Calendar No. 401

116TH CONGRESS *2d Session*	SENATE	REPORT 116–192

DOTGOV ONLINE TRUST IN GOVERNMENT ACT OF 2019

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2749

TO PROVIDE REQUIREMENTS FOR THE .GOV DOMAIN, AND FOR OTHER PURPOSES

JANUARY 6, 2020.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
99–010 WASHINGTON : 2020

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
MICHAEL B. ENZI, Wyoming
JOSH HAWLEY, Missouri

GARY C. PETERS, Michigan
THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

GABRIELLE D'ADAMO SINGER, *Staff Director*
JOSEPH C. FOLIO III, *Chief Counsel*
COLLEEN E. BERNY, *Professional Staff Member*
DAVID M. WEINBERG, *Minority Staff Director*
ZACHARY I. SCHRAM, *Minority Chief Counsel*
JEFFREY D. ROTHBLUM, *Minority Senior Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 401

116TH CONGRESS *2d Session* | SENATE | REPORT 116–192

DOTGOV ONLINE TRUST IN GOVERNMENT ACT OF 2019

JANUARY 6, 2020.—Ordered to be printed

Mr. JOHNSON, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 2749]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2749), to provide requirements for the .gov domain, and for other purposes, having considered the same, reports favorably thereon with amendments and recommends that the bill, as amended, do pass.

CONTENTS

	Page
I. Purpose and Summary	1
II. Background and Need for the Legislation	2
III. Legislative History	5
IV. Section-by-Section Analysis	6
V. Evaluation of Regulatory Impact	9
VI. Congressional Budget Office Cost Estimate	9
VII. Changes in Existing Law Made by the Bill, as Reported	10

I. PURPOSE AND SUMMARY

S. 2749, the DOTGOV Online Trust in Government Act of 2019, increases the utility and availability of the .gov domain to Federal agencies, state, local, tribal and territorial (SLTT) governments, and publicly-controlled entities. This bill sets specific timeline requirements for the transition of the .gov program and administration. Upon enactment, the .gov domain program is to transition from the General Services Administration (GSA) to the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). On a continuous basis thereafter, CISA is re-

quired to inventory all active hostnames and services in the .gov domain and provide that data to domain registrants at no cost.

Within 30 days of the bill's enactment, CISA is required to submit its operational and contractual transition plan for the .gov program to Congress. CISA is also required to begin administering the .gov domain program and publish domain registration requirements on a public website within 120 days of the bill's enactment. Upon CISA's publication of its registration requirements, GSA is required to rescind the requirements of 41 CFR, parts 102–173. Within 180 days, CISA is to develop and submit to Congress a strategy to counter malicious cyber activity using the .gov domain information.

CISA is also required to, within one year, publish an outreach strategy for engaging with SLTT and publicly-controlled entities on the benefits of the .gov domain, and develop and publish a reference guide for migrating to the .gov domain. Additionally, no later than one year after the bill's enactment, CISA must develop a five-year security enhancement strategy and implementation plan for the .gov domain and submit it to Congress. CISA is also required to submit a report to Congress on the outreach strategy, security strategy, inventory, services, and fees associated with .gov domain registration. After the submission of the initial report, CISA is to submit follow-up reports on a biannual basis for four years. Finally, this bill limits the fees charged for the administration of the program to the amounts charged on October 1, 2019, for the first five years of enactment.

II. Background and the Need for Legislation

Background on the .gov domain program

Over thirty years ago, in 1985, the .gov top-level domain (TLD) was established in the United States.[1] The GSA started administering the .gov program and registering Federal agencies in 1997.[2] In 2003, the .gov domain expanded to include SLTT governments.[3]

Today, there are a variety of TLDs available for websites, including .com, .org, .net, and .us.[4] However, these types of domains are not exclusive, whereas the .gov domain is only available to U.S. Government organizations.[5] To receive a .gov domain, registrants must meet the eligibility requirements, pass the validation process, and verify that they are legitimate U.S. Government entities.[6]

The Committee has determined that additional reforms are needed to secure and safeguard the .gov domain program. As discussed

---

[1] Jessica Salmoiraghi, U.S. Gen. Serv's Admin., The DotGov Program: Putting the US Government on the Internet, at 3 (2019), https://www.nass.org/sites/default/files/2019%20Summer/presentations/presentation-dotgov-summer19.pdf; *See also* Zahra, *Everything You Need to Know About .Gov Domains,* TownWeb (May 2018), https://www.townweb.com/2016/09/30/everything-need-know-gov-domains/.

