Date of Hearing: April 19, 2023

ASSEMBLY COMMITTEE ON LOCAL GOVERNMENT
Cecilia Aguiar-Curry, Chair
AB 1637 (Irwin) – As Amended March 16, 2023

SUBJECT: Local government: internet websites and email addresses.

SUMMARY: Requires local agencies that maintain websites to utilize a ".gov" or ".ca.gov" domain. Specifically, **this bill**:

1) Requires, no later than January 1, 2025, a 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 local agency that is subject to 1) above, maintains an internet website for use by the public that is noncompliant with 1) above, by January 1, 2025, 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, 2025, 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) Contains findings and declarations to support its purposes, including that this bill address a matter of statewide concern and is not a municipal affair as that term is used in Section 5 of Article XI of the California Constitution. Therefore, Section 1 of this bill adding 50034 to the Government Code applies to all cities, including charter cities.

6) Provides that no reimbursement is required by this bill because a local agency or school district has the authority to levy service charges, fees, or assessments sufficient to pay for the program or level of service mandated by this bill.

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

COMMENTS:

1) **Bill Summary and Author's Statement.** This bill requires local agencies that have a website or maintain public email addresses for their employees, by January 1, 2025, to utilize a ".gov" or a ".ca.gov" domain. This bill also requires a local agency that maintains an internet website that is noncompliant with the requirement to utilize a ".gov" or ".ca.gov" domain to redirect that internet website to a domain name that does utilize a ".gov" or ".ca.gov" domain. The requirements of this bill 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. 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 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."

2) **Cybersecurity and Infrastructure Security Agency.** According to the Department of Homeland Security, 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 is working to do the following:

   a) Build national critical infrastructure resilience against a growing array of complex threats.

   b) Mobilize risk management efforts around securing the critical infrastructure.

   c) Coordinate national efforts to defend federal and non-federal networks against malicious cyber activity.

   CISA works with a range of federal, state, local, tribal, territorial, private sector, and international partners to foster information sharing and collaboration to address risks. CISA uses its domain expertise and delivers regional, national, and enterprise services to stakeholders to help them secure the cyber, physical, and communications critical infrastructure against a dynamic threat environment.

   According to CISA, "'.gov' is a 'top-level domain', or TLD, similar to '.com', '.org', or '.us'. Enterprises use a TLD to register a domain name (often simply called a domain) for use in their online services, like a website or email. In many well-known TLDs, anyone can register a domain for a fee, and as long as they pay there are not many questions asked about whether the name they chose corresponds to their real-life name or services. While this can be a useful property for creative communication, it can also make it difficult to know whether the people behind a name are really who they claim to be."

   CISA sponsors the ".gov" TLD and makes it available solely to United States based government organizations and publicly controlled entities. A ".gov. domain is available without a fee for those that qualify. 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 you publish 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.

3) **Department of Technology.** According to the California Department of Technology (CDT), "CDT leads the state's drive to deliver clear, fast, dependable, and equitable public services. It provides for the delivery of digital government services through the oversight of statewide IT strategic planning, project delivery, procurement, policy and standards, and enterprise architecture. CDT is tasked with securing statewide information assets by providing oversight and infrastructure for many state departments and serves as the custodian of information for mission-critical and essential business applications. Home to the State Data Center, CDT provides infrastructure services for government customers that include on-premises and cloud-based services. CDT is leading statewide broadband planning and execution to deliver digital equity and reliability for all Californians. The Director of CDT is also the State Chief Information Officer (CIO), and advises the Governor on the strategic management and direction of the state's IT resources and policies."

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.

4) **Local Agency Websites.** As technology advances, the Legislature often amends statutes to capture these advancements and take advantage of any potential public benefits. For example, the Brown Act requires all local agencies to post the agenda for any regular meeting 72 hours in advance in a location that is freely accessible to the public. The agenda must clearly specify the meeting's time, location, and the topics that will be deliberated. Despite this requirement, a local agency's constituents still have to know when the agency plans to meet, where the agenda is posted, and physically travel to the location where the agenda is posted or contact the agency directly to discover what topics the agency is planning to discuss. With the proliferation of Internet access and local agencies utilizing this tool to communicate with their constituents, AB 1344 (Feuer), Chapter 692, Statutes of 2011, required all local agencies that have a website to post their meeting agendas on the website 72 hours in advance, effectively making the agenda more accessible to the public by taking advantage of advancements in technology. Additionally, SB 272 (Hertzberg), Chapter 795, Statutes of 2015, and AB 2040 (Garcia), Chapter 894, Statutes of 2014, required local agencies to post on their websites a list of the agency's enterprise systems and the agency's employee compensation report, respectively.

Additionally, in order to spur special districts to create and maintain a website, SB 929 (McGuire), Chapter 408, Statutes of 2018, required every independent special district, by January 1, 2020, to maintain a website. However, in recognition that California's special districts come in many shapes and sizes, SB 929 allowed for those districts that do not have

sufficient resources or broadband connectivity to adopt a resolution declaring a specific hardship to obtain an exemption. Also, understanding that circumstances change, SB 929 required a district to renew the hardship resolution annually in order to qualify for the exemption.

