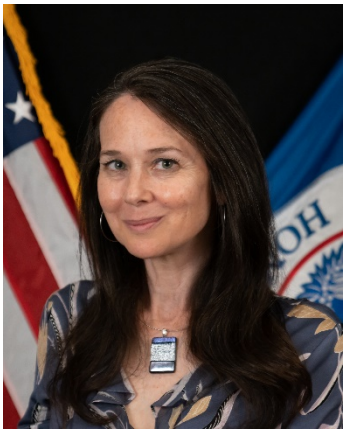
Operational and Contractual Transition of the .gov Internet Program

Year 2021 Report to Congress
August 27, 2021

Homeland Security

Cybersecurity and Infrastructure Security Agency (CISA)

Message from the Director of the Cybersecurity and Infrastructure Security Agency



August 27, 2021

The following report, "Operational and Contractual Transition of the .gov Internet Program" was prepared by the Cybersecurity and Infrastructure Security Agency (CISA). This document was compiled pursuant to requirements in the DOTGOV Online Trust in Government Act of 2020 (Pub. L. 116-260). Included is an overview.

Pursuant to congressional requirements, this document is being provided to the following Committees:

The Honorable Gary C. Peters
Chairman, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Rob Portman
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Amy Klobuchar
Chairwoman, Senate Committee on Rules and Administration

The Honorable Roy Blunt
Ranking Member, Senate Committee on Rules and Administration

The Honorable Bennie G. Thompson
Chairman, House Committee on Homeland Security

The Honorable John Katko
Ranking Member, House Committee on Homeland Security

The Honorable Carolyn B. Maloney
Chairwoman, House Committee on Oversight and Reform

The Honorable James Comer
Ranking Member, House Committee on Oversight and Reform

The Honorable Zoe Lofgren
Chairperson, House Committee on Administration

The Honorable Rodney Davis
Ranking Member, House Committee on Administration

Inquiries relating to this report may be directed to Erin Wieczorek, Chief External Affairs Officer (acting), at 703-235-2080.

Sincerely,

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

Executive Summary

The DOTGOV Online Trust in Government Act of 2020 (DOTGOV Act) authorizes the Cybersecurity and Infrastructure Security Agency (CISA) to administer the .gov top-level domain (TLD), assuming governance from the U.S. General Services Administration (GSA). This report, required by the Act, outlines CISA's plan for the operational and contractual transition of the .gov TLD.

CISA works to defend against today's cybersecurity threats and collaborates with partners to build more secure and resilient infrastructure for the future. The .gov TLD is used by each branch of the Federal Government, every state in the nation, hundreds of counties and cities, and many tribes and territories to serve the public on the internet. The TLD is foundational to thousands of online services that are relied upon by millions of users in and out of government, around the nation and throughout the world. As it underpins communication with and within U.S.-based government organizations, the .gov TLD is *critical infrastructure* and all aspects of its administration have cybersecurity significance.

Since passage of the DOTGOV Act, GSA and CISA have met frequently to coordinate the funding, public communication, and handoff tasks required to ensure a seamless transition of daily operations at the TLD. The transition team includes a staff member at CISA with direct experience from a recent year-long detail at GSA's DotGov Program. Most of the important operational changes occurring as part of the transition are *administrative in nature*, not technical changes that could jeopardize the stability of the .gov TLD. For instance, CISA does not anticipate needing to make any major changes to system controls in order to satisfy executive branch IT security requirements. Similarly, the .gov TLD's nameservers – the core domain name system (DNS) infrastructure managed by the .gov contractor that makes the TLD available on the internet – are not changing as part of this transition.

CISA began "operationally administering" the DotGov Program starting April 26, 2021, as required in Section 907(c) of the DOTGOV Act.

Funding for the DotGov Program and its support contract was not included in CISA's FY21 budget request or in the Consolidated Appropriations Act, 2021 (Pub. L. 116-260). CISA has requested funding in the FY22 budget.