[2] *Id.*

[3] *Id.*

[4] Salmoiraghi, *supra* note 1, at 9–10.

[5] *Id.; See also* U.S. Gen. Serv's Admin., Why .gov?, https://www.gsa.gov/cdnstatic/DotGov_One-Pager.pdf.

[6] DotGov Portal, Domain Requirements, https://home.dotgov.gov/registration/requirements/; *See also* Steve Grobman, *State County Authorities Fail at Midterm Election Internet Security,* McAfee (Oct. 24, 2018), https://www.mcafee.com/blogs/other-blogs/executive-perspectives/state-county-authorities-fail-at-midterm-election-internet-security/.

below, S. 2749 implements those reforms as improvements to the .gov internet domain program.

Increases awareness and supports the transition to .gov

As of April 2019, there were 6,000 .gov domain customers comprised of 56 percent local government, 22 percent Federal Government, 20 percent state government, and 3 percent tribal/native sovereign nations.[7] Local governments make up more than half of the .gov domain participation rate with approximately 3,360 participants, yet the U.S. Census Bureau reported 38,779 general purpose governments (counties, cities, towns, townships, villages, and additional jurisdictions) in 2017.[8] Thus, only approximately 8.7 percent of these types of local governments are currently utilizing the .gov domain.

In October 2018, McAfee examined the security of election infrastructure at the state and county level and found that "large majorities of county websites use top level domain names such as .com, .net and .us rather than the government validated .gov in their web addresses."[9] Specifically, "Minnesota and Texas had the largest percentage of non-.gov domain names with 95.4% and 95% respectively. They were followed by Michigan (91.2%), New Hampshire (90%), Mississippi (86.6%) and Ohio (85.9%)."[10] Arizona had the largest .gov domain participation with 66.7 percent of counties using validated addresses.[11] In addition, major cities throughout the nation are not utilizing the .gov domain, including Houston, Los Angeles, New York City, and Philadelphia.[12]

Utilizing the .gov domain helps local governments validate their information to residents. For example, in December 2018, the town website of Falmouth, Massachusetts switched from falmouthmass.us to falmouthma.gov.[13] According to their information technology director, Gregory Banwarth, "the .com., .org, .us name space is basically a public domain, so just about any company or any entity can grab those things, and we've seen an increase in the number of services [. . .] that are actually just masquerading state or municipal services with an extra cost attached . . ." In addition, he stated the public is becoming more aware of the .gov domain and knows it is legitimate government information.[14]

Currently, the Federal Government's authority to provision .gov domains is not codified in statute. S. 2749 increases awareness to the .gov domain by defining the purpose of the .gov internet domain program and codifying CISA's provision of .gov domain name registration services, and supporting services, to any Federal,

---

[7] Salmoiraghi, *supra* note 1, at 3–4, 6.

[8] U.S. Census Bureau, 2017 Census of Governments—Organization, Table 2. Local Governments by Type and State: 2017 (2017), https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html; Governing: the States and Localities, *Number of Local Governments by State*, e.Republic (2017), https://www.governing.com/gov-data/number-of-governments-by-state.html (citing U.S. Census Bureau); *See also* Salmoiraghi, *supra* note 1.

[9] Grobman, *supra* note 6.

[10] *Id.*

[11] *Id.*

[12] Brian Krebs, *It's Way Too Easy to Get a .gov Domain Name*, KrebsonSecurity (Nov. 26, 2019), https://krebsonsecurity.com/2019/11/its-way-too-easy-to-get-a-gov-domain-name/.

