

U C B E R K E L E Y
C E N T E R F O R L O N G - T E R M C Y B E R S E C U R I T Y



C L T C W H I T E P A P E R S E R I E S

Building Trust: Quantifying Use of the .gov Domain Below the Federal Level

C H R I S B A B C O C K

CLTC WHITE PAPER SERIES

Building Trust: Quantifying Use of the .gov Domain Below the Federal Level

CHRIS BABCOCK

The views expressed in this paper are those of the author and do not reflect the official policy or position of the U.S. government or the Department of Defense.

This report was published as part of the Center for Long-Term Cybersecurity's 2025 Public Interest Cybersecurity Research Call for Papers and was presented in June at the 2025 Cyber Civil Defense Summit.

September 2025

Contents

EXECUTIVE SUMMARY	1
INTRODUCTION	3
LITERATURE REVIEW	4
METHODOLOGY	10
RESULTS AND ANALYSIS	13
Section 1: Current Status of SLTT-I Entities	13
Section 2: Potential Barriers to .gov Adoption	21
RECOMMENDATIONS	24
APPENDIX A - STATE ANALYSIS	29
APPENDIX B - LOCAL DATA	31
APPENDIX C - TRIBAL DATA	39
REFERENCES	46
ACKNOWLEDGMENTS	49
ABOUT THE AUTHOR	50

Executive Summary

Trust in digital government services relies on users' ability to verify that websites and emails genuinely represent official institutions. The .gov top-level domain (TLD), managed by the Cybersecurity and Infrastructure Security Agency (CISA), serves as a trusted and secure digital identifier. Despite its benefits, adoption of the .gov domain below the federal level remains uneven and, in many cases, minimal. Worse, inconsistent, unstandardized, or unnecessarily complex uses of .gov risk eroding the very trust the domain is intended to provide.

This paper presents the first comprehensive analysis of .gov domain adoption across all non-federal U.S. government entities, collectively referred to as SLTT-I (state, local, tribal, territorial, interstate/intertribal). The study uses a mixed methods research approach to answer the question, "What are the adoption rates of the .gov TLD among SLTT-I entities in 2025, and what barriers might these entities face in adopting .gov?"

KEY FINDINGS

- **States:** All 50 U.S. states use .gov domains, but with significant variation. Some states, like Mississippi and California, demonstrate highly efficient domain usage through centralized and standardized structures. Others, such as Florida and Arizona, rely on fragmented and duplicative domain registration practices. The vast majority of state-level domains are held by executive branches (87.7%), with legislative and judicial branches underrepresented.
- **Local Governments:** Local jurisdictions make up nearly 99% of all entities eligible to use .gov, but account for only 85.7% of .gov registrations. Adoption is highly skewed: counties exhibit the highest adoption (78.5%), while school districts are drastically underrepresented (0.25%). Special districts, i.e., local governments created to deliver services not provided by cities and counties, also show low adoption (1.7%). Many localities likely remain unaware of their eligibility to use .gov domains or lack the capability to transition.
- **Tribal Nations:** Among 574 federally recognized tribes, only 194 (33.8%) have registered a .gov domain. State-recognized tribes show even lower adoption (5%). Most

tribes register only one domain, though some use .gov domains solely for redirection to unofficial sites, undermining the trust and simplicity inherent to the .gov structure.

- **Territories:** All six U.S. territories use .gov domains for executive branch functions. Legislative and judicial branch adoption is inconsistent. Some territories redirect from .gov to unofficial top-level domains (TLDs), such as .pr for Puerto Rico, which may reduce credibility and condition users to be more susceptible to cybersecurity risks.
- **Interstate and Intertribal Entities:** Of an estimated 272 eligible interstate or intertribal entities, only 24 use .gov domains. CISA's public dataset of .gov domains contains misclassifications in this category (domains listed as interstate actually represent other SLTT-I categories). Additionally, CISA's policies and public data structure do not explicitly address intertribal eligibility as a distinct category.

RECOMMENDATIONS

1. **Federate and standardize local use of the .gov domain:** Congress should authorize CISA to delegate to states, tribes, and territories the management of local domains and require local entities to use standardized subdomains (e.g., cityname.state.gov). In the interim, CISA should offer incentives (like enhanced protections and DNS services) for jurisdictions that adopt this model.
2. **Narrow allowable domain criteria:** CISA should limit each SLTT-I entity to a default cap on the number of their registered domains (e.g., 12 domains) and promote the use of subdomains or pages to reduce unnecessary domain proliferation and increase public trust.
3. **Promote enrollment and domain literacy:** Outreach efforts focused on encouraging the use of .gov domains should prioritize high-risk and underrepresented groups, such as school districts and election authorities. Digital literacy campaigns should educate the public on recognizing .gov as a sign of official status.
4. **Reconsider governance models for .gov:** Congress should study the feasibility of a federated governance framework, such as a multi-stakeholder council or statutory judicial review process, to mitigate potential concerns over CISA's unilateral revocation authority.

Introduction

U.S. state, local, tribal, territorial, interstate or intertribal (SLTT-I), and other publicly controlled entities maintain a diverse online presence to serve the public. School boards post meeting notices and minutes, and county websites help voters register and locate polling places; city court portals allow residents to pay fines and access dockets, and state websites provide tax filing instructions. SLTT-I entities also use email to communicate internally and externally with citizens, private organizations, and other governments.

Trust is at the center of all of these interactions. The information exchanged with U.S. governments online often includes highly sensitive data like tax records, law enforcement details, and voter registration information. For individuals or organizations to confidently engage with a government online, they must first trust that the website or email address genuinely represents that entity. The .gov top-level domain (TLD) is provided by the U.S. Cyber and Infrastructure Security Agency (CISA) and serves as a free, secure, and trusted resource that signals official status for U.S. governments and publicly controlled entities on the internet.

