# California Secretary of State
# Proposed Regulatory Action:
# CAL-ACCESS Software Vendor Certification
# Initial Statement of Reasons

## PUBLIC HEARING AND COMMENT

**Hearing Date:** No hearing date is scheduled. A public hearing will be held if any interested person, or his or her duly authorized representative, submits a written request for a public hearing to the contact person listed no later than 15 days prior to the close of the written comment period.

**Written Public Comment Period:** June 19, 2020 through August 3, 2020

**Subject Matter of Proposed Regulations:** CAL-ACCESS Software Vendor Certification

**Section(s) Affected:** Sections 23001, 23002, 23003, 23004, 23005, 23006, 23007, and 23008 of Title 2, Division 7, Chapter 16 of the California Code of Regulations

## PURPOSE AND NECESSITY

As required by Government Code section 84602, in 1999 the California Secretary of State (SOS) created CAL-ACCESS, a database and filing system used to make much of the lobbying and campaign finance information required by the Political Reform Act of 1974 (PRA) available online to the public at no cost to users. This system functioned well for years, but is now 20 years old, components of it are no longer supported by the vendor, and as a result the system has periodically crashed and denied public access. Senate Bill (SB) 1349 (Chapter 845, Statutes of 2016) modified Government Code section 84602 to require the SOS to replace CAL-ACCESS with a new system that uses a data-driven means or method that allows filers to submit required filings free of charge in a manner that facilitates public searches of the data.

Pursuant to Government Code section 84602(b), the SOS has drafted these proposed regulations to address the requirement for the system replacing the current CAL-ACCESS, the CAL-ACCESS Replacement System (CARS), that software vendors be able to file reports electronically. The SOS consulted with software vendors in drafting these regulations.

The SOS is proposing to add Chapter 16 to the California Code of Regulations to establish a certification process for software vendors who wish to file electronically with the CARS through an Application Programming Interface (API) that the SOS is creating to achieve this electronic filing. The software vendors requested that the SOS include the option of filing through an API in the CARS system and the SOS agreed to make sure the system retained that feature. Filing through an API enables software vendors to file statements and reports rapidly for multiple clients near the filing deadlines. These regulations only apply to software vendors who file through the API, and do not apply to filers who file in the CARS by other means, such as by bulk upload or filing individually with the system.

## FACTUAL BASIS / RATIONALE

With the move to exclusive electronic filing, it is critical that the SOS ensures the information a filer attests to is what they had intended to file. This is especially important given that filers will be signing filed reports and statements electronically under the penalty of perjury, but without original signatures. Under the PRA, candidates, treasurers and other filers are required to verify and sign under penalty of perjury that to the best of their knowledge the information they submit is true, complete and correct. The SOS must ensure this requirement is met when filings come through the API. These regulations allow the SOS to specifically delineate how this shall be done. These regulations provide for a certification process for software vendors that protects the security of the data transmitted into CAL-ACCESS and delineates expectations on software vendors for providing data compliant and consistent with the PRA, including future amendments to that law. These regulations clarify the application and certification procedures for software vendors to use the API. This protects the software vendors because it spells out the certification and decertification process as well as how issues can be resolved. A regulation that requires software vendors to make changes to their software when necessary prevents them from holding up changes the SOS makes to CAL-ACCESS, including changes needed due to changes in the law.

In addition, Government Code section 84602(b)(2)(A) requires the Secretary of State to publish and make available to the public a list of software vendors who have submitted acceptable test files for the CARS system. Vendors who have completed the certification process will be published on this list. Further, vendors may be certified to submit information for some campaign or lobbying forms, but not the full suite of forms. Through the certification process, vendors can clearly designate which forms they are seeking approval to be able to file through the API.

The proposed regulations accomplish the mandate of Government Code section 84602. The benefit of these proposed regulations is that they will provide guidance to the SOS and software vendors on the procedure for being certified to use the API to transmit data electronically to the CARS. These regulations protect software vendors by preventing them from being unreasonably decertified as the law or CAL-ACCESS changes, and furthers the purposes of the PRA by ensuring only accurate data is transmitted over the API.