[13] Salmoiraghi, *supra* note 1, at 11; *See also* Brad Cole, *Falmouth Getting New Website, E-Mail Address*, Falmouth Enter. (Dec. 6, 2018), https://www.capenews.net/falmouth/news/falmouth-getting-new-website-e-mail-addresses/article_bae21f6c-f0fe-54f3-bcf8-30dce2aaa202.html.

[14] *Id.*

SLTT government, or other publicly-controlled entity that complies with the registration requirements.

Improves security for those utilizing .gov

As previously mentioned, the vast majority of county and local governments are not currently utilizing the .gov domain. As a result, cybercriminals are targeting these governments, as well as small businesses and individuals, to obtain sensitive information. One phishing campaign was uncovered earlier this year that involved an effort to impersonate hundreds of local government websites and prey on small businesses.[15] According to Lookout Phishing AI,

> [t]he threat actor has registered more than 200 domains with the same email address since 2015, and is now averaging about seven to ten per week. And recently, the actor has created a series of fake local government websites, impersonating the likes of Dallas County, Polk County, the City of San Mateo, the City of Tampa, and the City of North Las Vegas.[16]

The fake sites were almost a perfect replica of the legitimate websites, but contained a "Vendor Registration Form" to compromise personally identifiable information and other credentials.[17]

While there are current security and verification processes in place for U.S. Government entities to apply for and obtain a .gov domain, individuals have recently attempted and successfully acquired a .gov domain.[18] In November 2019, a computer researcher submitted to Krebs on Security evidence that they "got a .gov domain simply by filling out and emailing an online form, grabbing some letterhead off the homepage of a small U.S. town that only has a '.us' domain name, and impersonating the town's mayor in the application." [19] Although the researcher did this as an experiment, there are malicious actors who will attempt this to create false websites and emails, and circulate fabricated news stories.[20]

This bill will improve cybersecurity for government websites by increasing the utilization of a trusted and secured .gov domain by Federal and SLTT governments, and other publicly-controlled entities. In addition, S. 2749 directs CISA to develop a security enhancement strategy and implementation plan to improve the cybersecurity benefits of the .gov domain. The strategy will include: a modernization plan for the information systems that support.gov domain operations; a modernization plan for the .gov program office and contracts to leverage and exploit emerging technologies; and, specific cybersecurity enhancements for the domain.

Ensures an effective transition from GSA to DHS

The GSA's Office of Information Integrity and Access currently manages the .gov internet domain program.[21] However, in con-

---

[15] Jeremy Richards, *Too Close to Home: Local Business Targeted by Phishing Attacks*, Lookout Blog (May 29, 2019), https://blog.lookout.com/local-businesses-phishing-attacks.
[16] *Id.*
[17] *Id.*
[18] DotGov Portal, *supra* note 6; *See also* Krebs, *supra* note 12.
[19] *Id.*
[20] *Id.*
[21] U.S. Gen. Serv's Admin., DotGov Domain Services (May 31, 2019), https://www.gsa.gov/policy-regulations/policy/information-integrity-and-access/dotgov-domain-services.

sultation with the Office of Management and Budget (OMB) and other Executive Branch agencies, the Committee believes that the .gov internet domain program should be moved from GSA to DHS's CISA.[22] S. 2749 ensures the .gov internet domain program is effectively transferred from GSA to CISA by laying out a transition timeline, requiring CISA to submit a plan to Congress for the program transition, begin operational control of the .gov internet domain program, and publicly publish .gov domain registration policies. GSA shall rescind its existing .gov domain requirements, which will count towards the "one in, two out" rule under the Presidential Executive Order on Reducing Regulation and Controlling Regulatory Costs.[23] During this transition period, and for a five-year period starting on the date of enactment, any fees for new registrations or annual renewals of .gov domains shall not be more than the amount of the fees charged as of October 1, 2019. The annual fee for the .gov domain as of that date was $400 per year.[24] It is not the Committee's intent to limit or define how the Executive Branch develops processes or policies for the coordination of the assignment of .gov domain names for Executive Branch agencies.