The .gov contract is in its final option year, adding further urgency on top of the requirements and timelines of the DOTGOV Act. A significant portion of CISA's effort this calendar year will be to prepare and execute on a new contract strategy. Given the nature of acquisition timelines and the responsibility to review and authorize any new .gov infrastructure in future awards *and seamlessly migrate to it*, CISA may require a short-term bridge contract to ensure continued stability in .gov operations.

Administering the .gov TLD enables CISA to set secure defaults for a platform many government organizations already use while assisting even more to use it. The TLD offers CISA central insight into certain classes of cyber threats, and under the actions required in the Act, we

expect our work to increase security and decrease complexity, particularly for state and local government organizations.

Operational and Contractual Transition of the .gov Internet Program

Table of Contents

I. Legislative Language

Section 907 of the DOTGOV Act of 2020, found in title IX of Division U of the Consolidated Appropriations Act, 2021 (Pub. L. 116-260), includes the following requirement.

(b) Not later than 30 days after the date of enactment of this Act, the Director shall submit a plan for the operational and contractual transition of the .gov internet domain program 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, the Committee on Oversight and Reform, and the Committee on House Administration of the House of Representatives.

II. Background

.gov is one of the six original top-level domains (TLD) in the internet's domain name system (DNS). DNS is the internet service that translates the names humans prefer into the numbers computers need to route a user to a website or to send an email. Only bona fide U.S.-based government organizations are authorized to obtain a .gov domain, and governments use .gov to show the public their online services are official.

.gov is used by each branch of the Federal Government. Every state in the nation, hundreds of counties and cities, and many tribes and territories use .gov domains to serve the public on the internet. The TLD is foundational to thousands of online services that are relied upon by millions of users in and out of government, around the nation and throughout the world. As it underpins communication with and within U.S.-based government organizations, the .gov TLD is *critical infrastructure* and all aspects of its administration have cybersecurity significance.

Since 1997, the U.S. General Services Administration (GSA) has been the policy and management authority over the .gov TLD, working to ensure that .gov domains are issued only to authorized registrants and that the TLD resolves in the global DNS. GSA's responsibilities were never codified into statute, which resulted in a lack of investment in the TLD's technological base and caused operational challenges in serving state, local, tribal, and territorial (SLTT) governments. With the passage of the Consolidated Appropriations Act, 2021, which included the DOTGOV Act, Congress directed the Cybersecurity and Infrastructure Security Agency (CISA) to administer the TLD. CISA is the nation's risk advisor, working with partners to defend against today's threats and collaborating to build a more secure and resilient infrastructure for the future. In consultation with the Office of Management and Budget (OMB), CISA administers the implementation of information security policies and practices at federal civilian executive branch agencies. CISA performs its functions pursuant to authority in the Federal Information Security Modernization Act of 2014 (FISMA), which sets specific responsibilities for the cybersecurity of certain agency information systems. Additionally, CISA is authorized to provide cybersecurity assistance to non-Federal entities.

This report outlines how CISA planned for the operational and contractual transition of the .gov internet domain program.

III. Operational and Contractual Transition Plan

Upon the introduction of the DOTGOV Act of 2019[1] in late 2019, GSA's DotGov Program staff and CISA team members met roughly monthly to discuss a transition. Both agencies outlined a transfer schedule with expected tasks and owners, including the nominal duration for each task. Since passage of the DOTGOV Act of 2020, GSA and CISA have met weekly – often multiple times per week – to outline a path forward and detail the transfer schedule. The tasks fit into three workstreams: determine funding, communicate with the public, and transition. The latter two tasks comprise the *operational* actions of the transfer, which are described first in this report, while the fund action represents the *contractual* side.

Operational

Public Communication

As of January 2020, there are 6,402 .gov domains and approximately 13,000 government officials or their representatives have accounts in the .gov registrar (https://domains.dotgov.gov). To inform current and potential .gov registrants of the pending change in management at the TLD, on March 8, 2021, the GSA DotGov Program notified registrants of the change via email and both GSA and CISA issued press releases.

