Date of Hearing: April 22, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 810 (Irwin) – As Amended April 10, 2025

SUBJECT: Local government: internet websites and email addresses

SYNOPSIS

The internet has enabled the widespread dissemination of information, which governments have leveraged to expand access to programs and keep constituents informed about local events. However, a major challenge remains: ensuring that the information people find online is accurate and trustworthy. To address this, the federal government uses ".gov" and California state government entities use ".ca.gov" domain names, which not only signal legitimacy but also come with built-in cybersecurity protections.

Despite this, not all government agencies are required to use these domains. As a result, many local government entities have adopted alternative domain types such as ".com," ".net," or ".org." This inconsistency has created opportunities for fraudulent actors to register similar-looking domain names, potentially misleading users into sharing personal information, making payments, or consuming false information.

To mitigate this risk, AB 1637 (Irwin, Ch. 586, 2023) was enacted, requiring cities and counties to transition their websites to ".gov" or ".ca.gov" domain names by January 1, 2029, ensuring users can more confidently access authentic government websites.

This author-sponsored bill would, by January 1, 2031, expand that requirement to include special districts, joint powers authorities, and other political subdivisions. The bill allows community colleges and community college districts to continue using ".edu" domains and exempts K–12 school districts. The bill is opposed by a coalition of water districts and the City of Garden Grove.

This bill previously passed the Assembly Local Government Committee on a 9-1 vote.

THIS BILL:

1) Requires, no later than January 1, 2031, a special district, joint powers authority, or other political subdivision that maintains a public internet website to use a ".gov" top-level domain or a ".ca.gov" second-level domain.

2) Requires a special district, joint powers authority, or other political subdivision that maintains an internet website that does not comply with 1) after January 1, 2031 to redirect that internet website to a domain name that does use a ".gov" top-level domain or a ".ca.gov" " second-level domain.

3) Requires a special district, joint powers authority, or other political subdivision that maintains public email addresses for its employees to ensure that each email address

provided to its employees uses a ".gov" domain name or a ".ca.gov" second-level domain no later than January 1, 2031.

4) Permits a community college district or community college to use an ".edu" domain name in place of a ".gov" top-level domain or a ".ca.gov".

5) Exempts K-12 public school districts.

EXISTING LAW:

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

2) Requires a local agency – defined as a city, county, or city and county – that maintains an internet website for use by the public to utilize a ".gov" top-level domain or a ".ca.gov" second-level domain by January 1, 2029. (Gov. Code § 50034)

3) Requires that a local agency that maintains public email addresses for its employees ensure that each email address provided to its employees utilizes a ".gov" domain name or a ".ca.gov" domain name January 1, 2029. (Gov. Code § 50034)

4) Requires a local agency that maintains an internet website for use by the public that does not have a ".gov" top-level domain or a ".ca.gov" to redirect that internet website to a domain name that does use a a ".gov" top-level domain or a ".ca.gov" second-level domain no later than January 1, 2029. (Gov. Code § 50034)

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

COMMENTS:

1) **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 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) **The Need for this Bill.** Last session, the author carried AB 1637, which required city and county government websites to use the ".gov" or ".ca.gov" domain address. This bill would expand this requirement to include special districts, joint powers authorities, and other political subdivisions, except for K-12 school districts..

When one types a URL like https://www.assembly.ca.gov into a Web browser or emails someone at an address such as first.last@asm.ca.gov, they 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 a ".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 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 Sacramento-Yolo Mosquito and Vector Control District uses the domain "fightthebite.net," the Metropolitan Water District of Southern California uses the domain "mwdh2o.com," and the Golden Gate Bridge Highway and Transportation District uses the domain "goldengate.org." Many other local government agencies 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 similar domain names 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, Metropolitan Water District of Southern California's "mwdh2o.com" domain. A search on GoDaddy, a popular, low-cost domain name registrar, revealed that "mwd-h2o.com", "h2omwd.com", and "mwdh2o.org" were available. Each could be an easy way to set up a fake Metropolitan Water District of Southern California 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 special districts, joint powers authorities, and other political subdivisions, except for K-12 school districts, to ensure that their public-facing internet websites

and email addresses use a ".gov" or ".ca.gov" domain name, no later than January 1, 2031. Under the circumstances that a local government entity already has a website, this bill would require that the original website redirect users to the mandated ".gov" or "ca.gov". This would ensure that there is no confusion over which website is official for an agency. Community college districts and community colleges may satisfy this requirement using ".edu" domain names.

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. The ".gov" domain 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. The ".ca.gov" domain 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 Elsinore Valley Municipal Water District writes:

> The proposed requirement would be costly to implement. Although changing a domain name may seem simple, in practice it involves updating all public-facing digital and printed materials, migrating employee email systems, coordinating with external vendors, retraining staff, and conducting public outreach. These tasks come with a substantial cost that would ultimately be passed on to local ratepayers.

The question of whether this measure would be a worthwhile use of local government resources for the Assembly Local Government Committee, which heard and passed the bill on a 9-1 vote.

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

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 California Special Districts Association, Association of California Water Agencies, and California Association of Recreation and Park Districts in a coalition letter objects on the grounds that the transition could be difficult because the domain name change may be very different from the current domain, writing:

> Compounding [our] concerns is the fact that special 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. Special districts opting for a .gov domain are also not guaranteed requests for their organization's initials or an abbreviated name; districts are similarly admonished that only federal agencies can request generic terms, and URLs must include California's two-letter state abbreviation or clearly spell out the state name unless city or county exceptions apply.

However, as noted above, similar domain names remain readily available and can be used to deceive or scam individuals within special districts. This transition to standardized domains should also serve to make domain names more intuitive and clearly tied to the purpose of the special district. For example, while "fightthebite.net" used by the Sacramento-Yolo Mosquito and Vector Control District is snappy, it does not clearly convey that it represents a legitimate government agency. Under current rules for ".gov" domains, names must "[r]elate to your organization's name, location, and/or services."[1] This requirement would help ensure that the new ".gov" domains established under this bill are both recognizable and relevant to the jurisdictions they represent. Lastly, this bill requires the redirection of users from previous web

[1] Information regarding ".gov" domain rules can be found at https://get.gov/.

addresses to the new ".gov" or ".ca.gov" domains, meaning that the original website would no longer be in use nor accessible, which should dispel any confusion regarding which website is real or correct.

ARGUMENTS IN SUPPORT: None on file.

ARGUMENTS IN OPPOSITION: In opposition to the bill, the City of Garden Grove writes:

> While we appreciate the intended goal of this measure and the perceived benefits that 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, 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. Local agencies, including cities and counties, across the state have worked hard to establish reliable websites that are known and trusted by the communities they serve. AB 810 will result in confusion and compromise local communities' trust in their local leaders, creating frustration in administering a transparent and user-focused government website.
>
> Additionally, 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. The cost of staff and consulting time and rebranding efforts just to make the transition have been identified as major cost drivers by public agencies. One larger agency has relayed that its tentative estimated costs to implement the transition called for in AB 810 would be between $500,000 to $600,000, plus an added 2,000 staff hours.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file.

Opposition

Association of California Water Agencies
California Association of Recreation & Park Districts
California Special Districts Association
City of Garden Grove
El Dorado Irrigation District
Elsinore Valley Municipal Water District
Inland Empire Utilities Agency
Kern County Superintendent of Schools Office
Solano County Water Agency
Water Replenishment District
Water Replenishment District of Southern California

Oppose Unless Amended

California Central Valley Flood Control Association

Analysis Prepared by: John Bennett / P. & C.P. / (916) 319-2200