III. Legislative History

On October 30, 2019, Ranking Member Gary Peters (D–MI) introduced S. 2749, DOTGOV Online Trust in Government Act of 2019, which was referred to the Committee on Homeland Security and Governmental Affairs. Chairman Ron Johnson (R–WI), Senator Amy Klobuchar (D–MN), Senator James Lankford (R–OK), Senator Roy Blunt (R–MO), and Senator Margaret Wood Hassan (D–DH) are cosponsors.

The Committee considered S. 2749 at a business meeting on November 6, 2019. During the business meeting, Ranking Member Peters offered an amendment and Senator Rick Scott offered an amendment as modified.

Peters Amendment 1 made three technical changes to the bill, including clarifying requirements for domain registrants. Scott Amendment 1 as modified added oversight language on the fees for making the .gov domain name registration and any supporting services available. This included adding additional language to the bill's findings that the .gov internet domain should be available at no cost or at a negligible cost; clarifying that the total fees collected shall not exceed the direct operational expenses to maintain the .gov internet domain program; adding to the reporting requirement on how CISA is developing, assessing, and determining .gov domain fees; and ensuring that any fees for .gov domains shall not be more than the amount of the fees charged as of October 1, 2019 for a five year period.

The Committee adopted Peters Amendment 1 and Scott Amendment 1 as modified *en bloc* by voice vote. Senators present for the votes on the amendments were: Johnson, Portman, Paul, Lankford,

[22] E-mail from Office of Mgmt. & Budget, Exec. Office of the President, to Staff of S. Comm. on Homeland Sec. and Gov'l Affairs (Sep. 10, 2019) (on file with the Committee).

[23] Exec. Order No. 13771, 82 FR 9339 (Jan. 30, 2017), https://www.whitehouse.gov/presidential-actions/presidential-executive-order-reducing-regulation-controlling-regulatory-costs/.

[24] Zahra, *supra* note 1.

Romney, Scott, Enzi, Hawley, Peters, Carper, Hassan, Sinema, and Rosen.

The Committee favorably reported the bill *en bloc*, as amended by Peter Amendment 1 and Scott Amendment 1, by voice vote. Senators present for the vote were: Johnson, Portman, Paul, Lankford, Romney, Scott, Enzi, Hawley, Peters, Carper, Hassan, Sinema, and Rosen.

Consistent with Committee rules, the Committee reports the bill with technical amendments by mutual agreement of the Chairman and Ranking Member.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section provides the bill's short title, the "DOTGOV Online Trust in Government Act of 2019" or the "DOTGOV Act of 2019."

Section 2. Findings

This section includes findings by Congress regarding the .gov domain, including that the .gov domain is a unique American resource based on its role in creating the Internet. It also recognizes that the .gov domain improves the public's safety and security because it is recognized as a safe and official resource, and difficult to impersonate. This section also states that the .gov should be made available at no cost or at a negligible cost to all levels of government in the United States. Finally, it states that the .gov internet domain provides a critical service and should be operated in a transparent manner.

Section 3. Definitions

This section defines several terms, including "Administrator," "Director," "online service," and "State."

Section 4. Duties of Department of Homeland Security

This section defines that the purpose of the .gov internet domain program is to legitimize and improve the public's trust in government entities and their online services; enable reliable connections to and from government entities; provide the registration of .gov internet domains in a simple and secure manner; improve the security for the .gov namespace the services provided; and to assist the public and domain registrants in discovering available government services.

Section 4(b)(1) amends Title XXII of the Homeland Security Act of 2002 by adding a new paragraph on carrying out the duties and authorities relating to the .gov domain. The paragraph then adds a new section at the end on the duties and authorities relating to the .gov domain.

Subsection (a) of the new section codifies that CISA shall offer .gov domain name registration services, and supporting services, to any Federal, SLTT government, or other publicly-controlled entity that complies with the requirements for registration developed by CISA, without requiring these entities to share unnecessary data with the federal government or requiring them to participate in any other federal programs.

Subsection (b) of the new section codifies that CISA, in consultation with OMB, shall establish and publicly publish the registration and operation policies of the .gov domains necessary to minimize the risk of .gov names that may mislead or confuse the public; shall not permit .gov domains to be used for commercial or campaign purposes; and, shall certify domains are registered and retained only by authorized people. It also limits CISA from sharing unnecessary information with other DHS components and Federal agencies.