The factual basis and rationale for each section of the proposed regulations are as follows:

**23001. Purpose**

(a) The purpose of this subdivision is to define the purpose of these regulations. This subdivision is necessary to give context to the regulations and to explain what the regulations apply to: a certification process for electronically filing with the Secretary of State's California Automated Lobbyist and Campaign Contribution and Expenditure Search System (CAL-ACCESS) through an Application Programing Interface.

(b) The purpose of this subdivision is to explain who these regulations apply to and who they do not apply to. This subdivision is necessary to limit the regulations only to those they

are intended to apply to and to prevent misinterpretation by other filers, who may otherwise think the regulations apply to them.

**23002. Definitions**

(a) The purpose of this subdivision is to define Application Programming Interface. This subdivision is necessary to explain the technology software vendors who obtain certification under these regulations will use to communicate with CAL-ACCESS.

(b) The purpose of this subdivision is to define business day. This subdivision is necessary to define this term to prevent ambiguity when it is used throughout the regulations.

(c) The purpose of this subdivision is to define CAL-ACCESS. This subdivision is necessary to prevent spelling out the full name and description of this system each time it is used throughout the regulations.

(d) The purpose of this subdivision is to define electronic filing specifications. This subdivision is necessary to define the term and describe how these specifications are created and maintained. These specifications are not incorporated by reference as they are not a requirements document but rather a set of formats that are necessary to ensure data can transmit over the API and post properly to CAL-ACCESS.

(e) The purpose of this subdivision is to define electronic filing system and to give a shortened version of that term, "system." This subdivision is necessary to provide clarity for when this term is used throughout the regulations.

(f) The purpose of this subdivision is to define filer with a reference to the same term in the PRA. This non-substantive subdivision is necessary to provide clarity of how that term is used throughout these regulations.

(g) The purpose of this subdivision is to define software vendor. This subdivision is necessary to provide clarity of how that term is used throughout these regulations.

**23003. Software Vendor Certification**

(a) The purpose of this subdivision is to state the requirement that certification is required in order to file with CAL-ACCESS through the API. This subdivision is necessary to provide this requirement. Certification is necessary to ensure the accurate transmission of data into CAL-ACCESS. Certification allows the California Secretary of State (SOS) to ensure software vendors seeking to use the API are compliant with these regulations both before they begin filing and as they continue to file. Certification protects software vendors because it spells out when they will be allowed and prevented from filing through the API as well as how issues can be resolved. Certification also ensures that software vendors shall make changes to their software when necessary which prevents them from holding up changes the SOS makes to CAL-ACCESS, including changes needed due to changes in the law.

(b) The purpose of this subdivision is to list certification requirements. This non-substantive subdivision introduces the list to follow.

    (1) The purpose of this paragraph is to require software vendors to complete, sign, and submit an application. This subdivision is necessary to state that software vendors must submit an application in order to be certified.

    (2) The purpose of this paragraph is to require software vendors to develop an electronic filing system that complies with the electronic filing specifications.

This subdivision is necessary to ensure the software vendors' software is compliant with the API and transmits accurate data to CAL-ACCESS.

(3) The purpose of this paragraph is to require software vendors to ensure their electronic filing systems are compatible with CAL-ACCESS. This paragraph references the statutory requirement for CAL-ACCESS to be a data driven system. This paragraph is necessary to make sure software vendors send data that can be presented in CAL-ACCESS in this manner. This is in contrast to the current version of CAL-ACCESS, which presents data in a forms-based method. This paragraph is necessary to ensure software vendors send data-driven information to CAL-ACCESS so that CAL-ACCESS accurately presents the data, as intended by the underlying statute.

(4) The purpose of this paragraph is to describe the method by which software vendors ensure filers submit filings under the penalty of perjury. This paragraph is necessary to describe the appropriate method for ensuring filing is done under the penalty of perjury and to ensure the statutory requirement of filing under the penalty of perjury is met.

