase the time frame from 10 to 45 days within which a search warrant for a computer, a computer system, or an electronic device must be returned to the court.[12] At the time the search warrant for the computer, computer system, or electronic device is issued by the court, the property must be in the actual possession of a law enforcement agency.[13]

Digital Evidence

Law enforcement agencies can glean a lot of information from a criminal suspect's computer, computer system, and electronic devices.[14] The Florida Department of Law Enforcement (FDLE) relies on specialized tools and techniques to recover data from electronic devices that have been used or involved in criminal cases. An increasing number of devices and gadgets, including laptops, cell phones, gaming consoles, and Internet of Things (IoT),[15] are being used by both victims and perpetrators of crimes. The digital evidence gathered from these devices, such as web browser history, location data, text messages, and call records can provide significant

[10] Section 933.05, F.S.
[11] *Moschella v. State*, 413 So. 3d 851 (Fla. 2d DCA 2025).
[12] Chapter 2025-176, s. 7, Laws of Fla. Note that other search warrants must be returned within 10 days of the warrant's issue date.
[13] Section 933.05, F.S.
[14] "Computer" means an internally programmed, automatic device that performs data processing. "Computer system" means a device or collection of devices, including support devices, one or more of which contain computer programs, electronic instructions, or input data and output data, and which perform functions, including, but not limited to, logic, arithmetic, data storage, retrieval, communication, or control. The term does not include calculators that are not programmable and that are not capable of being used in conjunction with external files. "Electronic device" means a device or a portion of a device that is designed for and capable of communicating across a computer network with other computers or devices for the purpose of transmitting, receiving, or storing data, including, but not limited to, a cellular telephone, tablet, or other portable device designed for and capable of communicating with or across a computer network and that is actually used for such purpose. Section 815.03, F.S.
[15] "Internet of Things" is described as a network of devices that are interrelated and connect and exchange data with similar devices and the cloud. The devices are generally embedded with various forms of technology which might include sensors and software. Alexander S. Gillis and Kinza Yasar, TechTarget Network, *What is IoT (internet of things)?* (July 21, 2025) https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT.

insight into the events and activities surrounding a particular crime or incident. Digital evidence analysts rely on advanced forensic tools and techniques to retrieve and extract data; however, they frequently encounter the challenges created by encryption and passcodes, damaged and corroded devices, and deleted data recovery.[16]

Law enforcement officials point out that strong, end-to-end encryption on devices, or what they have called "warrant-proof encryption," prevents them from gaining lawful access to certain data. Companies that employ such strong encryption have emphasized that they do not hold encryption keys. The practical effect is that they may not be readily able to unlock, or decrypt, the devices or communications—even if a law enforcement officer presents an authorized search warrant or wiretap order.[17]

A law enforcement agency's efforts to gain access to a device or its content may be affected by several factors. For example, if a law enforcement agency attempts to unlock a device it would likely use software to try multiple combinations of keys in an effort to unlock the device. The agency's success may depend, however, on the amount of time available to try to unlock the device.[18]

Electronic Communications

Section 934.23, F.S., specifies the requirements with which an investigative or law enforcement officer[19] (officer) must comply to require a provider of electronic communication service[20] to disclose the contents[21] of a wire communication[22] or electronic communication,[23] or information

[16] *Digital and Multimedia Evidence*, Forensics Disciplines, FDLE, available at https://www.fdle.state.fl.us/Forensics/Disciplines/Digital-Evidence, (last viewed February 3, 2026).
[17] Kristin Finklea, Congressional Research Service*, Law Enforcement and Technology: The "Lawful Access" Debate"* (Jan. 16, 2024) https://www.congress.gov/crs_external_products/IF/PDF/IF11769/IF11769.3.pdf.
[18] *Id.*
[19] "Investigative or law enforcement officer" means any officer of the State of Florida or political subdivision thereof, of the United States, or of any other state or political subdivision thereof, who is empowered by law to conduct on behalf of the Government investigations of, or to make arrests for, offenses enumerated in ch. 934, F.S., or similar federal offenses, any attorney authorized by law to prosecute or participate in the prosecution of such offenses, or any other attorney representing the State of Florida or political subdivision thereof in any civil, regulatory, disciplinary, or forfeiture action relating to, based upon, or derived from such offenses. Section 934.02(6), F.S.
[20] "Electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications. Section. 934.02(15), F.S.
[21] "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. Section 934.02(7), F.S.
[22] "Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception including the use of such connection in a switching station furnished or operated by any person engaged in providing or operating such facilities for the transmission of intrastate, interstate, or foreign communications or communications affecting intrastate, interstate, or foreign commerce. Section 934.02(1), F.S.
[23] "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects intrastate, interstate, or foreign commerce, but does not include:

about a customer or subscriber of an electronic communication service or remote computing service.[24] To require the disclosure of such information, an officer must either seek a warrant issued by a judge of a court of competent jurisdiction or, for such information that has been in electronic storage for more than 180 days, obtain a warrant[25] or subpoena.[26] To require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a customer or subscriber, not including the contents of a communication, the officer must have the consent of the subscriber, or he or she must obtain a warrant or subpoena.[27]