Subsection (c) of the new section codifies that in addition to .gov domains, CISA may offer supporting services specifically intended to increase the security, privacy, reliability, accessibility, and speed of those .gov domains. Nothing shall be construed to limit CISA's authorities to provide services or technical assistance, or to establish new authorities for services, other than those authorities that support the operation of the .gov domain or registrants' needs.

Subsection (d) of the new section also allows CISA to charge entities fees, if needed, to recover the costs of providing .gov domain services. However, the total amount of fees for new registrants or annual renewals of .gov domains cannot surpass the direct operational costs of maintaining the .gov internet domain.

Subsection (e) of the new section requires that CISA consult with OMB, GSA, other appropriate civilian Federal agencies, and representatives of state, local, tribal, or territorial governments on the strategic direction and requirements of the .gov domain, specifically on matters of privacy, accessibility, transparency, and technology modernization.

Subsection (f) of the new section directs CISA to inventory all .gov domain hostnames and services, and provide that data to all .gov users at no cost. This data can be obtained via the analysis of public and non-public sources, which include commercial data sets. CISA shall share all unique hostnames and services discovered within domain registrants' zones with Federal and non-federal domain registrants. CISA is further directed to share data collected or used by the program about Federal executive branch agencies as necessary with OMB in support of OMB's role overseeing Federal technology and cybersecurity under the Federal Information Security Management Act. CISA is further directed to publish the publicly accessible Federal website information online. CISA may also publicly publish analyses and data relating to compliance with industry best practices and Federal mandates. Additionally, CISA is directed to collect information on the use of non-.gov Federal domains and to collect information from SLTT governments on non-.gov domain use. This information is also to be published online.

Section 4(b)(2)sets forth additional duties of CISA that are not codified in the Homeland Security Act. Section 4(b)(2)(A) directs CISA to develop a strategy to utilize the information collected under this subsection to counter malicious cyber activities, and to submit this strategy within 180 days of enactment to the Senate Committee on Homeland Security and Governmental Affairs, the Senate Committee on Rules and Administration, the House Homeland Security Committee, and the Committee on House Administration. Within one year of enactment, CISA, in consultation with GSA and with entities representing SLTT governments, is required to develop an outreach strategy, and to submit this strategy to the

Senate Committee on Homeland Security and Governmental Affairs, the Senate Committee on Rules and Administration, the House Homeland Security Committee, and the Committee on House Administration. This outreach strategy will require specific engagement plans and information explaining the benefits, including security benefits, of moving to the .gov domain for these governments.

Section 4(b)(2)(B) directs CISA, in consultation with GSA and with entities representing SLTT governments, to develop and publish a public reference guide within one year of enactment on transitioning online services to the .gov domain. The guide will include process and technical information in carrying out a migration; cybersecurity best practices relating to registration and operation of a .gov domain; and CISA-vetted private sector resources and references to contract vehicles that may assist in performing the migration.

Section 4(b)(2)(C) directs CISA to develop a security enhancement strategy and implementation plan within one year after enactment to improve the cybersecurity benefits of the .gov domain over the next five years, and to submit the strategy to the Senate Committee on Homeland Security and Governmental Affairs, the Senate Committee on Rules and Administration, the House Homeland Security Committee, and the Committee on House Administration. The strategy will include a modernization plan for the information systems that support the operation of the .gov domain, a modernization plan for the structure of the .gov program office and contracts to best take advantage of emerging technologies, and specific cybersecurity enhancements.

Finally, section 4(b)(3) amends Section 2008(a) of the Homeland Security Act of 2002 and adds a new subsection that makes .gov migration costs an allowable expense under the Urban Area Security Initiative and State Homeland Security Grant Program.

Section 5. Report

This section requires CISA to submit a report or a detailed briefing one year after enactment, and again at three years and five years after enactment to the Senate Committee on Homeland Security and Governmental Affairs, the Senate Committee on Rules and Administration, the House Homeland Security Committee, and the Committee on House Administration. The report or detailed briefing shall include information on the status of the required outreach strategy, security enhancement strategy and implementation plan, .gov inventory, supporting services, and the development, assessment, and determination of the fees for new registrations or annual renewals of .gov domain registrants.

