

April 4, 2023

The Honorable Cecilia Aguiar-Curry  
Chair, Assembly Committee on Local Government  
1020 N Street, Room 157  
Sacramento, CA 95814

**RE: AB 1637 (Irwin) Websites: Domain Names.**  
**OPPOSE UNLESS AMENDED** (*As introduced*)

Dear Chair Aguiar-Curry,

The undersigned organizations are regrettably **opposed to Assembly Bill 1637 (Irwin) unless it is amended**. This measure would require local agencies to secure and utilize their website through a new .gov or ca.gov domain no later than January 1, 2025. It would also require all employee email addresses to reflect the updated domain within the same time frame.

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.

While the .gov domain is seen as more “secure” than other domains, several .gov websites have been compromised. As recently as 2019, someone impersonated the mayor of Exeter, Rhode Island successfully gained control of “exeterri.gov” domain name. Furthermore, many .gov websites have been victims of hacking and malware. BART.gov, OaklandCA.gov, USMarshals.gov, FBI.gov, and even closer to home, the California Department of Finance's website, were recently hacked and/or victims of serious ransomware attacks crippling their websites and how constituents accessed information on those websites.

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.

Initial sampling of impacted local governments has identified considerable costs and programmatic impacts. Extrapolated to all local agencies throughout the state, cumulative costs to local agencies are likely to be hundreds of millions of dollars. For example, one 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. Additionally, smaller, and rural local governments would also experience considerable costs and not just for matters directly related to migration .gov domains, given that information technology staff would likely have to be pulled off critical information technology infrastructure projects and life and safety projects, such as mapping wildfires via GIS, to complete the .gov migration.

Finally, local authorities and service districts provide critical information to communities every day. Requiring the change in domain names will require staff to expend effort that could take away from critical services at a time when these entities are already providing emergency services on behalf of the state and while dealing with wildfires, snowstorms, and severe flooding. Pulling staff off critical IT projects to work on a domain change could potentially put communities at risk. Especially in rural areas under the

threat of wildfire, these communities are often the smallest and do not have sufficient resources to redirect staff. Unfortunately, AB 1637 proposes an aggressive compliance date of January 2025, which will cause significant confusion for vulnerable populations who have relied on using these websites for decades.

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. If you have any questions, please do not hesitate to contact Damon Conklin, Legislative Affairs, Lobbyist, Cal Cities at [dconklin@calcities.org](mailto:dconklin@calcities.org), Kalyn Dean, Legislative Advocate, CSAC, at [kdean@counties.org](mailto:kdean@counties.org), Dorothy Johnson, Legislative Advocate, ACSA at [djohnson@ACSA.org](mailto:djohnson@ACSA.org), Aaron Avery, Senior Legislative Representative, CSDA at [aarona@cstda.net](mailto:aarona@cstda.net) and Jean Kinney Hurst, Legislative Advocate, UCCC at [jkh@hbeadvocacy.com](mailto:jkh@hbeadvocacy.com)

Sincerely,



Damon Conklin  
Legislative Affairs, Lobbyist  
League of California Cities



Kalyn Dean  
Legislative Advocate  
California State Association of Counties



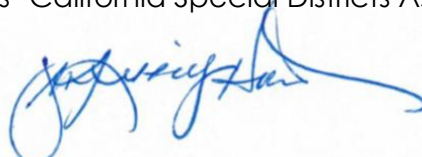
Dorothy Johnson  
Legislative Advocate  
Association of California School Administrators



Aaron Avery  
Senior Legislative Representative  
California Special Districts Association



Sarah Dukett  
Policy Advocate  
Rural County Representatives of California



Jean Kinney Hurst  
Legislative Advocate  
Urban Counties of California

cc: The Honorable Jacqui Irwin  
Members, Assembly Committee on Local Government  
Jimmy MacDonald, Consultant, Assembly Committee on Local Government  
Jith Meganathan, Chief Consultant, Assembly Committee on Privacy and  
Consumer Protection  
William Weber, Consultant, Assembly Republican Caucus