Date of Hearing:

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 1637 (Irwin) – As Amended March 16, 2023

As Proposed to be Amended

SUBJECT: Local government: internet websites and email addresses

SYNOPSIS

This bill would require local governments to ensure that their public-facing internet websites and email addresses use a ".gov" or ".ca.gov" domain name, no later than January 1, 2026.

It would have been helpful for internet cybersecurity if government entities had been legally required to take this step decades ago. Unfortunately, these requirements were not placed into law, meaning that there has been a proliferation of local government entities using .com, .net, and .org addresses.

The problem is that it is a trivial matter for a fraudulent actor to obtain a domain name that is similar to that of an existing local governmental agency, also using a non-.gov top level domain, and set up a fake website at that domain. If its content is sufficiently similar to a real website, search engines may pick up the fake website and display it when people search for the entity.

Because so many local governmental entities don't have .gov domain names, visitors have no reason to be suspicious of such domains; moreover, there is no quick, convenient way for users to verify the authenticity of the website they are visiting. A fake website that lures in real users who believe they are visiting a legitimate government website could then lure those users into sharing personal information, making payments, and conducting other compromising activities. A fake site could also spread misinformation, such as providing erroneous dates and addresses for voting sites or touting the supposed dangers of vaccines.

As discussed below, there are undoubted cybersecurity benefits from requiring the use of .gov or .ca.gov domain names. Transition difficulties could be addressed by a state-level help desk, perhaps housed at the California Department of Technology.

The bill is author-sponsored. It is opposed by the City Clerks Association of California and two California cities. A coalition of six local government associations, including the California Special Districts Association and the League of California Cities, have taken an "oppose unless amended" position on the bill.

This bill previously passed the Assembly Local Government Committee on a 5-0-2 vote.

SUMMARY: Requires California local agencies that maintain websites and email addresses accessible to the public to utilize a ".gov" or ".ca.gov" domain no later than January 1, 2026. Specifically, **this bill**:

1) Requires, no later than January 1, 2026, any local agency that maintains an internet website for use by the public to ensure that the internet website utilizes a ".gov" top-level domain or a ".ca.gov" second-level domain.

2) Specifies that if a local agency currently maintains an internet website for use by the public that does not comply with 1) above by January 1, 2026, then that local agency shall redirect that internet website to a domain name that does comply with 1) above.

3) Requires, no later than January 1, 2026, a local agency that maintains public email addresses for its employees to ensure that each email address provided to its employees utilizes a ".gov" domain name or a ".ca.gov" domain name.

4) Defines "local agency" to mean a county, city, whether general law or chartered, city and county, town, school district, municipal corporation, district, political subdivision, or any board, commission or agency thereof, or other local public agency.

5) Makes findings and declarations in support of the foregoing.

EXISTING LAW:

1) Establishes the California Department of Technology in the Government Operations Agency (GovOps). (Gov. Code § 11545.)

2) Requires every independent special district to maintain an Internet website, though provides an exemption for hardship such as inadequate broadband availability, limited financial resources, or insufficient staff resources. (Gov. Code § 53087.8)

FISCAL EFFECT: As currently in print this bill is keyed fiscal.

COMMENTS:

1) **Need for this bill.** When you type a URL like https://www.assembly.ca.gov into a Web browser or email someone at an address such as first.last@asm.ca.gov, you are implicitly relying on the internet's domain name system (DNS). The DNS is based on computers, called domain name servers, distributed throughout the global internet to translate human-readable domain names like "assembly.ca.gov" and "asm.ca.gov" into numeric Internet Protocol (IP) addresses. Once the numeric IP address is acquired, data sent on the internet to a particular domain (such as "asm.ca.gov") can be routed to the computer or network where it is meant to be delivered.

The top-level domain ".gov" was originally meant to be used by federal, state, and local government entities. The other original top-level domains each had their own particular functions: ".com" was meant for commercial use; ".org" was for nonprofits; ".edu" was for institutions of higher education; "net" was for internet service providers and other entities providing network infrastructure; and ".mil" was for the U.S. Department of Defense (DOD). Since then, a plethora of other top-level domains have emerged, such as ".info," ".biz," and even ".beer." Some of the original domain requirements remain strictly enforced; no one but the DOD can get a ".mil" domain, and it is difficult for non-educational institutions to obtain an ".edu" domain. Other requirements have not been strictly enforced; anyone can quickly obtain a ".com," ".net," or ".org" domain (to say nothing of ".beer") if it is available.

It would have been helpful for internet cybersecurity if government entities had been legally required to obtain .gov domain names decades ago. Unfortunately, these requirements were not placed into law, meaning that there has been a proliferation of local government entities using .com, .net, and .org addresses. In part, this is because the process for obtaining a .gov domain can

be a bit time-consuming (because the applicant must verify that it is actually a governmental entity), whereas a .com, .net, or .org, domain can be obtained in minutes.

As a result, we now live in a world where the Los Angeles Unified School District uses the domain "lausd.net," the Metropolitan Water District of Southern California uses the domain "mwdh20.com," and the City of Norwalk uses the domain "norwalk.org." Many other local governments have also foregone .gov domains for these quicker-to-obtain alternatives.