Section 6. Transition

This section lays out a transition timeline for transferring the .gov internet domain program from GSA to CISA. Within 30 days of enactment, it requires CISA to submit a plan for transitioning the program to the Senate Committee on Homeland Security and Governmental Affairs, the Senate Committee on Rules and Administration, the House Homeland Security Committee, and the Committee on House Administration. Not later than 120 days after enactment, CISA shall begin operational control of the .gov internet

domain program and shall publicly publish .gov domain registration policies, at which time GSA shall rescind its existing .gov domain requirements. In addition, this section states that for a five-year period starting on the date of enactment, any fees for new registrations or annual renewals of .gov domains shall not be more than the amount of the fees charged as of October 1, 2019.

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. Congressional Budget Office Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, November 21, 2019.

Hon. Ron Johnson,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for S. 2749, the DOTGOV Online Trust in Government Act of 2019.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

Phillip L. Swagel,
Director.

Enclosure.

S. 2749, DOTGOV Online Trust in Government Act of 2019
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on November 6, 2019

By Fiscal Year, Millions of Dollars	2020	2020-2024	2020-2029
Direct Spending (Outlays)	*	*	*
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	*	*	*
Spending Subject to Appropriation (Outlays)	*	*	not estimated

Statutory pay-as-you-go procedures apply?	Yes	Mandate Effects	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2030?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000

S. 2749 would codify the process through which federal and nonfederal entities request internet domain names specifically for governmental users (i.e. domain names ending in .gov). The bill would transfer the responsibility for overseeing the current process from the General Services Administration (GSA) to the Cybersecurity and Infrastructure Security Agency (CISA). The bill also would permit state and local entities to apply for homeland security grants to help fund the costs of transitioning to those governmental domain names.

GSA spends about $5 million each year to manage the program. CBO expects that under the bill, CISA would pay for those operating expenses instead; thus, any change in spending subject to appropriation would be insignificant.

GSA currently charges a $400 fee for each domain name request to recover the amount it pays vendors to process the transaction. S. 2749 would permit CISA to provide that service with or without reimbursement. A reduction in fee collections from nonfederal entities would be recorded as an increase in direct spending. CBO does not expect that CISA would waive the current fee; thus, any increase in direct spending would be insignificant over the 2020—2029 window, CBO estimates.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Leo Lex, Deputy Assistant Director for Budget Analysis.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

* * * * * * *

SEC. 1. SHORT TITLE; TABLE OF CONTENTS.

(a) * * *

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. * * *

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

2215. Duties and Authorities Relating To .Gov Domain.

* * * * * * *

TITLE XX—HOMELAND SECURITY GRANTS

* * * * * * *

Subtitle A—Grants to States and High-Risk Urban Areas

* * * * * * *

SEC. 2008. USE OF FUNDS

(a) * * *

(1) * * *

* * * * * * *

(13) any activity permitted under the Fiscal Year 2007 Program Guidance of the Department for the State Homeland Security Grant Program, the Urban Area Security Initiative (including activities permitted under the full-time counterterrorism staffing pilot), or the Law Enforcement Terrorism Prevention Program; [and]

(14) migrating any online service (as defined in section 3 of the DOTGOV Online Trust in Government Act of 2019) to the .gov domain; and

[(14)] *(15) any other appropriate activity, as determined by the Administrator.*

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

(a) * * *

(b) * * *

(c) * * *

(1) * * *

* * * * * * *

(10) carry out cybersecurity, infrastructure security, and emergency communications stakeholder outreach and engagement and coordinate that outreach and engagement with critical infrastructure Sector-Specific Agencies, as appropriate; [and]

(11) carry out the duties and authorities relating to the .gov domain, as described in section 2215; and

[(11)] *(12)* carry out such other duties and powers prescribed by law or delegated by the Secretary.

