

Date of Hearing: April 9, 2025

ASSEMBLY COMMITTEE ON LOCAL GOVERNMENT

Juan Carrillo, Chair

AB 810 (Irwin) – As Amended March 27, 2025

SUBJECT: Local government: internet websites and email addresses.

SUMMARY: Expands the list of local agencies that are required to use “.gov” or “.ca.gov” domain names for websites and email addresses, and permits community colleges to satisfy these requirements with a “.edu” domain. Specifically, **this bill**:

- 1) Applies the expanded definition in 2), below, to the existing requirement for local agencies to, by January 1, 2029, use a “.gov” top-level domain or a “.ca.gov” second-level domain for an internet website maintained by the agency for use by the public and for public email addresses maintained by the agency for its employees.
- 2) Expands the definition of a “local agency” to include:
 - a) Special districts;
 - b) School districts;
 - c) Joint powers authorities (JPAs); and
 - d) Other political subdivisions.
- 3) Permits community college districts and community colleges to use a “.edu” domain name for their internet websites and email addresses.
- 4) Makes non-substantive technical changes.
- 5) Provides that if the Commission on State Mandates determines that this bill contains costs mandated by the state, reimbursement to local agencies and school districts for those costs shall be made pursuant to Part 7 (commencing with Section 17500) of Division 4 of Title 2 of the Government Code.

EXISTING LAW: Requires cities and counties that maintain websites for use by the public or public email addresses for use by its employees to utilize a “.gov” or “.ca.gov” domain name. Cities and counties must comply with these requirements by January 1, 2029. (Government Code Section 50034)

FISCAL EFFECT: This bill is keyed fiscal and contains a state-mandated local program.

COMMENTS:

- 1) **Bill Summary and Author’s Statement.** This bill adds special districts, school districts, JPAs, and other political subdivisions to the list of local agencies that are required to use “.gov” or “.ca.gov” domain names for internet websites maintained for use by the public and for email addresses maintained for employees. This bill permits community colleges and

community college districts to satisfy these requirements with a “.edu” domain. This bill is sponsored by the author.

According to the author, “The public’s trust in government is foundational for a healthy democracy. With rising levels of misinformation and fraud perpetrated online, and more sophisticated threat actors intending to confuse and mislead, we can no longer be haphazard about how governments are presented online. California’s public agencies should take every effort to safeguard the public’s trust in our institutions, especially when they are recommended and offered free of charge by federal and state authorities. AB 810 requires special districts, school districts, and JPAs to join cities and counties in the transition of their websites and e-mails to the .gov or ca.gov domain, so when Californians look for government information or services, they can know with confidence they are receiving official information.”

- 2) **Domain Names.** A domain name is a simple, easy-to-remember web address that people use to visit a specific website. Computers translate domain names into numerical identifiers called Internet Protocol (IP) addresses. For example, the domain name “google.com” corresponds to the IP address 142.251.32.46, allowing users to access the same website using either method.

Since desirable domain names are limited, a system called the top-level domain (TLD) was developed to expand available options based on categories and geography. The TLD is the final part of a website name, such as “.com” for commercial sites, “.org” for organizations, “.gov” for government entities, and “.edu” for educational institutions.

Domain names are structured into hierarchical fields separated by periods. The field to the farthest right is the TLD. The field to the immediate left of the TLD is the second-level domain, and so on. For example, the domain name for the California Department of Motor Vehicles (DMV) is dmv.ca.gov, where “gov” is the TLD, “ca” is the second level-domain, and “dmv” is the third-level domain. Additional parts of a web address that follow a forward slash (“/”) are called subdirectories. For instance, dmv.ca.gov/portal directs users to a specific section (“portal”) of the DMV website.

- 3) **Cybersecurity and Infrastructure Security Agency and the “.gov” Domain.** The Cybersecurity and Infrastructure Security Agency (CISA) leads the federal government’s effort to understand, manage, and reduce risk to cyber and physical infrastructure. CISA sponsors the “.gov” TLD and makes it available solely to United States-based government organizations and publicly controlled entities, including special districts and school districts. According to CISA, “.Gov exists so that the online services of bona fide U.S.-based government organizations are easy to identify on the internet. Increasing and normalizing its use helps the public know where to find official government information – and where not to.”

