

**California Secretary of State
Proposed Regulatory Action:
CAL-ACCESS Software Vendor Certification
Proposed Regulation Text**

**Title 2. Administration
Division 7. Secretary of State
Chapter 16. Political Reform**

These proposed regulations add new Chapter 16 to Division 7 of Title 2 of the California Code of Regulations.

Article 1. CAL-ACCESS Software Vendor Certification

23001. Purpose

(a) The purpose of this Article is to establish standards and procedures for certifying software vendors to file information required under the Political Reform Act of 1974 with the Secretary of State's California Automated Lobbyist and Campaign Contribution and Expenditure Search System (CAL-ACCESS) electronic filing system through the Application Programming Interface (API).

(b) This Article only applies to software vendors and is not intended to apply to filers who only use a software vendor's electronic filing system for filing purposes.

Note: Authority cited: Section 84602, Government Code.

23002. Definitions

As used in this Article, the following words have the following definitions:

(a) "API" means the Application Programming Interface built within CAL-ACCESS to permit a software vendor's electronic filing system to communicate with the Secretary of State's CAL-ACCESS electronic filing system.

(b) "Business day" means each day in which the Secretary of State's office is open to the public for business, as specified in Government Code Section 11020.

(c) "CAL-ACCESS" means the Secretary of State's California Automated Lobbyist and Campaign Contribution and Expenditure Search System, an electronic filing system for campaign, slate mailer, and lobbying information maintained by the Secretary of State, as described in Government Code Section 84602, that provides financial information supplied by state candidates, donors, lobbyists, and others.

(d) "Electronic Filing Specifications" means the most current version of the nonproprietary standardized record format for the transmission of data that is required of persons and entities required to file online under Government Code Section 84605 and that conforms to the disclosure requirements of the Political Reform Act of 1974. The Electronic Filing Specifications are issued, updated periodically, and maintained by the Secretary of State.

(e) "Electronic filing system" or "system" means any web-based or desktop-based software that facilitates the filing of statements and reports with CAL-ACCESS through the API.

- (f) “Filer” shall have the same meaning as specified in Government Code Section 82026.
- (g) “Software vendor” means any person or entity outside of the Secretary of State that maintains an electronic filing system.

Note: Authority cited: Section 84602, Government Code. Reference: Sections 11020, 82026, and 84605, Government Code.

23003. Software Vendor Certification

- (a) Each software vendor that intends to submit filings to CAL-ACCESS through the API shall be certified by the Secretary of State prior to transmission of any filings.
- (b) In order for a software vendor to be certified by the Secretary of State, the software vendor shall:
 - (1) Complete, sign, and submit an application.
 - (2) Develop an electronic filing system that complies with the latest version of the Electronic Filing Specifications in effect at the time of certification.
 - (3) Ensure that its electronic filing system is compatible with CAL-ACCESS’ data-driven method described in Government Code Section 84602.
 - (4) Develop a procedure for filers to comply electronically with the requirement to verify and sign statements and reports under penalty of perjury. The software vendor’s system shall collect and maintain a secure electronic signature of the required individual that is submitted under penalty of perjury and that conforms to Government Code Section 81004 and Civil Code Section 1633.11(b). The software vendor shall transmit to CAL-ACCESS, through the API, the name of the individual who verifies and signs the statement or report, as well as the date signed.
 - (5) Successfully complete all certification testing of its system with the Secretary of State to determine whether the file format is in compliance with the Electronic Filing Specifications and is compatible with CAL-ACCESS by:
 - (i) Sending sample data through the API and ensuring that the data it posts to CAL-ACCESS is consistent with the data verified and signed by a filer in the electronic filing system; and
 - (ii) Resolving all certification related defects identified through testing. If all defects cannot be resolved, the software vendor shall identify a mitigated workaround, submit that workaround in writing to the Secretary of State, and implement the workaround upon the Secretary of State’s approval. This workaround shall remain in effect until the resolution of defects can be completed.
 - (6) Design its system such that all data filed using the electronic filing system may be maintained for the period during which an administrative action can be brought against a filer, as specified by Government Code Section 91000.5, and for the duration of any open administrative action, as follows:
 - (i) For the purpose of this paragraph, “data filed with CAL-ACCESS” means all of the information the filer submitted that was posted to CAL-ACCESS, the date and time the filer submitted that information, the filer’s name, the filer’s secure electronic signature, and identifying information about the filer such as their Internet Protocol (IP) address.