* * * * * * *

SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV DOMAIN

(a) AVAILABILITY OF .GOV DOMAIN.—The Director shall make .gov domain name registration services, as well as any supporting services described in subsection (c), generally available—

(1) to any Federal, State, local, or territorial government entity, or other publicly controlled entity, including any Tribal gov-

ernment recognized by the Federal Government or a State government, that complies with the requirements for registration developed by the Director as described in subsection (b);

(2) without conditioning registration on the sharing of any information with the Director or any other Federal entity, other than the information required to meet the requirements described in subsection (b); and

(3) without conditioning registration on participation in any separate service offered by the Director or any other Federal entity.

(b) REQUIREMENTS.—The Director, in consultation with the Director of the Office of Management and Budget, shall establish and publish on a publicly available website requirements for the registration and operation of .gov domains sufficient to—

(1) minimize the risk of .gov domains whose names could mislead or confuse users;

(2) establish that .gov domains may not be used for commercial or campaign purposes;

(3) ensure that domains are registered and maintained only by authorized individuals; and

(4) limit the sharing or use of any information obtained through the administration of the .gov domain with any other Department component or any other agency of the Federal Government for any purpose other than the administration of the .gov domain, the services described in subsection (c), and the requirements for establishing a .gov inventory described in subsection (f).

(c) SUPPORTING SERVICES.—

(1) IN GENERAL.—The Director may provide services to the entities described in subsection (a)(1) specifically intended to support the security, privacy, reliability, accessibility, and speed of registered .gov domains.

(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to—

(A) limit other authorities of the Director to provide services or technical assistance to an entity described in subsection (a)(1); or

(B) establish new authority for services other than those the purpose of which expressly supports the operation of .gov domains and the needs of .gov domain registrants.

(d) FEES.—

(1) IN GENERAL.—The Director may provide any service relating to the availability of the .gov internet domain program, including .gov domain name registration services described in subsection (a) and supporting services described in subsection (c), to entities described in subsection (a)(1) with or without reimbursement.

(2) LIMITATION.—The total fees collected for new .gov domain registrants or annual renewals of .gov domains shall not exceed the direct operational expenses of maintaining the .gov internet domain.

(e) CONSULTATION.—The Director shall consult with the Director of the Office of Management and Budget, the Administrator of General Services, other civilian Federal agencies as appropriate, and entities representing State, local, Tribal, or territorial governments

in developing the strategic direction of the .gov domain and in establishing requirements under subsection (b), in particular on matters of privacy, accessibility, transparency, and technology modernization.

(f) .GOV INVENTORY.—

(1) IN GENERAL.—The Director shall, on a continuous basis—

(A) inventory all hostnames and services in active use within the .gov domain; and

(B) provide the data described in subparagraph (A) to domain registrants at no cost.

(2) REQUIREMENTS.—In carrying out paragraph (1)—

(A) data may be collected through analysis of public and non-public sources, including commercial data sets;

(B) the Director shall share with Federal and non-Federal domain registrants all unique hostnames and services discovered within the zone of their registered domain;

(C) the Director shall share any data or information collected or used in the management of the .gov domain name registration services relating to Federal executive branch registrants with the Director of the Office of Management and Budget for the purpose of fulfilling the duties of the Director of the Office of Management and Budget under section 3553 of title 44, United States Code;

(D) the Director shall publish on a publicly available website discovered hostnames that describe publicly accessible Federal agency websites, to the extent consistent with the security of Federal information systems but with the presumption of disclosure;

(E) the Director may publish on a publicly available website any analysis conducted and data collected relating to compliance with Federal mandates and industry best practices, to the extent consistent with the security of Federal information systems but with the presumption of disclosure; and

(F) the Director shall—

(i) collect information on the use of non-.gov domain suffixes by Federal agencies for their official online services;

(ii) collect information on the use of non-.gov domain suffixes by State, local, Tribal, and territorial governments; and

(iii) publish the information collected under clause (i) on a publicly available website.

(3) STRATEGY.—Not later than 180 days after the date of enactment of this section, the Director shall develop and submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Rules and Administration of the Senate and the Committee on Homeland Security and the Committee on House Administration of the House of Representatives a strategy to utilize the information collected under this subsection for countering malicious cyber activity.

* * * * * * *

○