



Brief: Dot-Gov Domains

August 2026

Summary

[House Bill 707](#) aims to improve the credibility of government websites by requiring that every governmental organization carries a dot-gov domain. In its introduced form, no public institution is exempt from the bill. The bill also requires that public employees shall use a dot-gov email address. The bill directs the Virginia Information Technology Agency (VITA) to enforce the regulations provided by the bill.

The bill was proposed to lessen impersonation of government websites, one step in helping improve overall cybersecurity throughout the Commonwealth. By having every government agency utilize the same website domain, citizens could be confident that the information they were receiving came from a valid government source.

During the 2025 session, House Bill 707 was referred to JCOTS to compile stakeholder concerns through workgroup engagement.

Overview of Dot-Gov Domains

Dot-Gov is one of the many top-level domains available. Other well-known domains include dot-com, dot-org, and dot-us. These domains are significantly easier to acquire than a dot-gov domain, which is only available for eligible government agencies. Because of the low eligibility criteria, anyone can register a website such as [exampletown.com](#) or [exampletown.org](#).

In contrast, the eligibility criteria for a dot-gov domain is strict and complicated. The Cybersecurity and Infrastructure Security Agency (CISA) is the agency responsible for determining whether or not an entity is eligible. Eligibility is based on the [Census of Governments](#). If an agency is listed in this document, they are eligible, if not, they are not. Many stakeholders consulted for this brief mentioned the wordy and confusing language of the eligibility criteria. On the one hand, eligibility criteria is clearly stipulated by CISA and their reference documentation. On the other hand, interpreting the documentation can be

challenging. CISA staff acknowledged that they field many questions about eligibility and often need to consider eligibility on a case-by-case basis.

Acquiring a Dot-Gov domain is free and provides agencies with numerous benefits. There are two types of dot-gov domains that would be allowed under this bill. Federal Level (exampletown.gov) and State level (exampletown.virginia.gov). Agencies would be free to determine which one they would like to switch to. Both domains have different naming conventions for agencies to follow that insure the agency will remain identifiable under the domain. VITA oversees naming conventions for state level domains. CISA oversees naming conventions for federal level domains.

Dot-Gov domains grant numerous cybersecurity benefits to agencies once they make the switch. Some of these include clarity about the organization's purpose, higher credibility and trust of the website, improved visibility on search engines, consistency and branding, access to government resources, and protection from spoofing or impersonation.

The CISA website has a list of best practices for moving to the dot-gov domain. Firstly, they recommend that entities keep their old domain name as a redirect for the new dot-gov domain. This ensures that old links will still be valid after the transition, and that the old domain will not fall into the wrong hands, increasing the likelihood of spoofing. Secondly, they recommend all emails are moved to dot-gov, something that is mandated in the current version of the bill. Finally, they suggest using the transition period to audit existing website services, if it is within the capabilities of the organization.

CISA has cybersecurity grants available to entities wanting to increase their cybersecurity. This legislation requires that 80% of the grants they give to states are used to help local entities, with 25% designated to rural communities. This funding could help entities with the domain switch and other cybersecurity efforts if they apply. There are other requirements entities need to meet besides simply transitioning to the domain if they were to receive this federal funding. More information is linked [here](#).

This funding is not the only assistance offered. Although the entity would have to host their website and switch emails on their own, CISA offers domain name consultation, management support, and registration. This means that an entity does not have to worry about ensuring their name fits with CISA's standards; CISA will assist them in ensuring it does. It is important to note that domain names are not first-come-first-serve and CISA will work with entities to make sure they have a domain name that will remain valid for the years to come.

Policy Landscape: Other States

- There are numerous bills similar to 707 that have been recently passed including:
 - [Arkansas](#): This bill is flexible, with a statement for how agencies could bypass the requirements. The bill also has different implementation criteria for smaller localities.
 - [California](#): This bill has a statement regarding redirection of current websites to the dot-gov website. The bill also has requirements for email addresses.
 - [Connecticut](#): This bill only has a dot-gov requirement for municipalities.
 - [Minnesota](#): This bill requires localities that administer elections to have a dot-gov domain address. The bill also has different requirement dates for the application and the transition.
 - [New York](#): This bill requires all municipalities to have a website with a dot-gov domain, even if they did not previously have a website. The bill also has specific requirements for the website to include. The bill also has different implementation criteria for smaller localities.
 - [Utah](#): This bill allows for entities to bypass the requirements if the website is for internal use, temporary, or related to an event with a non-governmental organization. The bill also has a statement where if entities become eligible in the future they will have 15 months to implement the domain change.

Policy Landscape: Federal

Federal legislation has required federal agencies to use a dot-gov or dot-mil domain in the [DOTGOV Online Trust in Government Act of 2020](#).

In addition, the Department of Homeland Security has implemented a [State and Local Cybersecurity Grant Program \(SLCGP\)](#) that provides state, local, tribal, and territorial (SLLT) governments with grants in order to address cybersecurity threats to information systems owned by these SLLT governments. This funding is distributed to states, who distribute it to local governments, with requirements for a quarter of the funding to go to rural communities. One of the recommendations for how to use this funding is to implement a dot-gov domain.