- (ii) For web-based software, save a copy of all data filed with CAL-ACCESS on the software vendor's servers, on a cloud, on optical discs, or by another such a way that the data will be accessible to the filer.
- (iii) For desktop-based software, save a copy of all data filed with CAL-ACCESS on the filer's local device. The software vendor shall not be liable for a filer who deletes or fails to maintain the data saved on his or her local device.
- (c) Each software vendor may seek certification for some or all the Fair Political Practices Commission forms for which the API accepts filings. In addition, if a software vendor does not meet interface testing for a particular form, the Secretary of State may approve the software vendor for certification of fewer forms than the software vendor requests. The software vendor may resubmit for testing and approval the form(s) that did not meet requirements, and the Secretary of State may certify those forms without the software vendor submitting an additional application. If a software vendor seeks certification for a form that it did not apply for in its original application, the software vendor must submit a new application.
- (d) The Secretary of State will not unreasonably withhold certification for minor testing defects. The Secretary of State will not withhold certification of an entire electronic filing system for issues constrained to a particular form. However, if the Secretary of State and the software vendor cannot come to an agreement to resolve outstanding defects that affect the entire system, the Secretary of State will not certify the software vendor.
- (e) The Secretary of State will provide each certified software vendor with credentials to access the API. The software vendor shall not share these credentials.
- (f) If a certified software vendor transfers – in whole or in part – its electronic filing system to another person or entity, the transferee must independently certify with the Secretary of State in order to continue filing through the API. A transferee is not required to certify with the Secretary of State if it does not continue filing through the API. The Secretary of State will not unreasonably withhold certification to the transferee.
- (g) Each certified software vendor shall maintain compliance with the Electronic Filing Specifications, the requirements of Government Code Section 84602, and this Article in order to maintain certification. The Secretary of State may de-certify a software vendor that it discovers or determines is out of compliance, following the procedures described in Section 23008.

Note: Authority cited: Section 84602, Government Code. References: Section 1633.11, Civil Code and Sections 81004 and 91000.5, Government Code.

23004. Software Vendor Security

- (a) Each software vendor shall protect the security and integrity of the data and information stored on its servers and transmitted to CAL-ACCESS through its servers.
- (b) Each software vendor shall provide annual privacy and security awareness training to all its staff and contractors, if any, who have access to its servers that host its electronic filing system or who make code changes to its electronic filing system.
- (c) Each software vendor shall take the following security measures to ensure the security of its electronic filing system, to the extent that system is hosted on its servers, as well as the security of all systems used to make code changes to its electronic filing system:
 - (1) The servers shall be hardened to industry best practices.

- (2) The servers shall have anti-malware software installed and configured, and updates regularly applied.
- (3) Direct user access to the servers shall require, at a minimum, two-factor authentication.
- (d) Each software vendor shall implement security log management on its servers that host its electronic filing system as well as all systems used to make code changes to its electronic filing system, which includes the following:
 - (1) Enable logging on all systems and network devices with sufficient information collection.
 - (2) Review logs regularly for any errors, abnormal activities, and any system configuration changes.
 - (3) Securely store log files separately from the systems monitored and protect the logs from unauthorized modification, access, or destruction.
 - (4) Use log monitoring tools to send real-time alerts and notifications.
 - (5) Utilize multiple synchronized United States-based time sources.
- (e) Each software vendor shall report detected unauthorized use or unscheduled unavailability outages of any of its servers that host its electronic filing system or are used to make code changes to its electronic filing system to the Secretary of State within one (1) business day of discovery.
- (f) A software vendor shall not be responsible for the security of the systems of filers who use its electronic filing system.
- (g) The requirements in this section do not apply to filers who use an electronic filing system.

Note: Authority cited: Section 84602, Government Code.