(5) The purpose of this paragraph is to require certification testing and to list the steps to complete this testing. This paragraph is necessary to ensure that software vendors' electronic filing systems comply with the electronic filing specifications so that data is accurately transmitted to CAL-ACCESS through the API.

  (i) The purpose of this subparagraph is to require software vendors to send sample data through the API. This subparagraph is necessary to describe how data shall be verified to ensure it is being accurately transmitted.

  (ii) The purpose of this subparagraph is to require resolution of defects identified through testing in the previous subparagraph. This subparagraph provides for a workaround to be approved by the Secretary of State while defect resolution is in process. This subparagraph is necessary to ensure that defects are resolved before certification can be completed. The workaround requirement ensures testing can continue while the defects are resolved and allows software vendors being subject to continued compliance verification pursuant to Section 23007 to remain operational during this verification that uses the same procedures as initial certification.

(6) The purpose of this paragraph is to require software vendor systems to maintain filing data. This paragraph is necessary to ensure filing data is maintained for the period under which a filer may be subject to audit or enforcement action under the PRA. Maintaining filing with the software vendor system is important so that, if necessary, the accuracy of the data as entered by the filer can be compared with data as it is presented in CAL-ACCESS.

  (i) The purpose of this subparagraph is to define "data filed with CAL-ACCESS" as used in the remainder of this paragraph. This definition is necessary so that software vendors know what data they must maintain.

  (ii) The purpose of this subparagraph is to describe how data should be stored for web-based software solutions. This subparagraph is necessary to describe appropriate data storage methods for systems that store and transmit data centrally in a manner that the software vendor can control.

(iii) The purpose of this subparagraph is to describe how data should be stored for desktop-based software solutions. This subparagraph is necessary to describe appropriate data storage methods for systems that are installed on filers' computers and transmit data to CAL-ACCESS without sending it through a central location controlled by the software vendor.

(c) The purpose of this subdivision is to specify that software vendors can obtain either full or partial certification. This subdivision clarifies the process for changing certification to transmit different data to CAL-ACCESS than a software vendor is approved for. This subdivision is necessary to clarify this process.

(d) The purpose of this subdivision is to specify protections for software vendors against unreasonable certification withholding. This subdivision is necessary to clarify the Secretary of State's certification authority.

(e) The purpose of this subdivision is to clarify how the software vendor shall obtain credentials to use the API and that they cannot share those credentials with other software vendors. This subdivision is necessary to clarify the process and ensure the API is not accessed by uncertified software vendors.

(f) The purpose of this subdivision is to clarify that a software vendor may not transfer their certification and ability to transmit data through the API to another software vendor. This subdivision is necessary to ensure only certified software vendors transmit data through the API. This protects the integrity of the data in CAL-ACCESS and ensures each software vendor using the API has been through the certification process and is subject to these regulations.

(g) The purpose of this subdivision is to clarify the requirements that a software vendor must meet to maintain their certification. This subdivision cross-references another section of these regulations dealing with de-certification. This subdivision is necessary to clarify these continuing obligations and reference de-certification procedures.

**23004. Software Vendor Security**

(a) The purpose of this subdivision is to ensure software vendors protect the security and integrity of the data stored on its servers. This subdivision is necessary to clarify this obligation on software vendors, in order to protect the integrity of the data that is filed pursuant to the PRA. Reports and statements filed with software vendors through the API are original filings in CARS and therefore they must be protected from a security and data integrity perspective.

(b) The purpose of this subdivision is to require software vendor security training. This subdivision is necessary to ensure software vendor staff and contractors are using best practices to protect the security and integrity of data filed through the API.

(c) The purpose of this subdivision is to require software vendors to take specific measures to ensure the security of their electronic filing systems. This subdivision is necessary to require specific measures to ensure the security and integrity of data transmitted over the API. This subdivision introduces a list of specific security measures.

