The DOTGOV Online Trust in Government Act

Prepared by David St. John, NCSL Extern

The "DOTGOV Online Trust in Government Act of 2019," S. 2749 (hereinafter the Act) introduced by Senator Gary Peters (D-Mich.), Senator Ron Johnson (R-Wisc.), Senator Amy Klobuchar (D-Minn.), and Senator James Lankford (R-Okla.) would provide new requirements for the .gov website domain, with the goal to make it easier for state and local government entities to use the domain for their official websites. Use of the .gov domain for official government websites instead of alternatives like .us or .com makes those government websites and email addresses more secure. Using those less secure domains allows cybercriminals to more easily impersonate government officials to defraud the public and get citizens to share sensitive information. Some states and even more local governments still use these less secure domains for their official websites.[1] The Act would provide support services, security enhancements, and dedicated outreach to help state, local, territorial, and tribal governments to adopt the .gov domain, improving cybersecurity and trust in public services across the United States.

Transition

The Act would transfer authority over the .gov domain from the General Services Administration to the Cybersecurity and Infrastructure Security Agency (CISA). The Act would require that the director of CISA submit a plan for the transition of the .gov domain within 30 days of enactment to the Committee on Homeland Security and Governmental Affairs and the Committee on Rules in the Senate, and the Committee on Homeland Security and Committee on House Administration in the House of Representatives (hereinafter the committees). The Act would also require that the director of CISA begin operationally administering the .gov domain and publish registration requirements within 120 days of enactment.

Support to State and Local Governments

Within one year of enactment, the director must present a report to the committees on outreach to state and local governments to migrate to .gov domains. The director's strategy must include stakeholder engagement plans and information on how migration to .gov benefits the entities, including cybersecurity and federal supporting services.

[1] The following state legislatures do not currently use a .gov domain: Alabama (both houses), Arkansas (lower house), District of Columbia, Kansas (both houses), Minnesota (both houses), Nevada (both houses), New Hampshire (both houses), New Jersey (both houses), Pennsylvania (lower house), Rhode Island (both houses)

Whether to charge fees for services related to the .gov domain including name registration is left at the discretion of the director.

With one year, the director must develop a publicly available reference guide on process and technical information on migrating common services like web and email to a .gov domain, cybersecurity best practices for the .gov domain, and contract vehicles and other private sector resources vetted by the director that may assist state and local governments in the migration.

Additional Reporting and Publishing Requirements

The director must collect information on the use of non-.gov domain suffixes by federal agencies and state, local, tribal, and territorial governments for their official online services. The director must also publish this information on a public website along with best practices and compliance with federal mandates. The director has 180 days after enactment to present a strategy to the committees for using the collected data to counter malicious cyber activity. In addition, the director must inventory all hostnames and services in active use within the .gov domain and provide that inventory to .gov domain registrants at no cost.

Within one year of enactment, the director must develop and submit to the committees a .gov domain security enhancement strategy and implementation plan for improving cybersecurity benefits of the .gov domain for the five-year period after enactment. That strategy must include a modernization plan for information systems that support the .gov domain, a modernization plan for the structure of the .gov program and supporting contracts, and an outline of specific security enhancements .gov intends to provide over the five years after enactment.

Within one year of enactment and every two years thereafter for four years, the director must submit a report to the committees or conduct a detailed briefing to the committees on the status of the outreach strategy, the security enhancement strategy and implementation plan, the inventory of .gov domains, and supporting services to state and local governments.