Upon receiving a request for a “.gov” domain, CISA uses the U.S. Census Bureau’s criteria for classifying governments to help determine eligibility. CISA may ask the applicant for information such as legislation, a charter, or bylaws to verify eligibility. CISA’s review process can take 30 business days, but may take longer depending on the details of the request and volume of requests CISA is receiving. A “.gov” domain is available without a fee for those that qualify.

According to CISA, using a “.gov” domain increases security in the following ways:

- a) Multi-factor authentication is enforced on all accounts in the “.gov” registrar, which may not be the case for other commercial registrars.
 - b) All new domains are “preloaded.” This requires browsers to only use a hypertext transfer protocol secure (HTTPS) connection with a website. This protects a visitor’s privacy and ensures the content published is exactly what is received.
 - c) A security contact can be added for the domain, making it easier for the public to report potential security issues with the online services.
- 4) **California Department of Technology and the “.ca.gov” Domain.** The mission of the California Department of Technology (CDT) is to “partner with state, local government, and educational entities to advance California’s technology and ensure secure, equitable, and reliable solutions through effective policy and oversight, statewide strategies, and innovative services.”

According to CDT, “In order to extend the use of [the .gov] domain to state and local entities, CISA has delegated the State of California authority to administer the “.ca.gov” second-level domain.” As part of this delegated authority, the Government Operations Agency (GovOps) is responsible for overseeing the “.ca.gov” domain name program and CDT manages the registration, change, and certification process for “.ca.gov” domains.

CDT approval is required for any state entity, city, county, and government group that requests to use the ca.gov web domain. Web domains occupying the “.ca.gov” domain zone must comply with specific requirements similar to those for “.gov” domains. For example, permitted domain names for local agencies such as JPAs and special districts may include the group’s formal full name per their charter or the acronym of the group’s formal full name.

All entities that use the “.ca.gov” internet domain are required to annually re-certify compliance with state and federal policies. The annual re-certification process validates whether the domain(s) are still in use and the domain complies with federal policy and guidelines. The re-certification also confirms that the contact information associated with the domain is still current. Failure to complete the annual re-certification requirement within ten days of the domain’s expiration date may result in removal of the domain name.

- 5) **EDUCAUSE and the “.edu” Domain.** The “.edu” TLD is administered by EDUCAUSE, a nonprofit association whose mission is to advance the strategic use of technology and data to further the promise of higher education. According to the EDUCAUSE website, the .edu domain is one of the seven original top-level subdivisions of the Internet Domain Name System (DNS). The .edu domain is intended for accredited U.S. postsecondary institutions. It is managed under the authority of the United States Department of Commerce, which retains final authority over the membership and operations of the .edu domain. EDUCAUSE administers the .edu domain under a cooperative agreement with the Department of Commerce that requires the approval of both parties in order for substantive changes in domain policies and procedures to take effect.

Under the terms of Amendment 11 of the .edu Cooperative Agreement with the U.S. Department of Commerce, EDUCAUSE is authorized to assess a \$77.00 per year registration fee to recoup the expenses of managing the domain.

- 6) **Cybersecurity for School Districts.** According to CISA, “There is nothing more important than ensuring the safety and security of our schools from physical and cybersecurity threats alike. Unfortunately, adversaries have targeted our Kindergarten to Twelfth (K-12) education system due to the extensive amounts of personal and financial data they maintain about our kids, teachers, school staff and records on the schools themselves. Yet, most educational districts lack the resources to put in place a comprehensive cybersecurity program. So many of our schools across the nation are, what we call, ‘target rich, cyber poor’ in that they are often a frequent target for ransomware and other cyberattacks due to the extensive data kept on school networks, often without the proper protection. For K-12 schools, cyber incidents are so prevalent that, on average, there is more than one incident per school day.”