Workgroup Findings

JCOTS convened workgroup meetings on June 23, 2026 and July 14, 2026. A list of workgroup participants can be found at the end of this document. JCOTS held an open call for participants, without restrictions on participation (one representative from each entity was invited to attend). Entities that participated included VCU Health, The University of Virginia, Virginia Beach local government, and more.

Each workgroup was organized around a set of facilitated questions, and participants were not limited in number of contributions, nor speaking time. Although there were questions, the topics of discussion were not constrained to them, and participants were free to introduce additional topics if they wished.

JCOTS received numerous documents from stakeholders prior to the first workgroup documenting concerns with the bill. These pre-meeting documents informed the discussion of the first workgroup. Listed below are some of common concerns raised in pre-meeting submissions:

- 1) The original bill required entities using dot-edu and dot-museum domains to transition to a dot-gov domain.
- 2) There was little intent for what an “official website for public use” meant, and what kinds of websites were included.
- 3) School districts, an entity ineligible for a dot-gov domain, were required to utilize the domain per the original bill language.
- 4) There is a high cost for implementation in regards to switching marketing materials to display the new domain name.
- 5) There was little clarity in the original bill for which specific entities were eligible.
- 6) There was concern that having a dot-gov domain was only one aspect of cybersecurity.
- 7) There was concern of the ability for IT professionals of smaller localities to maintain the level of website security consistent with other dot-gov domains
- 8) There were concerns about the amount of time needed to switch to a dot-gov domain

June 23rd Workgroup

Basing our questions for stakeholders off of the concerns listed in the introductory documents, JCOTS hosted the first workgroup on June 23, 2026. This workgroup discussed implementation costs outside of usual concerns for marketing materials, ways stakeholders have dealt with spoofing and impersonation in the past, and other cybersecurity legislation that they would like to see implemented alongside, or instead of, the dot-gov domain requirement. Concerns for IT capabilities were highlighted, along with suggestions for cybersecurity education to be implemented across the Commonwealth.

JCOTS used the initial documents as well as the comets and suggestions from the first work group to facilitate the creation of a draft brief. The brief contained a summary of the bill, resolved stakeholders concerns, and information about relevant state and federal legislation, and potential recommendations for the bill.

July 14th Workgroup

One week prior to the July 14, 2026 workgroup, stakeholders were sent the draft brief and the second workgroup centered on their responses. Questions were asked on stakeholder's opinions to potential recommendations and other states bills. Questions were also asked on potential implementation of the cybersecurity education campaign brought up in the first workgroup. Concerns for VITA enforcement were highlighted, noting that VITA does not currently have the capacity to enforce the bill. Implementation timelines and costs were also highlighted. When asked about the cybersecurity education campaign, the representative for the Virginia Library Association discussed the Library of Virginia's abilities to implement cybersecurity education across the Commonwealth, due to the presence of libraries as community education systems.

In the second workgroup, several stakeholders requested reaching out to entities that had recently changed their domains to a dot-gov in order to understand fiscal impacts and the time taken for implementation. Following the workgroup meeting, JCOTS staff contacted several Virginia-based entities that had recently undergone the transition. Several entities responded to this request for information. They generally regarded the process as tedious, with one of them noting a 12 month transition period, but they noted that the transition was worth it. In the case of one town using a Microsoft 365 email tracking system, they observed that switching to dot-gov was inexpensive and effortless. Although the costs of implementation were reportedly low, according to entities that recently transitioned, they acknowledged that the true financial burden was the printed media transition, communication of the change to constituents, and the system integration.

Primary Policy Questions

- Spoofing: What standards are necessary to lessen the likelihood of government website impersonation?
- Confidence in Government Websites: What can be done to ensure that citizens are confident in the validity of their government websites? How can citizens be informed that their information is from a viable source?
- Funding: How will smaller entities with little funding for IT departments reasonably be able to manage the change?
- Eligibility: What classifies as a government agency? How can an agency know they are required to comply with a bill? Are there any exemptions that should be considered?
- Enforcement: Who is responsible for enforcement? What is the best way to ensure agencies are complying with the bill? What should happen if an agency isn't compliant?
- Cybersecurity: Besides Dot-Gov, how else can we improve cybersecurity and cybersecurity knowledge across the Commonwealth? What groups are the most at-risk for spoofing?