(1) The purpose of this paragraph is to require software vendors' servers to be hardened to industry best practices. These best practices are not spelled out, as they are commonly known. The intention of this paragraph is not to require specific practices, but rather that software vendors keep up to date on evolving

and current best practices. This paragraph is necessary to ensure the continued security of software vendor servers to protect data sent over the API.

(2) The purpose of this paragraph is to require software vendors' servers to have anti-malware software installed and configured. This subdivision is necessary to ensure software vendors' servers are protected from malware that could compromise data sent over the API.

(3) The purpose of this paragraph is to require two-factor authentication for those who access software vendors' servers. Two-factor authentication is a commonly understood industry term and as such is not defined in these regulations. This paragraph is necessary to prevent unauthorized access to software vendor servers so that the data stored on those servers and transmitted over the API, as well as the software hosted on those servers used to file through the API, are protected.

(d) The purpose of this subdivision is require security log management on its servers and to introduce specific requirements for security log management. This subdivision is necessary to ensure software vendors have the tools to determine whether their servers and software on those servers have been improperly accessed or changed and that they take action to protect against and remedy improper access or changes.

(1) The purpose of this paragraph is to specify that logging must be enabled on all systems and network devices. This requirement is necessary to clarify on which systems and devices logging must be enabled. This logging allows the software vendors to be aware of and remedy access on any systems and devices that may impact their electronic filing system software and/or data sent through the API.

(2) The purpose of this paragraph is to require regular review of logs. This requirement is necessary to ensure that improper activities are noticed and remedied if appropriate.

(3) The purpose of this paragraph is to require that logs be stored separately from monitored systems and protected. This requirement is necessary to ensure that bad actors are not able to hide their improper activities by modifying logs showing the activities they took.

(4) The purpose of this paragraph is to require tools that alert software vendors to improper activities contained in the logs. This requirement is necessary to provide faster notification of potential improper activities.

(5) The purpose of this paragraph is to require the use of multiple time sources in logs. This requirement is necessary to ensure bad actors are not able to manipulate time and date information on software vendor systems and devices to obscure their improper activities.

(e) The purpose of this subdivision is to require reporting of detected unauthorized use or unscheduled unavailability outages on any of its servers hosting their electronic filing system. This requirement only applies to servers under the control of software vendors, not client computers that access or use the electronic filing system. This subdivision is necessary to ensure activities that may affect the integrity of data sent through the API are reported to the SOS so that the SOS can take appropriate action, as necessary.

(f) The purpose of this subdivision is to state that software vendors are not responsible for the security of the systems of filers who use their electronic filing systems. This subdivision is necessary to limit software vendors' responsibility to their own servers and to clarify that this responsibility does not extend to filers.

(g) The purpose of this subdivision is to state that the requirements in this section only apply to software vendors, not filers. This subdivision is necessary to clarify filers' responsibilities for the security of their own servers and other devices used to file through the API using software vendor electronic filing systems.

**23005. System Changes**

(a) The purpose of this subdivision is to require software vendors to keep their electronic filing systems up to date with changes in CAL-ACCESS. This subdivision is necessary to ensure that filings sent through the API continue to be consistent and compliant with evolving laws and regulations related to the Political Reform Act of 1974.

(b) The purpose of this subdivision is to specify the time period by which software vendors need to update their electronic filing systems to represent changed laws and regulations. This subdivision also states that the SOS shall allow reasonable extensions to this time period upon request. This subdivision is necessary to clarify the time period by which software vendors need to make updates and to require the SOS to not unreasonably hold software vendors to this time period.

(c) The purpose of this subdivision is to specify that the SOS may de-certify a software vendor who fails to update their electronic filing system consistent with subdivisions (a) and (b). This subdivision cross-references de-certification procedures in section 23008. This subdivision is necessary to cross-reference de-certification procedures and clarify that they can occur as a result of not implementing system changes.

(d) The purpose of this subdivision is to require software vendors to notify the SOS when they make changes to their electronic filing systems that may affect data moving through the API. This subdivision specifies a time period before the change can be made. This subdivision requires SOS approval before changes are made. This subdivision is necessary to ensure that software vendors do not take actions that may affect data sent through the API without giving the SOS the opportunity to determine whether it will affect data filed in CAL-ACCESS.