DNA Database

Florida's DNA database was established in 1989[28] to assist law enforcement agencies in the identification and detection of individuals in criminal investigations and the identification and location of missing and unidentified persons. The FDLE administers the statewide DNA database, which is capable of classifying, matching, and storing analyses of DNA and other biological molecules and related data.[29]

The DNA database may contain DNA data obtained from the following types of biological samples:

- Crime scene samples.
- Samples obtained from "qualifying offenders."
- Samples lawfully obtained during the course of a criminal investigation, including those from deceased victims or deceased suspects.
- Samples from unidentified human remains.
- Samples from persons reported missing.
- Samples voluntarily contributed by relatives of missing persons.
- Other samples approved by FDLE.[30]

Under s. 943.325, F.S., a "qualifying offender" includes both juveniles and adults who are committed to a county jail or who are committed to or under the supervision of the Department of Corrections (DOC) or the Department of Juvenile Justice, and who are:

- Convicted of or arrested for committing a felony offense or an attempt to commit a felony offense;

- Any wire or oral communication;
- Any communication made through a tone-only paging device;
- Any communication from an electronic or mechanical device which permits the tracking of the movement of a person or an object; or
- Electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds. Section 934.02(12), F.S.

[24] "Remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system. Section 934.02(19), F.S.

[25] The term "order" is used in statute, but the underlying requirements for such an order are identical to that of a search warrant issued under ch. 933, F.S.

[26] Section 934.23(1) – (3) and (5), F.S.

[27] Section 934.23(4) and (5), F.S.

[28] Chapter 89-335, Laws of Fla.

[29] Section 943.325(4), F.S.

[30] Section 943.325(6), F.S.

- Convicted of specified misdemeanor offenses; or
- In the custody of a law enforcement agency and subject to an immigration detainer.[31]

A qualifying offender is required to submit a DNA sample for inclusion in the statewide database if he or she is:

- Arrested or incarcerated in Florida; or
- On probation, community control, parole, conditional release, control release, or any other type of court-ordered supervision.[32]

If a court order fails to order a qualifying offender to submit a DNA sample, a prosecutor may seek an amended order from the sentencing court requiring such an offender to provide such a sample.[33] Alternatively, FDLE, DOC, a law enforcement agency, or the prosecutor may seek a warrant authorizing the seizure of the qualifying offender for the purpose of securing the required DNA sample.[34] The court must issue such a warrant upon a showing of probable cause.[35]

Law Enforcement Use of Drones

Section 934.50, F.S., the "Freedom from Unwarranted Surveillance Act," (Act) restricts the use of drones by individuals and government entities to conduct surveillance. Specific to law enforcement, a law enforcement agency,[36] is prohibited from using a drone to gather evidence or other information, except:

- To counter a high risk of a terrorist attack by a specific individual or organization if the United States Secretary of Homeland Security determines that credible intelligence indicates that there is such a risk.
- If the law enforcement agency first obtains a search warrant signed by a judge authorizing the use of a drone.
- If the law enforcement agency possesses reasonable suspicion that, under particular circumstances, swift action is needed to prevent imminent danger to life or serious damage to property, to forestall the imminent escape of a suspect or the destruction of evidence, or to achieve purposes including, but not limited to, facilitating the search for a missing person.
- To provide a law enforcement agency with an aerial perspective of a crowd of 50 people or more or to provide and maintain the public safety of such a crowd, provided that:
    - The law enforcement agency must have policies and procedures that include guidelines:
        - For the agency's use of a drone.
        - For the proper storage, retention, and release of any images or video captured by the drone.
        - Address the personal safety and constitutional protections of the people being observed.

[31] Section 943.325(2)(g), F.S.
[32] Section. 943.325(7), F.S.
[33] Section 943.325(12)(b), F.S.
[34] *Id.*
[35] *Id.*
[36] "Law enforcement agency" means a lawfully established state or local public agency that is responsible for the prevention and detection of crime, local government code enforcement, and the enforcement of penal, traffic, regulatory, game, or controlled substance laws. Section 934.50(2)(d), F.S.

  - The head of the law enforcement agency using the drone for this purpose must provide written authorization for such use and must maintain a copy on file at the agency.
- To assist a law enforcement agency with traffic management; however, a law enforcement agency may not issue a traffic infraction citation based on images or video captured by a drone.
- To facilitate a law enforcement agency's collection of evidence at a crime scene or traffic crash scene.
- In furtherance of providing and maintaining the security of an elected official pursuant to s. 943.68, F.S.[37]

If a law enforcement agency violates any of the restrictions on the use of drones as provided under the Act:
- A person may initiate a civil action against the law enforcement agency to obtain all appropriate relief to prevent or remedy such a violation. [38]
- Any evidence obtained or collected in violation of the Act is not admissible as evidence in a criminal prosecution.[39]

III. Effect of Proposed Changes:

The bill amends s. 933.02, F.S., to provide that a search warrant may be issued to recover a dead body based on the probable cause presented to a judge in a sworn affidavit by a law enforcement officer.