Policy Recommendations

JCOTS recommends reintroducing the original version of HB 707 with the following recommendations for consideration:

- 1) Modify the bill to state that the requirement only applies to entities that are eligible for a dot-gov domain under the CISA definition (entities listed in the Census of Governments).
 - a) Add a provision stating that if an entity is eligible for a dot-gov *and* a dot-edu domain, they may choose either domain
 - b) Add a provision stating that if an entity is eligible for a dot-gov *and* a dot-museum domain they may choose either domain
 - c) Add a provision to the bill stating that if an entity were to become eligible for a dot-gov domain following the enactment of the bill, that they would have 3 years after the first date of eligibility to make the transition
 - d) Exempt VCU Health from the requirements of the bill. VCU Health is the only health system authority in the Commonwealth explicitly mentioned in the Census of Governments. Along with this, their commercial focus and patient-centered identity are inconsistent with typical government agencies.
- 2) Introduce a budget amendment to support small localities with the costs that come with the adoption of dot-gov domains
 - a) Between now and November, JCOTS staff will work to develop a definition of “small” localities and the specific amount of the request.
- 3) Require entities eligible under the bill’s provisions to list third-party vendors that may communicate directly with the public on behalf of a dot-gov-eligible entity, in a clear and easy to find location on their website or the site they use to communicate with the general public.
 - a) Base the language off of Va. Code § 2.2-3504
- 4) Implement language stating that entities that fail to comply with the provisions listed under the bill must submit an annual report to the Virginia General Assembly detailing the non-conforming domains along with an estimated fiscal audit of what it will cost to transition.
- 5) Research Enforcement: Between now and November, JCOTS staff will work with the Office of the Secretary of Administration and the Office of the Attorney General to identify the most appropriate office to handle enforcement.

Policy Considerations

- 1) Promote the use of the State and Local Cybersecurity Grant Funding that Virginia receives every year as a way for localities to improve their website cybersecurity and reduce some of the financial burdens associated with the domain change.

- 2) Implement cybersecurity education and digital literacy through a freely available online resource distributed through the [Find-It Virginia](#) platform from the Library of Virginia to all Virginia Public Libraries. This can be supplemented through additional in-person education, training, and outreach from public library systems.

How this Brief was Developed

House Bill 707 was referred to JCOTS in order to compile a workgroup for stakeholder perspectives on the bill. Prior to the workgroups, JCOTS staff compiled relevant information pertaining to dot-gov domains from the Cybersecurity and Infrastructure Security Agency (CISA) and documents detailing concerns with the bill from each stakeholder. Using these facts and concerns, questions were compiled for the first workgroup. Following the first workgroup, a draft brief was developed from additional research and stakeholder input from the first workgroup. In the second workgroup, stakeholders gave input to the draft brief. Following the second workgroup, staff reached out to municipalities that have made the switch to a dot-gov domain in the past year. Then, all of the information was compiled to create recommendations and considerations for the continuation of House Bill 707.

Thanks to:

Arlington Public Schools
City of Alexandria
City of Richmond
Office of the Secretary of Administration
Office of Delegate Cliff Hayes
Old Dominion University
Science Museum of Virginia
University of Virginia (UVA)
UVA Health
Virginia Beach
Virginia Commonwealth University (VCU)
VCU Health
Virginia Library Association
Virginia Municipal League
Virginia Tech
Virginia Information Technology Agency (VITA)
York County

For participating in one or both of the work-groups and providing helpful information and background during the preparation of this brief.

References:

- Astrella, Chris. "Dot Gov Decoded: How to Switch Over to Dot Gov Domain." Dot Gov Decoded: How to Switch Over to Dot Gov Domain, <https://www.youtube.com/watch?v=tMdwmOdYISg>.
- Babcock, Chris. *Building Trust: Quantifying Use of the .Gov Domain Below the Federal Level*. UC BERKELEY CENTER FOR LONG-TERM CYBERSECURITY, Sept. 2025, <https://cltc.berkeley.edu/publication/building-trust-quantifying-use-of-the-gov-domain-below-the-federal-level/>. CLTC WHITE PAPER SERIES.
- Bureau, US Census. "Population of Interest." *Census.Gov*, <https://www.census.gov/programs-surveys/gus/technical-documentation/methodology/population-of-interest.html>. Accessed 31 July 2026.
- "City Transitioning to Official .Gov Domain." *City of Delaware, Ohio*, 7 Jan. 2026, <https://www.delawareohio.net/Home/Components/News/News/1276/14>.
- "Colorado Wants \$2 Million to Change Its Domain Name to .Gov." *Youtube*, Next9News, 23 Dec. 2022, <https://www.youtube.com/watch?v=greWaEM8fSU>.
- Fortwrightky.Gov. "Press Release - City of Fort Wright Transitions to .Gov Domain for Enhanced Security." *City of Fort Wright, KY*, 17 July 2024, <https://www.fortwrightky.gov/2024/07/17/press-release-city-of-fort-wright-transitions-to-gov-domain-for-enhanced-security/>.
- Get.Gov*. <https://get.gov/help/faq/>. Accessed 4 June 2026.
- A BILL to Amend the Code of Virginia by Adding in Chapter 55.3 of Title 2.2 a Section Numbered 2.2-5514.2, Relating to State Government; Transaction of Public Business; Prohibited Website Domains. 55.3, 2.2, no. 707, 14 Jan. 2026.
- Requirements for the Registration and Use of .Gov Domains in the Federal Government / Digital.Gov*. 14 May 2024, <https://digital.gov/resources/requirements-for-the-registration-and-use-of-gov-domains-in-the-federal-government>.