While prior research has examined .gov adoption within specific subsets of SLTT-I entities (particularly those involved in election administration), no comprehensive study has assessed adoption rates across all SLTT-I categories. Without a comprehensive understanding of SLTT-I adoption rates, CISA cannot effectively manage or secure the TLD. Additionally, without such an accounting, Congress and the public cannot meaningfully understand or debate the value, challenges, and opportunities of building and sustaining trust online using the .gov TLD.

This paper addresses that gap by using a mixed methods research approach to answer the question, “What are the adoption rates of the .gov TLD among SLTT-I entities in 2025, and what barriers might these entities face in adopting .gov?”

Literature Review

THE .GOV TOP-LEVEL DOMAIN

SLTT-I and other publicly controlled entities register internet domains to provide the public with a stable, memorable, and easily accessible way to find their websites and communicate using email. Domains serve as human-readable translations of numerical Internet Protocol (IP) addresses through the Domain Name System (DNS). DNS is a critical protocol that allows users to navigate the internet without needing to remember complex numerical strings.

At the core of DNS are top-level domains (TLDs). The most common TLD is .com, which accounts for almost half of all registered domains globally.¹ However, the Internet Assigned Numbers Authority (IANA) now recognizes 1,592 distinct TLDs,² each managed by a registry operator that is responsible for maintaining the TLD and overseeing domain registrations. Domain names are typically acquired either directly from a registry operator or through an intermediary known as a registrar.

While most TLDs are available for general use, a small subset known as sponsored TLDs (sTLDs) are restricted to specific categories of users. These domains are governed by rules set by their sponsoring registry operator and serve as a signal of legitimacy. For example, the .edu TLD is reserved for accredited higher education institutions, and .mil is restricted to the U.S. military. The .gov domain, an sTLD, is managed by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), which assumed control of it in March 2021 after Congress passed the DOTGOV Online Trust in Government Act of 2020.³ CISA is required by the act to:

1. Make the .gov TLD available to agencies of the federal government, SLTT-I, and other publicly controlled entities;
2. Minimize the risk of misleading or confusing .gov domain names;

1 Szurdi, Janos. 2021. "A Peek into Top-Level Domains and Cybercrime." Unit42. November 11, 2021. <https://unit42.paloaltonetworks.com/top-level-domains-cybercrime/>.

2 Internet Assigned Numbers Authority. "Root Zone Database." Internet Assigned Numbers Authority. <https://www.iana.org/domains/root/db>.

3 U.S. Government. "Requirements for the registration and use of .gov domains in the federal government." Digital.gov. <https://digital.gov/resources/requirements-for-the-registration-and-use-of-gov-domains-in-the-federal-government>.

3. Convey that .gov domains cannot serve commercial or political campaign purposes;
4. Prevent unauthorized domain registration; and
5. Minimize information collection and sharing with other parts of the federal government, other than to improve the provision and administration of the domain.⁴

In accordance with the act, CISA administers .gov for exclusive use by the U.S. federal government, and for eligible SLTT-I and other publicly controlled entities. The value of the .gov domain stems largely from this exclusivity. CISA verifies the eligibility of each applicant, ensuring that only legitimate publicly controlled entities such as SLTT-I are granted domains. As a result, individuals, private organizations, and other governments can be confident that any website or email using .gov is operated by an authorized U.S. government entity. Additionally, .gov domains are free for eligible SLTT-I entities and include some performance and security enhancements provided by CISA.

However, these benefits come with trade-offs. Because CISA acts as the registry operator, it retains ultimate authority over the use of .gov domains. This means that entities that adopt .gov cede control over access to their public-facing digital presence. If CISA determined that a domain should be revoked, it could act unilaterally and rapidly by removing the entry from its DNS records, rendering associated websites and email addresses inaccessible within minutes. Although the hosted content would remain intact, it would be essentially inaccessible until the affected entity established and notified its constituencies of its new domain, a process that would be complex and time-consuming, and would make the affected entity acutely vulnerable to impersonation attacks.

DOMAIN-RELATED ATTACKS

Malicious cyber actors exploit a variety of techniques to achieve objectives such as phishing, malware distribution, and online fraud. In a study of domain abuse between 2019 and 2020, Zhanhao Chen and Janos Szurdi of Palo Alto Networks' Unit 42 identified eight categories of

4 U.S. House of Representatives. "6 USC 665: Duties and authorities relating to .gov internet domain." U.S. Code. [https://uscode.house.gov/view.xhtml?req=\(title:6%20section:665%20edition:prelim\)%20OR%20\(granuleid:USC-prelim-title6-section665\)&f=treesort&edition=prelim&num=0&jumpTo=true](https://uscode.house.gov/view.xhtml?req=(title:6%20section:665%20edition:prelim)%20OR%20(granuleid:USC-prelim-title6-section665)&f=treesort&edition=prelim&num=0&jumpTo=true).

attacker objectives, and further organized six prevalent methods used to deceive users by impersonating legitimate domains, collectively known as cybersquatting techniques.⁵

Cybersquatting refers to the use of domain names that closely resemble authentic ones, with the intent to mislead users. Attackers may impersonate legitimate websites to perform credential harvesting; steal credit, debit, or bank account information; or steal personally identifiable information for use in identity theft. In the worst cases, these types of attacks could be used to damage U.S. national security if conducted as part of a foreign campaign of subversion. These techniques exploit users' assumptions, visual shortcuts, and trust in familiar naming patterns.