The problem is that it is a trivial matter for a fraudulent actor to obtain a domain name that is similar to that of an existing local governmental agency, also using a non-.gov top level domain, and set up a fake website at that domain. If its content is sufficiently similar to a real website, search engines may pick up the fake website and display it when people search for the entity. Take, for example, Los Angeles Unified School District's "lausd.net" domain. According to the author, as of March 2023, "la-usd.net," "la-usd.org," and "lausdca.org" were all available on GoDaddy, a popular, low-cost domain name registrar; each of these would be easy options for setting up a fake L.A. Unified website.

Because so many local governmental entities don't have .gov domain names, visitors have no reason to be suspicious of such domains; moreover, there is no quick, convenient way for users to verify the authenticity of the website they are visiting. A fake website that lures in real users who believe they are visiting a legitimate government website could then lure those users into sharing personal information, making payments, and conducting other compromising activities. A fake site could also spread misinformation, such as providing erroneous dates and addresses for voting sites or touting the supposed dangers of vaccines.

In response, this bill would require local governments to ensure that their public-facing internet websites and email addresses use a ".gov" or ".ca.gov" domain name, no later than January 1, 2026.

The requirements of this bill would apply to any county, city, whether general law or chartered, city and county, town, school district, municipal corporation, district, political subdivision, or any board, commission or agency thereof, or other local public agency.

2) **Author's statement.** 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 1637 requires local agencies to transition 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.

3) **How local governments can obtain .gov and .ca.gov domains.** The Cybersecurity and Infrastructure Security Agency (CISA), part of the U.S. Department of Homeland Security, leads the federal government's effort to understand, manage, and reduce risk to cyber and physical infrastructure. In 2020, administration of the .gov domain program was transferred from the federal General Services Administration to CISA. ".gov" has been reserved for U.S.-based

government organizations and publicly controlled entities. This includes state, tribal, interstate, independent intrastate, city, and county governments. If a local government wishes to obtain a .gov domain, it may follow the instructions available at https://get.gov/registration/requirements/.

The California Department of Technology (CDT) administers the .ca.gov second-level domain. ".ca.gov" may be used by any state entity, county, city, state-recognized tribal government, Joint Powers Authority, or independent local district within the State of California. If a local government wishes to obtain a .ca.gov domain, it can use CDT's Domain Name Request System, available at https://domainnamerequest.cdt.ca.gov/.

There is no annual fee associated with a .gov or .ca.gov domain name.

4) **The contested aspects of this measure are largely in other Committees' jurisdictions.** Most of the opposition's arguments raise issues that lie in other Committees' jurisdictions. For example, the City Clerks Association of California writes, "Switching our website and email addresses would create an unnecessary, costly issue for cities and would direct public resources away from serving residents in other ways. This unfunded mandate is not the best use of limited local resources during a time of fiscal instability and uncertainty." The question of whether this measure would be a worthwhile use of local government resources is a topic for the Assembly Local Government Committee, which heard and passed the bill last week.

.If passed by this Committee, the bill will next be heard by the Assembly Appropriations Committee, which will consider its costs. Accordingly, the sole focus of this Committee's analysis are the bill's impacts on cybersecurity.

5) **What are the benefits of this measure for cybersecurity?** As discussed above under "Need for this bill," the main benefit of this measure will be to ensure that members of the public know that when they access a California local governmental website with an internet address ending with ".gov" or ".ca.gov," or email a government employee at such an address, that they are not going to be the victim of a hacker's fake website.

While it is of course possible for a ".gov" or ".ca.gov" website to be hacked, this is much more difficult than setting up a fake website using a ".org" or ".net" top-level domain. Moreover, as noted in the Assembly Local Government Committee analysis:

> Using a ".gov" domain increases security in the following ways:
>
> a) Multi-factor authentication is enforced on all accounts in the ".gov" registrar, which is different than 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 on the website] 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.
>
> Eligibility for a ".gov" domain is attested through a letter signed by the public agency. CISA reviews the letter, may review or request founding documentation, and may review or request additional records to verify the public agency's claim that they are a United States based

> government organization. There are requirements for choosing a name, and activities that are required and prohibited, among others, for local governments. Requests from non-federal organizations are reviewed in approximately 20 business days, but may take longer in some instances.

The City Clerks Association of California objects on the grounds that public trust could be weakened during the transition to the new domain, writing:

> [T]he impacts of the measure go beyond websites and email addresses to include the need to convert all public facing branding, including fleets, outreach, materials, ballots, etc. While these do have natural turnover, waiting to transition current supply could take many years and create confusion in branding and ultimately compromise the trust of the public. Although the measure allows for website redirection, this only adds to the confusion as residents are redirected from our current website, the one they have checked for many years, to a new landing page that wouldn't comport to the addresses on public facing material. The result could compromise local communities' trust in their local leaders and would only add to the frustration in transparent and user-focused government administration.

But this issue—potential resident confusion during the transition to a .gov domain—will never go away. It always take time and money to migrate to a .gov or .ca.gov domain. To accept this as a reason not to make the transition would mean never making the transition.