23005. System Changes

- (a) Each certified software vendor shall update its electronic filing system to conform to changes to the CAL-ACCESS system and the Electronic Filing Specifications made by the Secretary of State. These changes may be due to system improvements or modifications; changes in disclosure requirements in the Political Reform Act of 1974, Fair Political Practices Commission regulations or forms, or other state laws and regulations; revised business processes; or other system modifications.
- (b) Each certified software vendor shall update its electronic filing system to conform to changes to the CAL-ACCESS system and the Electronic Filing Specifications made by the Secretary of State within the time period specified by the Secretary of State. This time period may vary based on the scope and urgency of the changes but will be no less than thirty (30) business days after notification by the Secretary of State. The Secretary of State will provide software vendors with information regarding changes to the Electronic Filing Specifications and the ability to test their systems. The Secretary of State will not unreasonably deny software vendor requests for additional time to make these changes.
- (c) If a certified software vendor does not update its electronic filing system to comply with system changes after notification of such changes by the Secretary of State, the Secretary of State may de-certify the software vendor, as described in Section 23008.
- (d) If a certified software vendor makes a significant change to its electronic filing system that affects data moving through the API, the software vendor shall notify the Secretary of State at least ten (10) business days before implementing the change and conduct certification testing of

the changes if requested by the Secretary of State. The software vendor shall not implement the change until the Secretary of State approves the change.

Note: Authority cited: Section 84602, Government Code.

23006. Bugs or Defects

- (a) For the purposes of this section, a “serious bug or defect” in a certified software vendor’s electronic filing system is one that changes the content or format of the data moving through the API such that the information submitted by the filer is not materially similar to the information posted to CAL-ACCESS. A bug or defect that results in minor formatting issues, such as a small number of extra spaces between words, shall not be considered serious.
- (b) Each certified software vendor shall log all serious bugs or defects in its electronic filing system and provide those logs to the Secretary of State within one (1) business day upon the Secretary of State’s request.
- (c) Each certified software vendor shall report all serious bugs or defects in its electronic filing system as soon as practicable, but no later than one (1) business day after discovery, to the Secretary of State.
- (d) Each certified software vendor shall resolve any serious bug or defect in its electronic filing system within three (3) business days of reporting it to the Secretary of State, or by a mutually-agreed-on date between the software vendor and the Secretary of State.
- (e) Upon discovery of a serious bug or defect in its electronic filing system, the certified software vendor shall immediately cease transmission through the API of the unintended data or formats. The software vendor shall not resume data transmission until the bug or defect causing the issue is resolved and the Secretary of State notifies the software vendor that it may resume data transmission.
- (f) Each certified software vendor shall, in a timely manner, notify all filers affected by any serious bug or defect in its electronic filing system of the issue and provide instructions on alternate means to file with the Secretary of State until the issue is resolved. This notification requirement shall apply only to filers for whom the software vendor has contact information, such as its customers.

Note: Authority cited: Section 84602, Government Code.

23007. Continued Compliance Verification

- (a) To ensure continued compliance with the requirements of the API and this Article, the Secretary of State may request that a certified software vendor conduct updated interface testing of its electronic filing system. The purpose of this testing is to ensure that all data in CAL-ACCESS sent by the software vendor’s electronic filing system is consistent with the data verified and signed by the filer in the software vendor’s electronic filing system.
- (b) The Secretary of State will notify a certified software vendor at least ten (10) business days before conducting interface testing with the software vendor’s electronic filing system. However, the testing may begin earlier than that planned date if the software vendor agrees.
- (c) Testing for continued compliance verification will be the same type of testing that is done for certifying a software vendor, as described in Section 23003.

(d) If continued compliance verification shows deficiencies in data sent to CAL-ACCESS, the software vendor shall submit corrected data for previous filings to the Secretary of State immediately, by any method specified by the Secretary of State, and follow the resolution procedure in Section 23006 to prevent further data discrepancies.

Note: Authority cited: Section 84602, Government Code.

23008. Software Vendor De-certification

(a) The Secretary of State may de-certify a software vendor if the software vendor is out of compliance with this Article and fails to timely resolve any compliance issues.

(b) At least thirty (30) business days prior to de-certification, the Secretary of State will provide written notice to the software vendor specifying the reasons for de-certification.

(c) A software vendor shall have the opportunity to cure any defects or bugs cited by the Secretary of State as reason for de-certification according to the process described in Section 23006.

(d) A software vendor shall have the opportunity to implement any system changes cited by the Secretary of State as reason for de-certification according to the process described in Section 23005.

(e) The Secretary of State will not unreasonably de-certify the software vendor while the software vendor works to resolve any issues cited as reasons for de-certification. However, the Secretary of State may de-certify the software vendor if the Secretary of State determines that the software vendor is not making reasonable progress or if keeping the software vendor certified would interfere with accurate filing.

(f) A software vendor whose electronic filing system has been de-certified shall be eligible to re-apply for certification following de-certification utilizing the process described in Section 23003.

Note: Authority cited: Section 84602, Government Code.