Table 1 summarizes the six most common cybersquatting techniques identified by Chen and Szurdi and highlights whether each is mitigated by the use of the .gov TLD. As the table shows, the use of .gov domains mitigates five of the six cybersquatting methods. Because attackers cannot register .gov domains unless they are verified U.S. government entities,⁶ malicious actors are effectively denied the ability to imitate .gov addresses. This TLD restriction introduces a visible mismatch between authentic and attacker-controlled domains, providing an additional layer of defense. For example, while an attacker may register login-example.com, they cannot register login-example.gov.

However, the effectiveness of .gov as a cybersecurity control depends on users recognizing .gov as the only legitimate TLD for a given SLTT-I entity. If users expect a government entity to use .com, .org, or .us instead, the protective value of .gov diminishes. Accordingly, successful adoption of .gov as a trust-enhancing tool requires more than just domain registration. It depends on digital literacy among users, consistent branding by SLTT-I entities, and public communication strategies that reinforce .gov as the authoritative domain for government services.

⁵ Chen, Zhanhao, and Janos Szurdi. "Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers." Unit 42, September 1, 2020. <https://unit42.paloaltonetworks.com/cybersquatting/>.

⁶ For the purposes of this study, it is assumed that attackers would always be denied the opportunity to register or leverage a .gov domain for their attacks. This assumption may not be true. The degree to which CISA protects existing .gov domains and prevents unauthorized registrations was not investigated within the scope of this research, but is a potential area for further study.

Table 1. Cybersquatting Techniques

Technique	Description	Mitigated by .gov
Typosquatting	<i>Use of misspelled variants of a domain</i> Authentic: example.com Attacker: exem p le.com	Yes – more than one factor distinguishes the authentic and attacker domains Authentic: example.gov Attacker: exem p le. com
Combosquatting	<i>Addition of a believable phrase to a domain</i> Authentic: example.com Attacker: login-example.com	Yes Authentic: example.gov Attacker: login-example.com
Homographsquatting	<i>Use of foreign characters to visually mimic a domain</i> Authentic: example.com Attacker: èxample.com	Yes Authentic: example.gov Attacker: èxample.com
Soundsquatting	<i>Use of similar sounding words or spellings to phonetically mimic a domain</i> Authentic: example.com Attacker: ecsample.com	Yes Authentic: example.gov Attacker: ecsample.com
Bitsquatting	<i>Exploits the potential for single-bit errors in computer processing</i> Authentic: example.com Attacker: dxample.com	Yes Authentic: example.gov Attacker: dxample.com
Levelsquatting	<i>Uses authentic domain as a subdomain</i> Authentic: example.com Attacker: example.com.blog	No – only one factor (addition of the .blog domain) distinguishes the authentic and attacker domains Authentic: example.gov Attacker: example.gov. blog

DIGITAL LITERACY

The risks associated with poor digital literacy are illustrated by a campaign described by Unit 42 in April 2025, in which attackers impersonated the U.S. Internal Revenue Service (IRS).⁷

7 Ramesh, Reethika, and Zhanhao Chen. “IRS-themed Domains Used for CAPTCHA-Style Paste Hijacking Pages.” GitHub. April 15, 2025. <https://github.com/PaloAltoNetworks/Unit42-timely-threat-intel/blob/main/2025-04-15-IOCs-for-IRS-themed-domains-used-in-CAPTCHA-style-paste-hijacking.txt>.

Unable to obtain a domain under the restricted .gov top-level domain, the attackers instead relied on levelsquatting, a technique that embeds the string “.gov” within a subdomain of a non-government TLD (e.g., example.gov.blog, where “.blog” is the true TLD) to mislead users. Levelsquatting in this context exploits the assumption that the appearance of “.gov” anywhere in a web address signals authenticity.

Research has shown that users tend to form trust judgments quickly about websites based on simple heuristics (for example, using cues based on the visual design of the website),⁸ but that some users browse with a more sophisticated approach that allows them to more reliably detect inconsistencies by critically examining cues.⁹ This underscores the potential role of SLTT-I entities in fostering trust through deliberate and strategic choices about their online presence. By adopting .gov domains and educating the public about their significance, U.S. government organizations and their partners can reinforce digital trust and reduce the effectiveness of domain-based deception.

PRINCIPLES OF TRUST

A multidisciplinary review of research from psychology, behavioral economics, sociology, and marketing highlights three key attributes that organizations can leverage to build trust: simplicity, consistency, and standardization. These attributes are especially relevant for SLTT-I entities seeking to build and maintain trust in their digital interactions with the public.

- **Simplicity:** From the field of psychology, the concept of cognitive fluency is central. Cognitive fluency refers to the ease with which a person processes information. Research shows that the simpler an experience or design is to process, the more trustworthy it is perceived to be.¹⁰ This insight has practical implications for SLTT-I domain-naming practices: shorter, more intuitive domain names increase cognitive fluency and, by extension, user trust. For example, a domain like townsville.

8 Metzger, Miriam J., and Andrew J. Flanagin. “Psychological Approaches to Credibility Assessment Online.” *The Handbook of the Psychology of Communication Technology*, First Edition, ed. by S. Shyam Sundar (John Wiley & Sons, Inc., 2015), 451.

9 Wineburg, Sam, and Sarah McGrew. “Lateral Reading and the Nature of Expertise: Reading Less and Learning More When Evaluating Digital Information.” *Teachers College Record*, 2018. https://stacks.stanford.edu/file/druid:yk133ht86o3/Wineburg%20McGrew_Lateral%20Reading%20and%20the%20Nature%20of%20Expertise.pdf.