6) **How burdensome is it to migrate domains to .gov and .ca.gov?** Local governments report vast discrepancies as to the time, effort, and expense required to transition to using ".gov" and ".ca.gov" domains.

The Chief Information Officer of Ventura County (population 847,000) was asked by the author to provide feedback on what this bill would require, as the county uses a "ventura.org" domain name. He responded that the county operates over 70 websites that use the "ventura.org" domain name. Here is how he explained the migration process:

> We would start with our home site and once that is complete, move to the others.
>
> 1. [C]lone the site
> 2. [M]ass change all ventura.org references to the new .gov name
> 3. Internal test for some weeks
> 4. Add Domain to DNS (local and outside)
> 5. Redirect .org to .gov. Both sites kept in synch and both active.
> 6. Press release
> 7. Decommission .org site.
>
> [Ventura County's hosting provider] can convert a site very quickly (hours). A small number of days to convert all our sites.
>
> Only one [full time employee] would be required in addition to [the hosting provider's] efforts…with some misc support for less than a week for the technical efforts. This is within our budget.

By contrast, an opposition coalition consisting of six local government associations reports:

> [O]ne large local government that recently went through the process of migrating to a .gov domain required 15 full-time information technology professionals and over 14 months to complete the project. This included changing all websites, web applications, emails, and active directory accounts for over 12,000 employees and contractors–a considerable endeavor and exactly what is required, should AB 1637 be enacted as currently drafted. One suburban local government ran preliminary estimates that suggested that the costs for migration to .gov could range from $750,000 to $1 million. Another large urban local government itemized costs of about $6.3 million and anticipates that most of the work that would be required would have to be completed by contract labor due to the large number of high-priority projects that information technology staff are currently completing.

Given these discrepancies, one wonders if there is some fundamental misunderstanding as to what is required to implement this bill. Perhaps there are easy steps that could be taken by all, or most, local governments to facilitate an efficient transition to a .gov domain.

To that end, one possible amendment discussed by the author would be to set up help desk functionality at an appropriate state agency in order to provide technical assistance and advice on best practice to local governments transitioning to .gov and .ca.gov domains. A state-level help desk could possibly be paid for through federal grant funding. According to the author, the bipartisan Infrastructure Investment and Jobs Act (Pub. L. 117-58) created the State and Local Cybersecurity Grant Program (SLCGP), which allocated $1 billion over four years to states for cybersecurity initiatives, with a requirement of 80% pass through to local governments. It may be possible for an SLCGP grant to fund a state-level help desk, perhaps housed at CDT. According to the author, total SLCGP grant funding for California could amount to $50 million over the four years. More information about the SLGCP can be found at https://www.cisa.gov/sites/default/files/publications/SLCGP_FAQ-FINAL_508c.pdf; migration to a .gov domain is among the seven best practices listed therein.

7) **Committee amendment—extending implementation deadline by one year.** The bill in print would have required migration to a ".gov" or ".ca.gov" domain by January 1, 2025. An amendment agreed upon in the Assembly Local Government Committee permits local government agencies an additional year to comply with this measure, as follows:

> **Government Code 50034.**
>
> (a) (1) No later than January 1, ~~2025~~ ***2026,*** a local agency that maintains an internet website for use by the public shall ensure that the internet website utilizes a ".gov" top-level domain or a ".ca.gov" second-level domain.
>
> (2) If local agency that is subject to paragraph (1) maintains an internet website for use by the public that is noncompliant with paragraph (1) by January 1, ~~2025~~ ***2026,*** that local agency shall redirect that internet website to a domain name that does comply with paragraph (1).
>
> (b) No later than January 1, ~~2025~~ ***2026***, a local agency that maintains public email addresses for its employees shall ensure that each email address provided to its employees utilizes a ".gov" domain name or a ".ca.gov" domain name.

8) **Related legislation.** SB 386 (Newman, 2023), as originally introduced, would have required a county elections internet website to have a .gov domain. That provision has been amended out of the bill. Status: Senate Appropriations.

SB 929 (McGuire, Chap. 408, Stats. 2020) required every independent special district to maintain an internet website by January 1, 2020, but permitted a hardship exemption for districts without sufficient resources or broadband connectivity.

AB 1344 (Feuer, Chap. 692, Stats. 2011) required all local agencies that have a website to post their meeting agendas on the website 72 hours in advance.

ARGUMENTS IN OPPOSITION: A coalition of six local government associations, including California Special Districts Association and League of California Cities, summarizes its opposition to the bill:

> While we appreciate the intended goal of this measure and the perceived benefits that some believe utilizing a new domain may provide, we remain deeply concerned about the added costs associated with migrating to a new domain and corresponding email addresses; 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 proposed migration.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Oppose unless Amended

Association of California School Administrators
California Special Districts Association
California State Association of Counties (CSAC)
League of California Cities
Rural County Representatives of California (RCRC)
Urban Counties of California (UCC)

Opposition

City Clerks Association of California
City of Redwood City
City of San Marcos

Analysis Prepared by: Jith Meganathan / P. & C.P. / (916) 319-2200