**23006. Bugs or Defects**

(a) The purpose of this subdivision is to define "serious bug or defect" as used in this section. This definition is necessary to ensure software vendors are aware of what bugs trigger the requirements in this section and which do not. This section ensures that serious bugs or defects require prompt attention, but the actions needed interfere with filing so they should only be done for serious bugs or defects.

(b) The purpose of this subdivision is to require software vendors to log all serious bugs or defects and provide those logs to the Secretary of State upon request. This subdivision is necessary to ensure software vendors keep a record of serious bugs or defects should that information be needed by the SOS.

(c) The purpose of this subdivision is to require software vendors to report serious bugs or defects in their electronic filing systems to the SOS. This subdivision is only intended to require the reporting of bugs or defects that could affect data sent through the API and filed with CAL-ACCESS. This subdivision gives a one business day time period for reporting such bugs or defects. This subdivision is necessary to ensure data is not filed with CAL-ACCESS that was not intended by the filer. The quick notification period is

necessary so that the SOS can quickly take action related to these bugs or defects to ensure the accuracy and reliability of data presented to the public in CAL-ACCESS.

(d) The purpose of this subdivision is to require software vendors to resolve serious bugs or defects within three business days, or as agreed by the software vendor and the SOS. This subdivision is necessary to ensure serious bugs or defects are remedied in an expedient manner in order to both ensure the accuracy and reliability of data presented to the public in CAL-ACCESS and to allow continued filing by filers using that software vendor's services as quickly as possible.

(e) The purpose of this subdivision is to require software vendors to immediately cease transmission of data through the API upon discovery of serious bugs or defects. This subdivision is necessary to ensure the accuracy and reliability of data presented to the public in CAL-ACCESS.

(f) The purpose of this subdivision is to require software vendors to notify filers using their services about any serious bugs or defects. This subdivision is necessary to ensure filers are aware of potentially incorrect data sent through the API and so that filers are aware that their data transmission is temporarily halted while the bugs or defects are resolved.

**23007. Continued Compliance Verification**

(a) The purpose of this subdivision is to specify that the SOS can implement testing of certified electronic filing systems. This testing can be initiated at the SOS's discretion, and no set time frame is stated for how often testing could occur. This subdivision is necessary to allow the SOS to take steps to ensure data that electronic filing systems remain compliant with these regulations. This discretionary testing is offered in lieu of routine testing due to the nature of CAL-ACCESS and laws and regulations that affect it. Periodic testing may not be necessary if significant portions of CAL-ACCESS remain the same and/or no issues are noticed in data filed through a particular software vendor. However, significant changes to filing requirements and the structure of CAL-ACCESS and/or reported issues with data filed using a specific software vendor's electronic filing system may necessitate testing sooner than a scheduled testing period may allow. This subdivision is intended to balance the integrity of data in CAL-ACCESS filed through the API with the burden on software vendors of this testing.

(b) The purpose of this subdivision is to specify the notification period before SOS begins discretionary testing. This subdivision is necessary to clarify this time period and to protect software vendors from unreasonable testing obligations initiated by the SOS.

(c) The purpose of this subdivision is to specify that discretionary testing shall be of the same type as initial certification testing pursuant to section 23003. This subdivision is necessary to clarify the nature of discretionary testing.

(d) The purpose of this subdivision is to specify resolution measures for issues identified through this discretionary testing. This subdivision is necessary to clarify these procedures.

**23008. Software Vendor De-certification**

(a) The purpose of this subdivision is to state that the SOS may de-certify software vendors only when they fail to resolve compliance issues. This subdivision is necessary to state that de-certification can occur and what it can be based on.