CISA recommends that schools take steps to enhance their cybersecurity, including implementing multifactor authentication, identifying and fixing known security flaws, performing backups, minimizing exposure to common attacks, developing a cyber incident response plan, and creating a training and awareness campaign.

- 7) **Impact to K-12 public schools.** According to the Assembly Education Committee, “School districts are one type of local educational agency (LEA) that serves kindergarten through grade 12 public school students. Other types of LEAs serving public school students include county offices of education (COEs) and charter schools. It is unclear if the bill also applies to COEs and charter schools.

“LEAs utilize their websites for a number of purposes, but the primary function of a LEA website is to convey information to the public they serve. Information regarding school and LEA boundaries, school calendars, and programs offered often receives the most traffic from users. An LEA is statutorily required to post certain information on their website: two of the most well-known include the LEA’s 3-year plan (also known as the Local Control and Accountability Plan [LCAP]), and information related to filing a complaint (also known as the Uniform Complaint Process [UCP]). As most modes of communication are now provided digitally, rather than through paper and other means, an LEA website is a vital resource for the public school system.

“If this bill were adopted as written, many LEAs report they would be required to abandon their current domain name and find a compliant one. The resulting impact has the potential to be confusing for a community, and particularly for the families served by the LEA. It may take time to transition to a new domain name, and families could be without necessary information for a period of time. Further, with approximately 1,000 school districts, 58 COEs and nearly 1,300 charter schools, it may prove to be challenging finding domain names that are compliant with the bill for all of these LEAs. For example, there are three COEs with names that lend themselves to the same acronym: Alameda COE, Alpine COE, and Amador COE. As a result, their current domain names help to differentiate between the three: www.acoe.org (Alameda COE), www.alpinecoe.k12.ca.us (Alpine COE), and amadorcoe.org (Amador COE). Finally, the impact to this change may be costly for the LEA, and require that the use of already limited funds be directed towards changing domain names that could instead be directed to provide direct resources to students and staff.”

- 8) **State and Local Cybersecurity Grant Program.** Through the Infrastructure Investment and Jobs Act (IIJA) of 2021, Congress established the State and Local Cybersecurity Improvement Act, which established the State and Local Cybersecurity Grant Program

(SLCGP). The SLCGP helps eligible entities address cybersecurity risks and threats to information systems owned or operated by – or on behalf of – state, local, and territorial governments.

Congress appropriated \$200 million for the SLCGP for fiscal year (FY) 2022, \$400 million for FY 2023, \$300 million for FY 2024, and \$100 million for FY 2025. On December 7, 2022, the federal government awarded California \$8 million in first-year funding for the SLCGP. The funds are administered by the California Office of Emergency Services (CalOES) and are required to be allocated according to a Cybersecurity Plan, which was developed by a subcommittee of the California Cybersecurity Task Force called the Cybersecurity Investment Planning Subcommittee. The Cybersecurity Plan was approved by the federal government in September 2023.

80% of total state allocations of the SLCGP must support local governments, who are eligible to apply as subapplicants of CalOES and must work with the Cybersecurity Investment Planning Subcommittee to receive subawards. Local agencies may be awarded up to \$250,000. In 2024, SLCGP awards were received by 95 local and tribal governments, ranging from elementary schools and community colleges to cities and irrigation districts.

The SLCGP has stated that they will be releasing funding opportunities in 2025 and 2026. It is unclear whether federal funding for local agency cybersecurity will be available beyond 2026.

- 9) **AB 1637 of 2023.** AB 1637 (Irwin), Chapter 586, Statutes of 2023, required cities and counties that maintain websites to utilize a “.gov” or “.ca.gov” domain.