Beyond being a common courtesy and useful to marketing .gov, this communication is crucial because several government organizations have asked GSA and CISA about the transition. The communications were also an opportunity to generate interest from SLTT entities with whom CISA might consult on the strategic direction of the .gov TLD (under Section 2215(g) of the Homeland Security Act of 2002, as added by Section 904(b)(1)(B) of the DOTGOV Act), an outreach strategy (under Section 904(b)(2)(A)), and a migration guide (under Section 904(b)(2)(B)).

Transition

A transition for responsibility of daily operations from the GSA DotGov Program to a new CISA DotGov Program is being carefully conducted to ensure continuity for registrants, the .gov contractor, and the TLD generally. Aiding this transition is the fact that CISA staff have direct experience at GSA's DotGov Program. From December 2017 – December 2018, CISA detailee to GSA managed daily operations, interacted regularly with the current contractor, and facilitated key strategic and security decisions. This individual will be managing the CISA DotGov Program and their hands-on experience will support a seamless transition.

Documentation

As part of the transition, GSA has shared programmatic and security documentation with CISA. This includes:

[1] https://www.congress.gov/bill/116th-congress/senate-bill/2749/text

- The contract with the .gov vendor and its statement of objectives.
- The handbook for the DotGov Program, which details daily operations for screening/approving new domain requests and describes communication flow with the .gov contractor.
- "Authority to operate", or ATO, documentation, which outlines the security controls that apply to the .gov TLD infrastructure the contractor operates. This also includes relevant executive branch security and privacy documentation such as the TLD's high value asset paperwork and privacy threshold assessment information.
- Historic documentation, including presentations and legacy policies.

Digital Assets

Most of the key operational infrastructure for the .gov TLD (particularly the authoritative nameservers and the .gov registrar) is maintained by the .gov contractor, which will continue under a program transition to CISA. However, several digital assets will transfer from GSA to CISA. These include:

- The registration for the domains 'dotgov.gov' and 'nic.gov'
- GSA's 'dotgov-home' GitHub repository[2] and the portion of GSA's 'data' repository that house .gov information[3]
- Management of the web publication platform that powers the DotGov Program website

CISA staff obtained administrative accounts to the .gov register and are trained by GSA's DotGov staff in processing new domain requests and publishing new .gov domain data.

Authority to Operate (ATO)

The ATO documentation was transmitted to CISA. CISA intends to accept the ATO that GSA prepared, which was approved by GSA within the last few months. Though executive branch agencies have different methods of approving and authorizing systems for production use, CISA does not anticipate any major changes to documentation (and, thereby, related system controls) in order to satisfy Department of Homeland Security IT security requirements, or those requirements that stem from CISA's High Value Asset (HVA) directive[4] or OMB's HVA memo[5].

Similarly, GSA's privacy documentation is slightly different from DHS's, but the CISA DotGov Program has prepared new privacy documents in alignment with Department processes and anticipates no system changes.

[2] https://github.com/GSA/dotgov-home/
[3] https://github.com/GSA/data/tree/master/dotgov-domains
[4] Binding Operational Directive 18-02, https://cyber.dhs.gov/bod/18-02/
[5] OMB Memorandum 19-03 https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

Providing Notice to Relevant Internet Governance Organizations

The internet's DNS is a distributed system, but its management is not decentralized. GSA has notified the Public Technical Identifiers (PTI), an affiliate of the Internet Corporation for Assigned Names and Numbers (ICANN) and which manages the Internet Assigned Numbers Authority (IANA) functions, of the change in administrator of the .gov TLD to CISA. GSA also notified the Department of Commerce's National Telecommunications and Information Administration, which has a historic and continuing role in coordinating internet governance issues on behalf of the U.S. Government about the transition.