10 Alter, Adam L., and Daniel M. Oppenheimer. “Uniting the Tribes of Fluency to Form a Metacognitive Nation.” *Personality and Social Psychology Review*, vol.13, no. 3 (2009). <https://doi.org/10.1177/1088868309341564>.

mo.gov is likely to inspire more trust than a more complex alternative such as thecityoftownsvilleinmo.gov, even though both could be valid under CISA policy.¹¹

- **Consistency:** The field of behavioral economics adds another insight: consistency reduces uncertainty and enhances trust. As demonstrated in the work of Daniel Kahneman and others, people rely on consistent cues when forming judgments under uncertainty.¹² Marketing research reinforces this principle. Brand consistency strengthens trust by setting clear expectations over time.¹³ Zajonc’s work on the exposure effect further supports the idea that repeated exposure to a consistent experience increases perceived trustworthiness.¹⁴ For CISA and SLTT-I organizations, these findings suggest that domain structures, naming conventions, and presentation styles should be consistent across websites and emails.
- **Standardization:** A key concept in sociology, standardization also plays a powerful role in building trust. Zucker argues that standardized processes (especially those that appear routine or institutionalized) communicate stability and reliability.¹⁵ This suggests that SLTT-I entities should not only aim for internal consistency but also adopt shared standards that reinforce a collective sense of order and legitimacy.

Together, the three principles — simplicity, consistency, and standardization — provide a conceptual foundation for policy and design decisions that can significantly enhance public trust in government digital services.

11 Cybersecurity and Infrastructure Security Agency. “Choosing your .gov domain name.” CISA. Accessed on June 1, 2025. <https://get.gov/domains/choosing>.

12 Kahneman, Daniel. *Thinking Fast and Slow* (Farrar, Straus and Giroux, 2013).

13 Keller, Kevin Lane. “Conceptualizing, Measuring, and Managing Customer-Based Brand Equity.” *Journal of Marketing* 57, no. 1 (1993), pages 7-8. <http://www.jstor.org/stable/1252054>.

14 Obermiller, Carl. “Varieties of Mere Exposure: The Effects of Processing Style and Repetition on Affective Response.” *Journal of Consumer Research*, vol. 12, no. 1 (1985), pages 18–19. <http://www.jstor.org/stable/2489378>.

15 Zucker, Lynne G. “Production of trust: Institutional sources of economic structure, 1840–1920.” *Research in Organizational Behavior*, vol. 8, (1986), pages 53–111. <https://digicoll.lib.berkeley.edu/record/70599>.

Methodology

TOTAL NUMBER OF ELIGIBLE SLTT-I ENTITIES

To estimate the total number of SLTT-I entities eligible to use the .gov domain, this study compiled and synthesized data from multiple authoritative sources. For the purposes of this analysis, the executive, legislative, and judicial branches are treated as a single entity at the state, tribal, territorial, and local levels. This approach reflects a simplified structural model, though it does not fully capture the complexity of governance in certain jurisdictions. Many tribal nations maintain unique governance structures with competing sovereign branches, and several states use a plural executive model in which independently elected department heads serve as distinct centers of authority within the executive branch.

Due to the diverse and often jurisdiction-specific nature of SLTT-I internal branch structures, this paper treats each SLTT-I entity as one unit rather than counting each sovereign branch. A valid alternative methodology would treat each sovereign branch or office as a separate eligible SLTT-I entity. Under such an approach, the estimates presented in this paper would represent a lower bound on the true size of the eligible SLTT-I population.

DOMAIN REGISTRATION DATA

To evaluate .gov adoption rates below the federal level, data were drawn primarily from the CISA .gov registrant list, obtained from CISA's dotgov-data GitHub repository on April 10, 2025 ("current-full.csv").¹⁶ Internet searches and manual review were conducted to assess the accuracy of select data subsets, specifically for states, territories, and interstate/intertribal domains, as those datasets were relatively small. Due to the overall dataset size (11,273 unique domain entries across five fields), only limited data cleaning and normalization procedures were performed. More extensive normalization was constrained by the lack of jurisdiction-specific context, which made it difficult to determine when multiple domains represented a single SLTT-I entity.

¹⁶ Cybersecurity and Infrastructure Security Agency. "Official list of .gov domains" GitHub. Accessed on April 10, 2025. <https://github.com/cisagov/dotgov-data>.

For state-level analysis, two additional steps were taken. First, targeted web searches were conducted to identify branch-specific websites in states that appeared to lack domains for one or more of their three branches. This process revealed cases in which state branches used unofficial domains or hosted their websites as subdomains under another branch's domain. Second, a utilization efficiency metric was calculated for each state by standardizing the number of registered domains using z-scores. Utilization efficiency is defined here as the number of registered domains required to achieve comparable functions.

The z-scores were calculated by subtracting the mean number of domains from each state's total domain count and dividing by the standard deviation: $Z = \frac{\chi - \mu}{\sigma}$. This method allows comparative utilization efficiency to be studied without regard for the absolute number of domains registered by a state. States were grouped into one of five utilization efficiency categories based on their score Very High ($z < -0.5$), High ($-0.5 \leq z < 0$), Moderate ($0 \leq z < 1$), Low ($1 \leq z < 2.5$), and Very Low ($z \geq 2.5$). Category thresholds were selected due to the data exhibiting a long tail of low to moderate values with two strong outlier states.

LIMITATIONS

This study is subject to several key limitations, including:

1. Pre-existing errors in the CISA dataset, such as misclassified entries;
2. Exclusion of subdomains, which are not captured in CISA's registrant list and may lead to undercounting;
3. Duplicate representation of entities, where multiple unique domains in the dataset may correspond to a single SLTT-I entity, potentially leading to overcounting;
4. Unmeasured use of unofficial domains, such as .com, .org, or .us, by eligible SLTT-I entities; and
5. An unmeasured number of eligible SLTT-I entities that have no website or email at all.

No automated tools were used to detect or quantify the use of subdomains, unofficial domains, or the absence of digital infrastructure. While future research could leverage tools to address these gaps, domain attribution remains a complex challenge due to the scale and diversity of the SLTT-I landscape.