5) **Policy Considerations.** The committee may wish to consider the following:

   a) **Cost vs. Benefit.** Concerns have been raised by a coalition of local agencies stating that, "While applying for and obtaining a .gov domain has no fees, there are significant costs that an agency must budget for to recode, establish corresponding e-mail, and network login changes, single sign on/multi-factors authentication, encryption keys, revising and redesign website/url links, updating social media and external entities. All of these costs are increased two-fold to co-exist both the previous and newly acquired domains." The coalition of local agencies offer a few examples of the costs associated with complying with AB 1637's requirements, including one large urban local government anticipating costs of $6.3 million. The opposition also identifies a few instances of websites using the ".gov" domain being compromised in recent years, including BART.gov, OaklandCA.gov, USMarshals.gov, FBI.gov, and the California Department of Finance's website.

      However, the author has offered arguments in response, stating:

      i) "That multi-year federal funding for state and local cybersecurity is already being awarded. The State and Local Cybersecurity Grant Program (SLCGP) awarded California $9 million in FY'22 with federal amounts likely to total $50 million over the 4 year program. Additional state matching fund requirements, increasing year over year (10% up to 40%), will also bring more state funds to the table to achieve local cybersecurity goals. The SLCGP requires certain critical activities of local agencies, this includes the transition to the .gov."

      ii) "While registering a .gov domain does provide additional technical protections to some vulnerabilities — namely domain name service (DNS) attacks which involves the credentials of domain administrator being stolen and the website being rerouted to a malicious website— it does not protect against every vulnerability. The author's office doesn't contend the .gov to be a silver bullet. It is only one of the 16 required elements of the SLCGP State Cybersecurity Plans. The hacks mentioned in the letter were not even related to these public agencies' domain names. The threat vectors of those attacks are listed below, but none of them were DNS attacks, they were almost entirely ransomware attacks which encrypted the agencies systems. This made their websites unavailable to the public because everything on their network was encrypted and unavailable for the DNS service to pull from to display a webpage, the equivalent of unplugging the server."

      In light of the differing points of view between the author and the opposition coalition, the committee may wish to consider if this bill strikes the right balance between the potential cost to local agencies and the benefits of the additional security provided to the local agencies and their constituents.

b) **Timeline.** The size and sophistication of local agencies varies widely in California. Some have budgets that range in the billions of dollars to as little as tens of thousands. The opponents argue that while this bill could require local agencies to shift resources away from critical services, smaller, and often rural, areas do not have sufficient resources to redirect staff and funding. The Committee may wish to consider if this bill provides sufficient time for all local agencies to comply with its requirements.

6) **Committee Amendments.** In order to address the above policy considerations, the Committee may wish to amend the bill as follows:

50034. (a) (1) No later than January 1, **2026** ~~2025~~, 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 **a** 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, **2026** ~~2025~~, that local agency shall redirect that internet website to a domain name that does comply with paragraph (1).
(b) No later than January 1, **2026** ~~2025~~, 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.
(c) For purposes of this section, "local agency" has the same meaning as that term is defined in Section 54951.

Due to timing constraints, these amendments should be adopted in the Privacy and Consumer Protection Committee.

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

8) **Arguments in Opposition.** According to a coalition of local agency associations, "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.

"To secure and register a .gov domain, an authorization letter must be submitted to the Cybersecurity and Infrastructure Security Agency (CISA). Competing domain names are not processed on a first come, first served basis, but rather by a review process to determine which agency most closely related will receive it. As a result, this process can take long periods of time with some applicants citing weeks, if not months, to have CISA process and approve a domain. CISA's registrar manages .gov domain hosts and by requiring thousands of California-based local governments (cities, counties, special districts, water authorities, parks, fire, police, sheriff, county hospitals, school districts/students, etc.) to migrate to a .gov domain, it will cause interruptions to support lines, thus creating interruptions and confusion for constituents trying to access critical information on a local government website.

"Also, it should be noted that not all federal governments use the .gov domains. Some U.S. government-related websites use non-.gov domain names, including the United States Postal Service (e.g., usps.com) and various recruiting websites for armed services (e.g.,

goarmy.com), as well as the United States Department of Defense and its subsidiary organizations typically use the .mil top-level domain instead of .gov...

"For these reasons, we propose that AB 1637 narrow its scope to permissively encourage local governments to acquire .gov domains and provide state resources to match available federal grants, as well as establish technical assistance resources for applicants seeking to utilize the .gov domain. Furthermore, we recommend that Cal OES and the California Cybersecurity Integration Center utilize a series of surveys and information requests administered through newly established working groups composed of representatives of local agencies to collect data on the cybersecurity needs around the State and to provide a report summarizing those needs to the Governor and the Legislature. Collectively, our organizations and respective members promote safe, recognizable, and trustworthy online services; however, AB 1637 goes too far, too soon, and contains no resources to help local authorities comply with the proposed mandate."

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

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

Association of California School Administrators (unless amended)
California Special Districts Association (unless amended)
California State Association of Counties (unless amended)
City Clerks Association of California
City of Redwood City
City of San Marcos
League of California Cities (unless amended)
Rural County Representatives of California (unless amended)
Urban Counties of California (unless amended)

Analysis Prepared by: Jimmy MacDonald / L. GOV. / (916) 319-3958