On December 16, 2024, the County of Santa Clara filed a test claim with the Commission on State Mandates to seek a decision regarding whether the state must reimburse the costs of implementing AB 1637. According to the test claim, compliance with the mandate requires new activities to be undertaken by employees and third-party professionals working in areas including change management; network, development operations, testing, and security engineering; user experience design; business systems analysis; cloud infrastructure; information security operations; quality assurance; project and change management; solution architecture; and system and application administration. The County must also undertake new activities to inform its employees and the public about its web and email migration, including designing and initiating a public relations campaign; replacing references and links to legacy websites, web applications, and email addresses in the County’s internet resources; and redesigning and reprinting paper documents containing the legacy addresses. As reported in the test claim, the County estimated that the new activities to comply with the mandates will cost the county approximately \$918,868. The County estimated statewide costs for all cities and counties to implement AB 1637 to be \$90.9 million per fiscal year until the compliance deadline of January 1, 2029, resulting in a total statewide estimated cost of \$454.5 million. While the impact to each agency is likely different, it is possible that similar new activities will be required for special districts, school districts, and JPAs to comply with this mandate as were reported in the County of Santa Clara’s test claim. The Commission on State Mandates has not yet made a decision on this test claim, so it is unclear what level of reimbursement will be approved and can therefore be expected for other local agencies.

- 10) **Estimated Costs to Special Districts.** The California Special District’s Association (CSDA), which represents over 1,300 organizations, solicited their members for estimated

compliance costs for this mandate. The estimates ranged widely, from \$6,000 for a small sanitary district with 7 full-time employees, to \$1 million for a large water district. Several estimates fell between \$50,000 and \$100,000. The large water district that estimated \$1 million stated, “The cost of staff and consulting time, replacement of office supplies, staff apparel, promotional items, and rebuild and rebranding effort just to make the transition would be about \$1M. May impact water conservation program which requires active customer engagement.” One large sanitation agency estimated that implementing this mandate would require approximately 2,000 staff hours and \$500,000-\$600,000. One small community services district providing water, wastewater and fire services, serving fewer than 500 customers, estimated a cost of \$20,000-\$25,000 and stated, “Plus, this would add incremental on-going support costs that we do not have today. We may even need to do another rate case to reflect increased operating costs.”

11) **Policy Considerations.** The Committee may wish to consider the following:

- a) **Unique Impact to Schools.** In addition to the technical, financial, and naming redundancy concerns raised by many local agencies, schools have unique challenges due to their distinct role in the community. A coalition of school districts and educational management organizations note that the staff time and financial resources required to implement AB 810 would divert funds away from the classroom—at a time when many schools are already struggling to balance their budgets. Unlike other local governments, schools generally lack the ability to generate their own revenue.

Moreover, the coalition emphasizes that public schools strive to be seen as part of the “community” rather than the “government.” While this bill aims to improve public confidence in local agencies' websites, the coalition argues that it could have the opposite effect for schools. The coalition also notes that, given that students and families rely on schools for a broad range of essential services, any decrease in trust could have serious implications. The Committee may wish to consider these unique impacts on schools as it evaluates this bill.

- b) **Timeline.** When AB 1637 was chaptered in 2023, it gave cities and counties until January 1, 2029, to transition their domains. This bill extends the same domain change requirement to special districts, school districts, JPAs, and other political subdivisions—but with the same January 1, 2029, deadline. As a result, these local agencies effectively have two fewer years to comply than do cities and counties. The Committee may wish to consider whether the local agencies added by this bill would benefit from additional time to complete the transition.
- c) **Too Soon to Expand the Scope?** When AB 1637 was heard in this committee just two years ago, it applied to counties, cities (including charter cities), towns, schools districts, municipal corporations, districts, political subdivisions, boards, commissions, and other local agencies, but was later amended in the Assembly Appropriations Committee to only apply to cities and counties. While some cities and counties have begun the process of implementing AB 1637, the full scope of the transition’s effects cannot yet be evaluated. The Committee may wish to consider whether the Legislature would benefit from additional time to evaluate the effects of AB 1637 before requiring additional entities to meet these mandates.

12) **Committee Amendments.** In order to address some of the policy considerations raised above, the Committee may wish to consider the following amendments:

- a) Removing school districts from the list of local agencies required to comply with the bill's mandates.
- b) Extending the compliance deadline to January 1, 2031 for special districts, JPAs, and other political subdivisions, not including K-12 public school districts.