BUILDING TRUST

Additionally, no direct surveys of SLTT-I entities were conducted to assess reasons for .gov adoption or non-adoption. Instead, secondary and tertiary sources were used to develop initial hypotheses about factors that may influence domain choices. Each of these limitations points to opportunities for future research.

Results and Analysis

SECTION 1: CURRENT STATUS OF SLTT-I ENTITIES

Overview

This section describes the findings for the overall number of eligible jurisdictions and .gov domain registrations, and specific findings within the state, local, tribal, territory, and interstate/intertribal categories. This study finds that there are 91,801 sub-federal entities in the U.S. that are eligible to register a .gov domain, and that 89% of the 12,636 unique .gov domains in CISA's public dataset are attributable to sub-federal organizations. Within the 50 U.S. states, state-level use of the .gov TLD varies widely, with many highly efficient states (those that use between 2-12 domains for all state needs) and two outlier states that use over 100 state-level domains. State-level use of .gov between and within branches is often inconsistent and unstandardized. At the local level, school districts and counties contrast as having very low and very high domains-per-jurisdiction, respectively. Federally recognized tribal nations are almost seven times more likely to use the .gov domain than are tribes that are only recognized by a state. All executive branches within the territories use .gov, but the judicial and legislative branches exhibit inconsistent use. Finally, this study assesses that only 10% of eligible interstate/intertribal entities use the .gov domain. This assessment is made with low confidence due to challenges in measuring the overall number of eligible entities in this category.

Eligible Jurisdictions

The total estimated number of eligible SLTT-I entities in the United States is presented in Table 2. This count draws from multiple authoritative sources. For tribal entities, the U.S. Bureau of Indian Affairs recognizes 574 federally recognized tribes and Alaska Native entities,¹⁷ while an additional 63 tribes are recognized exclusively at the state level.^{18, 19, 20}

17 U.S. Government. "Federally recognized American Indian tribes and Alaska Native entities." Last modified March 25, 2025, <https://www.usa.gov/indian-tribes-alaska-native/>.

18 Koenig, Alexa, and Jonathan Stein. "Federalism and the State Recognition of Native American Tribes: A Survey of State-Recognized Tribes and State Recognition Processes across the United States." *Santa Clara Law Review*, vol. 48, no. 1 (2008), page 83. Accessed at <https://digitalcommons.law.scu.edu/lawreview/vol48/iss1/2>.

19 National Conference of State Legislatures. "Federal and State Recognized Tribes." Archived by the Internet Archive on September 1, 2022, <https://web.archive.org/web/20220901061023/https://www.ncsl.org/legislators-staff/legislators/quad-caucus/list-of-federal-and-state-recognized-tribes.aspx>.

20 Native Nations Institute at the University of Arizona. "Governance Under State Recognition." Accessed April 19, 2025, <https://nni.arizona.edu/our-work/research-policy-analysis/governance-under-state-recognition>.

The local level includes four primary types of government: counties, municipalities (including cities, towns, and villages), special districts (such as water, utility, or fire districts), and independent school districts. The U.S. Census Bureau’s 2022 Census of Governments provides official counts for these categories, which are shown in the table.²¹

Table 2. SLTT-I Category Comparisons

Category - Subcategory	Jurisdictions in the U.S.	Percent of Total
State	50	0.05%
Local	90,837	98.95%
Local - County	3,033	3.30%
Local - Municipality	35,705	38.89%
Local - Special District	39,555	43.08%
Local - School District	12,546	13.67%
Tribal	637	0.69%
Tribal - Federally Recognized	574	0.63%
Tribal - State Recognized	63	0.07%
Territory	6	<0.01%
Interstate / Intertribal	272	00.30%
Total	91,801	100.0%

Interstate and intertribal organizations, defined as entities comprising two or more states or tribes, present a more complex case. There is no centralized or authoritative count of all such entities. However, the National Center for Interstate Compacts lists 270 active compacts, which this paper uses as a proxy for the number of interstate organizations.²² Two intertribal entities were identified in CISA’s .gov registrant data, though others likely exist.²³ Due to the lack of CISA policy explicitly addressing intertribal eligibility, this paper does not attempt to estimate the total number of qualifying intertribal organizations.

Based on the best available data, this paper estimates that 91,801 sub-federal entities in the U.S. are eligible to register a .gov domain.

21 Census Bureau. “2022 Census of Governments - Organization.” Last revised April 23, 2025, <https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html>.

22 National Center for Interstate Compacts. “NCIC Database.” Last updated April 7, 2025, <https://compacts.csg.org/database/>.

23 Although CISA does not distinguish between tribes and intertribal organizations in its registrant data, this paper considers the intertribal organizations found on CISA’s .gov registrant list to be bonafide eligible entities due to the fact that CISA approved their requests for domains.

Domain Registrant Data

As of April 10, 2025, CISA listed 12,636 unique .gov domains in its public dataset. Of these, 89% were attributed to SLTT-I entities, with the remaining 11% classified as federal. This analysis focuses on the SLTT-I subset of the data, which comprises 11,237 domain registrations, as shown in Table 3. While only limited data cleaning was performed due to the size and complexity of the dataset, apparent categorization errors were corrected when encountered.