Generally, a search warrant must be returned to the court within 10 days after issuance. The bill amends s. 933.05, F.S., to eliminate the date of the *warrant's issuance* as one of the 10 days in the countdown to the deadline to return the warrant.

A search warrant served on an out-of-state provider of electronic communications data as described in s. 934.23, F.S., must be returned within 20 days.

A search warrant Providing that a warrant to search for and seize specimens from a specific person for DNA analysis and comparison, including blood and saliva samples, or to seize specimen pursuant to s. 943.325, F.S., for entry into the DNA database must be returned within 30 days.

The bill gives a law enforcement agency up to 365 days to return a search warrant to the court for a computer, a computer system, or an electronic device. It deletes the current 45 day return date in lieu of the 365 days.

The bill specifies that if a search warrant is issued to search for and seize *data or information contained in* a computer, computer system, or electronic device, the warrant is considered *timely executed* if the computer, computer system, or electronic device was *seized* by a law enforcement agency within 10 days of the *issuance* of the search warrant, not including the date of issuance.

[37] Section 934.50(3), F.S.
[38] Section 934.50(5)(a), F.S.
[39] Section 934.50(6), F.S.

Additionally, this does not require that law enforcement complete the analysis or review of data or information contained in a computer, computer system, or electronic device within the period provided, if such computer, computer system, or electronic device was timely seized by a law enforcement agency.

Appearing with the Judge Remotely

The bill creates s. 934.025, F.S., a new section of law authorizing a law enforcement officer to appear remotely before the judge to apply for a search warrant or court order pursuant to ch. 934, F.S., using audio-video communication technology.

The bill amends s. 933.07, F.S., to provide that a law enforcement officer may appear remotely before a judge to apply for a search warrant.

Searches and Seizures Using Drones

Finally, the bill amends s. 934.50(4)(b), F.S. to allow law enforcement to obtain a search warrant to search an area or areas where evidence that a crime was committed might reasonably be found. The phrase "evidence that a crime was committed might reasonably be found" does not equate to probable cause that a crime was committed.[40]

The bill takes effect on July 1, 2026.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

The bill does not appear to require cities and counties to expend funds or limit their authority to raise revenue or receive state-shared revenues as specified by Article VII, s. 18, of the State Constitution.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

[40] "[N]o search warrant shall be issued except upon probable cause, supported by oath or affirmation particularly describing the place to be searched and the person and thing to be seized." See U.S. Const. amend. IV.

E. Other Constitutional Issues:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

The bill may not have a fiscal impact on local law enforcement agencies unless the bill results in law enforcement agencies storing computers, computer systems, and electronic devices until such time as secure storage becomes less available for other items, and secure storage will have to be increased.

It is possible that the Florida Department of Law Enforcement may incur additional costs related to workload and forensic DNA laboratory supplies and sample storage, depending on how much of an increase the department experiences in DNA specimen intake from the bill.

VI. Technical Deficiencies:

None.

VII. Related Issues:

It is unclear when the return of a search warrant for data or information contained in a computer, etc., must occur. The bill allows for the return of a search warrant to search and seize a computer, a computer system, or an electronic device, must be returned in 365 days. However, the bill also states that a search warrant to search for and seize data or information contained in a computer, computer system, or electronic device is considered timely executed if the computer, computer system, or electronic device was seized by a law enforcement agency within 10 days. If the seizure was timely executed, law enforcement is not required to complete the analysis or review of data or information contained in the computer, computer system or electronic device within the proscribed time period in subsection (2). The bill is silent on the return date for a warrant for data or information, but would likely be required to be returned in 365 days as required for a computer, computer system, or electronic device.

VIII. Statutes Affected:

This bill substantially amends ss. 933.02, 933.05, 933.07, 934.50 of the Florida Statutes.
The bill creates s. 934.025 of the Florida Statutes.

IX. Additional Information:

A. Committee Substitute – Statement of Substantial Changes:

(Summarizing differences between the Committee Substitute and the prior version of the bill.)

CS by Rules on February 17, 2026:

- Authorized a search warrant to be issued to recover a deceased body.
- Authorized a judge to allow a law enforcement officer to appear remotely when applying for certain search warrants and court orders.
- Specified return periods for search warrants that are issued to recover certain electronic communications data and for warrants that are issued to seize blood and saliva specimens.
- Specified the time period in which a search warrant issued for a computer, computer system, or electronic device is timely executed.
- Specified that a law enforcement agency is not required to complete an analysis or review of information seized from a computer, computer system, or electronic device within the 365 day warrant return period.
- Authorized a law enforcement agency to use a drone to conduct a search of an area or areas where evidence might reasonably be found if the agency first obtains a search warrant.

B. Amendments:

None.