(b) The purpose of this subdivision is to specify a notification period before a software vendor will be de-certified. This subdivision is necessary to clarify that the SOS will not immediately de-certify software vendors. This subdivision protects software vendors from unreasonable cessation of their activities. This subdivision also protects filers using software vendors from having to immediately change their filing activities (such as by choosing a new software vendor or switching to filing directly with CAL-ACCESS) if their software vendor is de-certified.

(c) The purpose of this subdivision is to state that software vendors may remediate issues causing de-certification. This subdivision states the requirements for resolving those issues, referencing section 23006. This subdivision is necessary to clarify that notification of de-certification by the SOS does not prevent software vendors from resolving issues and continuing to file through the API.

(d) The purpose of this subdivision is to state that software vendors may implement system changes pursuant to section 23005 that caused de-certification. This subdivision states the requirements for resolving those issues, referencing section 23005. This subdivision is necessary to clarify that notification of de-certification by the SOS does not prevent software vendors from updating their electronic filing system to come into compliance with current electronic filing specifications.

(e) The purpose of this subdivision is to state that the SOS will not unreasonably de-certify a software vendor. This subdivision is necessary to delineate the protections offered by these regulations to software vendors and to appropriately limit the authority of the SOS.

(f) The purpose of this subdivision is to state that software vendors who have been de-certified may re-apply for certification at any time after de-certification. This subdivision is necessary to clarify that there is no waiting period after de-certification during which a software vendor is prevented from attempting to resume filing through the API, and to prevent the SOS from blacklisting software vendors who have had issues in the past.

## ECONOMIC IMPACT STATEMENT

Government Code section 84602(b)(1) requires the SOS to develop an online filing and disclosure system that, among other criteria, ensures the security of data entered and stored in the system. Government Code section 84602(b)(2) requires the SOS to accept test files from software vendors and others wishing to file reports electronically. These regulations implement those statutory requirements.

Based on the analysis below, the SOS concludes that the adverse or other economic impact, including the ability of California businesses to compete with businesses in other states, will not be significant.

### Creation or Elimination of Jobs within the State of California

It is not anticipated that these regulations will create or eliminate jobs within the State of California. Numerous software vendors already electronically file with the existing CAL-ACCESS system. These regulations provide clarity for how they will continue those activities with the CARS. The new certification process is necessary to ensure compliance with the new

data-driven method for filers to submit required filings, but does not significantly change the relationship between CAL-ACCESS and software vendors.

Creation of New or Elimination of Existing Businesses within the State of California

It is not anticipated that these regulations will create or eliminate existing businesses within the State of California. Numerous software vendors already electronically file with the existing CAL-ACCESS system. These regulations provide clarity for how they will continue those activities with the CARS. The new certification process is necessary to ensure compliance with the new data-driven method for filers to submit required filings, but does not significantly change the relationship between CAL-ACCESS and software vendors.

Expansion of Businesses or Elimination of Existing Businesses within the State of California

It is not anticipated that these regulations will expand businesses or eliminate existing businesses within the State of California. Numerous software vendors already electronically file with the existing CAL-ACCESS system. These regulations provide clarity for how they will continue those activities with the CARS. The new certification process is necessary to ensure compliance with the new data-driven method for filers to submit required filings, but does not significantly change the relationship between CAL-ACCESS and software vendors.

Benefits of the Regulations

The proposed regulations accomplish the mandate of Government Code section 84602 and also furthers the SOS's dedication to making government more transparent and accessible in the areas of elections, business, political campaigning, legislative advocacy, and historical treasures. These proposed regulations protect the integrity of information to the public seeking government information electronically, as well as providing filers with a sound electronic filing process. As a result, this indirectly benefit the general welfare of California. Moreover, the benefits of these regulatory action is that they will provide guidance to the SOS and software vendors by preventing them from being unreasonably decertified as the law or CAL-ACCESS changes, and furthers the purpose of the PRA by ensuring only accurate data is transmitted over the API.

SOS finds that this regulatory proposal does not affect the health and welfare of California, worker safety, and the state's environment because the proposed changes establish a certification process for software vendors who wish to file electronically with CARS through an API that SOS is creating to achieve this electronic filing.