Table 3. Registered Domain Category Comparisons

Category - Subcategory	Domains Registered	Percent of Total
State	1,295	11.52%
Local	9,628	85.68%
Local - County	2,380	21.18%
Local - Municipality	6,554	58.33%
Local - Special District	663	5.90%
Local - School District	31	0.28%
Tribal	258	2.30%
Tribal - Federally Recognized	255	2.27%
Tribal - State Recognized	3	0.03%
Territory	32	0.28%
Interstate / Intertribal	24	0.21%
Total	11,237	100.0%

States

Although states account for only 0.05% of all eligible SLTT-I entities, they represent a disproportionately large share of all non-federal .gov domain registrations, at 11.52%. All 50 states utilize the .gov domain in some capacity. As outlined in the methodology section, this paper assesses state-level domain utilization efficiency using z-scores to compare how many domains each state has registered relative to the national average. This paper defines domain utilization efficiency as the number of registered domains required to achieve comparable functions. A state with high efficiency uses few domains relative to the national average, whereas a state with low efficiency uses more. As shown in Table 4, most states exhibit high or very high utilization efficiency. Twelve states fall into the moderate or low categories, while Florida and Arizona stand out with very low efficiency. A full table with domain counts, z-scores, and utilization efficiency is included in Appendix A.

Table 4. U.S. States' Domain Utilization Efficiency

Very High	High	Moderate	Low	Very Low
Mississippi (2)	Idaho (13)	Montana (27)	Tennessee (53)	Florida (102)
California (3)	Illinois (14)	Wisconsin (31)	New Jersey (57)	Arizona (143)
Hawaii (4)	Virginia (16)	West Virginia	Ohio (58)	
Missouri (4)	Maryland (18)	(37)	Kansas (64)	
Utah (4)	Maine (18)	Colorado (37)	Iowa (67)	
Delaware (5)	Nebraska (18)	Texas (38)	North Carolina	
New Hampshire	New York (18)	Alabama (41)	(68)	
(6)	Pennsylvania (18)			
Georgia (8)	Oklahoma (19)			
Minnesota (8)	Wyoming (19)			
Kentucky (9)	Michigan (19)			
Washington (9)	North Dakota (21)			
Alaska (10)	Nevada (21)			
New Mexico (10)	Oregon (21)			
South Dakota (10)	Massachusetts			
Connecticut (11)	(22)			
Rhode Island (11)	South Carolina			
Arkansas (12)	(23)			
Indiana (12)	Louisiana (24)			
Vermont (12)				

Each state's total number of domains registered with CISA is listed in parenthesis after the state name.

A preliminary comparison of states at the extremes (those with very high and very low domain utilization efficiency) suggests that underlying policy choices (or inaction) by states to organize their use of .gov domains may explain these differences. It is unlikely that a state would achieve high efficiency by chance, particularly given the decentralized nature of state government structures. The existence of separate branches and the frequent use of a plural executive model introduce more centers of decision-making, increasing the likelihood of fragmented domain registration. High efficiency, then, likely results from deliberate efforts to coordinate domain use.

This paper hypothesizes two contrasting models of domain governance at the state level: an organized approach and an opportunistic approach. In the organized approach, the state implements policies or laws to govern domain usage, centralizing web presence and limiting redundant domain registrations. In the opportunistic approach, state agencies are free to register .gov domains independently, often without a unifying framework guiding naming conventions or consolidation.

Mississippi exemplifies the organized approach. The state uses a centralized domain (ms.gov), with many agencies and services hosted as pages or subdomains. This model aligns with

principles of simplicity, consistency, and standardization. By contrast, Florida illustrates the opportunistic model. Its Department of Health alone holds 33 separate .gov domains, each dedicated to narrow topics such as youth vaping prevention (“http://endteenvapingfl.gov”) or licensure for orthotists and prosthetists (“http://floridasorthotistsprosthetists.gov”). Florida’s Agency for Health Care Administration maintains four more .gov domains. Altogether, Florida’s health-related agencies alone use more unique .gov domains than the total number of domains registered by most other states.

Overreliance on unique domains runs counter to the common web design practice of utilizing subdomains or pages to manage content. In most sectors, users expect to complete all interactions for a given organization within a single domain. For instance, a clothing retailer would typically host all product categories on pages within a single domain (e.g., brand.com/fall-line/), rather than creating separate domains for each season (e.g., brand-fall-line.com, brand-spring-clearance.com). Fragmenting content across multiple domains creates friction for users by violating their expectations and runs contrary to the principles of simplicity and consistency.

Further variation exists in how different branches of state government use the .gov domain. As shown in Table 5, the executive branch dominates state-level domain registrations, accounting for 87.7% of the total. The legislative and judicial branches account for only 5.5% and 6.8%, respectively. While most states use .gov domains across all three branches, notable exceptions exist. The judicial branches in Hawaii, Oklahoma, Pennsylvania, and South Carolina use unofficial TLDs (e.g., .com, .org, .net).²⁴ Additionally, Massachusetts, Michigan, and Texas use the unofficial .us TLD to host voter and election information.²⁵

Example: Connecticut’s main judicial branch website is hosted as a subdomain under the executive branch site ct.gov, but the judicial branch also maintains a dedicated probate court domain (ctprobate.gov). All Connecticut legislative branch websites are hosted as subdomains under the ct.gov domain (e.g., cga.ct.gov).

Table 5. State Branch Comparisons

Category - Subcategory	Domains Registered	Percent of Total
Executive	1,136	87.72%
Legislative	71	5.48%
Judicial	88	6.80%
Total	1,295	100.0%

24 URLs: <https://www.courts.state.hi.us/>, <https://www.oscn.net/v4/>, <https://www.pacourts.us/>, <https://www.sccourts.org/>.

25 URLs: <https://www.sec.state.ma.us/OVR/>, <https://mVIC.sos.state.mi.us/Voter/Index>, <http://www.sos.state.tx.us/index.shtml>.