13) **Previous Legislation.** AB 1637 (Irwin), Chapter 586, Statutes of 2023, required cities and counties that maintain websites for use by the public or public email addresses for its employees to utilize a ".gov" or ".ca.gov" domain name.

SB 929 (McGuire), Chapter 408, Statutes of 2018, required all independent special districts, with certain exceptions, to maintain a website.

14) **Arguments in Support.** None on file.

15) **Arguments in Opposition.** The California Special Districts Association (CSDA), Association of California Water Districts (ACWA), and California Association of Recreation and Park Districts (CARPD), state, "We remain deeply concerned about the added costs associated with migrating to a new domain and corresponding email addresses, the confusion that will be created by forcing a new website to be utilized, and the absence of any resources to better assist local agencies with this mandate.

"While applying for and obtaining a .gov domain requires no fees, there are significant costs that an agency must budget for to recode, implement the corresponding e-mail and network login changes, single sign on/multi-factor authentication, encryption keys, revising and redesigning website URLs, and updating public materials, social media, and external entities.

"In addition to the fiscal impacts, special district public outreach would be affected by this bill... Special districts intentionally undertake public awareness and outreach campaigns to reduce uncertainty around jurisdictional boundaries and improve familiarity with provided services. AB 810 would require special districts opting for a ca.gov domain to observe the website naming conventions established by the California Department of Technology... Unfortunately ... various special district outreach websites would be subject to rejection, hindering those outreach programs.

"Compounding these concerns is the fact that special districts, like school districts, are more numerous than cities or counties; the potential for conflicts due to sharing similar names or initialisms is increased with the larger population of special districts, which may result in special districts adopting website URLs that are further removed from their previously established identities.

"Finally, it is important to note that Assembly Bill 1637 (Chapter 586, Statutes of 2023), the legislation that established these website requirements for cities and counties, provided those types of agencies with over five years' time to bring their websites and emails into compliance. AB 810 instead would provide special districts, school districts, joint powers authorities, or other political subdivisions with approximately three years to bring their websites into compliance."

A coalition of school districts and educational management organizations state, “Due to the substantial workload imposed upon districts by this bill, it will pull away the very limited number of IT staff available to our schools. The sheer number of hours and staff time needed to implement the provisions of AB 810 reduces the technology department’s ability to assist other departments – many of which ensure students’ access to educational content and quality instruction.

“To that end, we would point out that AB 810 provides no funding mechanisms to help school agencies implement the provisions of the bill. At a time when many of our schools are already struggling to balance their local budgets, AB 810 would impose yet another unfunded mandate that will siphon dollars away from the classroom where they belong. Furthermore, based on the .gov program parameters it is not clear if schools are eligible to access the limited resources currently available through federal and state programs that provide either direct resources or technical assistance.

“School community members are facing deep fears about the actions of government agencies; to the point of not sending their students to school when there is reported activity by federal immigration agents... We contend that shifting school domains to “.ca.gov” or “.gov” would have the opposite impact of the stated goal of the bill and would in fact decrease trust between us and our local families.

“In addition, schools have the added burden of providing student email addresses. While AB 810 would only apply to employee email addresses this means LEAs will have to maintain two separate domains in order to provide the “.gov” address to employees and the current or alternative domain for student emails. Providing students, who are minors, with “.gov” emails draws out many potential scenarios that run counter to cybersecurity best practices.”

16) **Double-Referral.** This bill is double-referred to the Assembly Committee on Privacy and Consumer Protection.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

Alameda County Office of Education
 Association of California School Administrators
 Association of California Water Agencies
 California Association of Recreation & Park Districts
 California Association of School Business Officials
 California County Superintendents
 California It in Education
 California School Boards Association
 California Special Districts Association
 El Dorado Irrigation District
 Kern County Superintendent of Schools Office
 Los Angeles County Office of Education

Los Angeles Unified School District
Office of the Riverside County Superintendent of Schools
San Joaquin County Office of Education
Solano County Water Agency
Water Replenishment District of Southern California
California Central Valley Flood Control Association (unless amended)
Desert Water Agency (unless amended)

Analysis Prepared by: Julia Mouat / L. GOV. / (916) 319-3958