Because the .gov TLD's nameservers, the servers that put .gov on the internet, are not changing as part of this transition – those will still be managed by the .gov contractor – the change occurring at PTI is administrative in nature, not technological.

Contractual

Fund

Current

Funding for the DotGov Program and its support contract were not in CISA's FY21 budget request or in the Consolidated Appropriations Act, 2021 (Pub. L. 116-260). CISA, GSA and OMB worked together to determine the best path forward for the current and forthcoming fiscal year. In December 2020, GSA funded the current contract through the end of the period of performance. CISA reprogrammed funds for the DotGov Programs to account for current fiscal year costs, and has requested FY22 finds. As required, CISA began "operationally administering" the DotGov Program by the date required in Section 907(c) of the DOTGOV Act (April 26, 2021).

The .gov contract, which includes operating the .gov nameservers, the .gov registrar, a help desk, and some ancillary support services, is in its final option year, closing December 2021. This adds further urgency on top of the requirements and timelines of the DOTGOV Act. A significant portion of CISA's effort this calendar year is to prepare and execute a new contract strategy. Given the nature of acquisition timelines and the responsibility to review and grant an ATO for any new .gov infrastructure in future awards and seamlessly migrate to it, CISA may require a short-term bridge contract to ensure continued stability in .gov TLD operations.

Future

The .gov TLD is critical infrastructure for U.S.-based government organizations – but the TLD has never been fully funded through appropriation in its roughly 35-year existence, instead relying in part on user fees that are kept by the vendor.

The DOTGOV Act states Congress' findings that "the .gov internet domain should be available at no cost or a negligible cost to any Federal, State, local, or territorial government-operated or publicly controlled entity, including any Tribal government recognized by the Federal

Government or a State government, for use in their official services, operations, and communications". Consistent with this intent, CISA removed user fees as part of the transition via a payment to the support contractor.

Keeping user fees removed in the future, or ensuring they are significantly decreased, consistent with Congress' finding, is a key goal for CISA because it enables all U.S.-based government organizations to obtain a .gov domain name without high cost; .gov domains were $400 per year from 2017 to 2021 whereas .us and .org domains average approximately $12 per year. Consistent with Congress' finding to add new "supporting services" enables a new operating model, where near-term fixes and long-term enhancements increase security across the .gov ecosystem.

Supporting the program with appropriations while phasing out user fees, consistent with Congress' findings, and re-architecting support contracts is key to keeping program costs down while adding the new services contemplated in the Act (under Section 2215(e) of the Homeland Security Act of 2002, as added by Section 904(b)(1)(B) of the DOTGOV Act). Doing so demonstrates that the program is an integral part of CISA's efforts to fulfill its statutory duties to protect the nation from cyber threats and puts it on similar footing as other vital cybersecurity initiatives CISA manages.

IV. Conclusion

The DOTGOV Act outlines the rationale for and responsibilities of the .gov TLD. Administering the .gov TLD enables CISA to set secure defaults on a platform many government organizations already use and offer services to support the "security, privacy, reliability, accessibility, and speed" of their domain (Section 2215(e) of the Homeland Security Act of 2002, as added by Section 904(b)(1)(B) of the Act). The TLD strengthens CISA's ability to defend the nation from today's cyber threats and provides central insight into certain classes of threats to help secure against tomorrow's attacks. Under the actions required by the Act, we expect our work will increase security and decrease complexity, particularly for state and local government organizations. We look forward to interacting with federal and non-federal government organizations – current and future users alike – to provide a valuable service to them and the public.

V. Appendix: List of Acronyms

Acronym	Expansion
CISA	Cybersecurity and Infrastructure Security Agency
DNS	Domain Name System
DOTGOV	DOTGOV Online Trust in Government Act of 2020
FISMA	Federal Information Security Modernization Act of 2014
GSA	U.S. General Services Administration
HVA	High Value Asset
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
OMB	Office of Management and Budget
PTI	Public Technical Identifiers
SLTT	State, Local, Tribal, and Territorial
TLD	Top-level domain