The structural organization of domains within states also varies. In many cases, the legislative branch operates as a subdomain under an executive domain (e.g., “senate.mo.gov” and “house.mo.gov”). Less commonly, all three branches share a domain space, or the judicial branch is nested under the executive while the legislative branch maintains an independent domain. Even within branches, inconsistencies stand out. For example, the Minnesota House of Representatives uses a subdomain beneath the executive branch-managed mn.gov domain (“house.mn.gov”) while the Senate uses a separate website registered on the .mn TLD (“senate.mn”). Despite coincidentally matching the U.S. Postal Service two letter code for Minnesota, .mn is a country code TLD reserved for (but not exclusively used by) the country of Mongolia. Similarly, the Ohio Legislature uses an executive branch subdomain while the Senate maintains its own exclusive .gov domain (“ohiosenate.gov”). These variations underscore the broader point: without centralized guidance or policy, state domain usage patterns show inconsistency and a lack of standardization that reflect institutional fragmentation rather than coherent digital strategy.

Local

The local category includes four primary subtypes: counties, municipalities (e.g., cities, towns, and villages), special districts (such as water or utility authorities), and independent school districts. Local governments account for the vast majority (98.7%) of eligible SLTT-I entities. In practice, they also represent a dominant share of .gov usage: 85.6% of all registered SLTT-I domains are attributed to local governments.

Despite this strong representation in absolute terms, adoption remains limited relative to the number of eligible jurisdictions. The national average indicates that only 10.6% of local entities have a registered .gov domain. This percentage, shown in Table 6, underscores considerable room for growth. However, the exact figure should be interpreted with caution. CISA’s registrant data likely contains duplicate domains for the same locality (e.g., a city police department and a city government registering separately), while also omitting localities that operate under a subdomain structure provided by their parent state, tribe, or territory.

Table 6. Total Local Domains Per Jurisdiction

Category - Subcategory	Domains	Jurisdictions in the U.S.	Domains-Per-Jurisdiction Percentage
Local	9,628	90,837	10.60%
Local - County	2,380	3,033	78.47%
Local - Municipality	6,554	35,705	18.36%
Local - Special District	663	39,555	01.68%
Local - School District	31	12,546	00.25%

Appendix B provides additional detail by state and local subtype. Among the most striking patterns is the relatively high domains-per-jurisdiction ratio among counties and the near absence of .gov domains among school districts. The high rates of adoption by counties may reflect their central role in U.S. election administration, a function that has historically drawn attention to the need to reinforce election integrity from a cybersecurity perspective and to maintain or increase public trust.^{26, 27} As .gov domains are a trust signal, it is plausible that previous federal efforts to improve election integrity led to higher adoption rates of the domain by counties.

In contrast, only 31 of the 12,546 independent school districts in the United States have registered a .gov domain directly through CISA, a domains-per-jurisdiction rate of just 0.25%. This underutilization is especially notable given that U.S. school districts are presently ineligible for the .edu TLD, which is reserved for postsecondary institutions. For K–12 school systems, .gov represents the only TLD that signals verified government status. The virtual absence of adoption may indicate significant barriers that warrant further investigation.

Tribes

Analyzing .gov adoption among tribal nations presented unique challenges due to limited metadata in CISA’s registrant dataset, the diversity of tribal governance structures, and the large number of eligible entities. A full count of domains per tribe is provided in Appendix C. Based on the available data, 194 of the 574 federally recognized tribes have registered at least one .gov domain, yielding an estimated utilization rate of 33.8%. In addition, three of the 63

²⁶ National Association of Counties. “America’s County Governments: A Primer on County-Level Election Administration.” November 4, 2024. <https://www.naco.org/resource/americas-county-governments-primer-county-level-election-administration>.

²⁷ Menon, Theo and William T. Alder. “More Election Offices are Adopting Verified, .gov Websites,” July 19, 2024, <https://bipartisanpolicy.org/blog/more-election-offices-are-adopting-verified-gov-websites/>.

state-recognized tribes (i.e., those recognized by individual U.S. states but not by the federal government) have adopted the .gov domain, for a much lower utilization rate of 5%.

Most tribes, regardless of recognition status, register only a single domain. The median domain count is one per tribe, with an average of 1.3 domains. An outlier is the Chickasaw Nation, which has registered eight unique .gov domains. However, these domains primarily serve as redirects to websites hosted on the unofficial .net TLD. While redirection can serve as a transitional mechanism when migrating from unofficial to official domains, excessive or permanent reliance on redirection (especially to unofficial TLDs) can confuse users, particularly those with lower digital literacy. This practice also violates the principle of simplicity, one of the three core elements that foster trust in digital government services.

Territories

All six U.S. territories utilize the .gov domain to some extent. Adoption rates among territorial branches vary, with 100% of executive branches, 83% of legislative branches, and 66% of judicial branches using the domain.

The District of Columbia maintains the most domains, with 14 unique .gov registrations, while Guam, the Northern Mariana Islands, and Puerto Rico each maintain three domains. Notably, the website for Puerto Rico's Office of the Comptroller redirects visitors to a .pr domain.²⁸ Although .pr is a country-code TLD associated with Puerto Rico, it is not restricted to official use and is thus treated here as an unofficial domain.

Redirecting from a .gov domain to .pr introduces two key risks. First, it undermines consistency, as other Puerto Rican government entities maintain a .gov presence without such redirection. Second, it exposes the agency to greater impersonation risk via cybersquatting attacks and may confuse users who are trained to associate .gov with authenticity and trust.

Interstate and Intertribal

Among the 270 active interstate compact organizations, only 22 (or approximately 8%) use a .gov domain. Only two intertribal organizations, the Northern Circle Indian Housing Authority and Columbia River Inter-Tribal Fish Commission, were found to do so. The domains for these two intertribal entities were listed as tribal in CISA's registrant list, alongside domains registered

28 URL: <https://www.ocpr.gov.pr/>.

by individual tribes. Although CISA does not separately classify intertribal organizations, this study categorizes these two entities as more akin to interstates due to their roles serving multiple sovereign tribes.

Importantly, CISA’s designation of entities as “interstate” in the data appears to contain a substantial number of inaccuracies. Of the 40 domains listed as interstate in CISA’s dataset, only 22 were verified as true interstate entities. The remaining 18 were clearly misclassified, as they represent *intrastate* organizations, such as the Illinois State Treasurer’s Office and an entity promoting Florida’s advantages to the space industry.²⁹

SECTION 2: POTENTIAL BARRIERS TO .GOV ADOPTION

Outreach Challenges

As detailed in prior sections, the federal government has made the .gov domain available to a large and highly fragmented group of 91,801 jurisdictions. This figure may represent a lower bound, given the existence of multiple branches within jurisdictions and varying governance structures across SLTT-I entities. One likely barrier is lack of awareness: many of the 98.95% of SLTT-I entities at the local level may not know they are eligible for a .gov domain or understand its value.

Given the sheer number and diversity of eligible organizations, effective outreach by CISA or any other national actor is a formidable challenge. However, a coordinated campaign that draws on the findings of this paper and tailors messages to jurisdiction-specific contexts could expand adoption.

SLTT-I Resource Limitations

A 2023 systematic review published in *Sustainability* synthesized findings from 60 academic articles on digital technology adoption in local governments.³⁰ The review identified ten common technology challenges, seven of which have clear external validity as potential barriers to .gov adoption. These challenges and their relevance to domain adoption are summarized in Table 7.

29 URLs: <http://illinoistreasurer.gov>, <http://spaceflorida.gov>.

30 David, Anne, Tan Yigitcanlar and R.Y. M., et al. “Understanding Local Government Digital Technology Adoption Strategies: A PRISMA Review.” *Sustainability* 15, 9645 (2023): 11-14, <https://doi.org/10.3390/su15129645>.

An additional barrier may arise from sunk costs tied to an entity’s existing domain infrastructure. SLTT-I organizations that have heavily invested in unofficial domain branding through printed materials, public outreach campaigns, or longstanding web-based services may face higher transition costs. Updating content, rebranding assets, and re-establishing search visibility can be time-intensive and financially burdensome. Paradoxically, better-resourced entities may face higher transition penalties due to the scale of their existing investments.

Table 7. Challenges to SLTT-I .gov Adoption

Challenge	Number of Studies Cited	Applicability to .gov Adoption
Lack of ethical framework and regulation	11	The absence of guiding technology frameworks and regulations may decrease the ability of SLTT-I entities to leverage resources like .gov.
Lack of technical infrastructure readiness	11	SLTT-I entities that do not have a website or email address face a more significant barrier in .gov adoption than those that are transferring an existing web presence.
Lack of decision-makers’ support	9	Some SLTT-I jurisdictions may lack clarity on whose decision it would be to direct or initiate a transition to .gov. Those with clarity may not prioritize the transition over other efforts.
Lack of technical staff and knowledge	8	SLTT-I entities without significant staff knowledge or continuity in the management of existing web and email infrastructure may find .gov adoption challenging.
Lack of planning	8	Transition of an existing web presence to .gov requires detailed planning, especially to communicate the change to constituents.
Lack of internal and external collaboration	5	Adoption of the .gov domain requires external coordination with CISA, and may require additional coordination with a higher-level jurisdiction like a state, tribe, or territory.
Compatibility	3	Adoption of .gov may break existing custom software applications or workflows if the SLTT-I entity is unable or unwilling to modify them.

This table is adapted from a study that synthesized findings from 60 academic articles on digital technology adoption in local governments. The “number of studies cited” column shows the number of academic articles analyzed in the study that listed the particular challenge. For more information, see the original study: “Understanding Local Government Digital Technology Adoption Strategies: A PRISMA Review,” by David, Anne, Tan Yigitcanlar, and R.Y. M., et al. in *Sustainability* 15, 9645 (2023): 11–14, <https://doi.org/10.3390/su15129645>.

SLTT-I Motivation

Even when an SLTT-I entity is aware of its eligibility, has sufficient resources, and faces none of the structural barriers described in Table 7, it may still decline to adopt a .gov domain. One reason may be a desire to maintain autonomy, either from a parent SLTT-I jurisdiction (in the case of subdomains) or from the federal government more broadly.

As discussed in the literature review, CISA has ultimate authority over all .gov domains, including the ability to suspend or revoke domain access. Technically, CISA could make a domain inaccessible within minutes, with full propagation delays extending up to 48 hours. During this window, the affected SLTT-I entity would be unable to send or receive email or maintain access to its public-facing websites. If this occurred during a critical event like an election, the effects could be catastrophic and potentially irreparable.

While the affected entity could register an unofficial domain in response, the transition would be sudden, disorganized, and likely confusing for users. There would be no automatic redirection available from the old .gov domain without CISA's cooperation. During the disruption, the entity would be vulnerable to impersonation, misinformation, and reduced public trust.

Importantly, the risk of revocation is not limited to abuse of power or political disputes. CISA retains revocation authority for legitimate security purposes, including in response to suspected compromise by advanced persistent threats. As of June 1, 2025, the agency's published guidance notes that malicious cyber activity may result in domain suspension or termination; it states that CISA will "make reasonable efforts to contact a registrant, including emails or phone calls," and will "make reasonable accommodations for remediation timelines based on the severity of the issue."³¹ However, this language appears to reflect CISA's internal policy and is not codified in federal law. Unless a formal agreement is in place, an SLTT-I entity may have limited legal recourse to challenge or reverse a revocation decision, especially if CISA invokes provisions of the DOTGOV Act as the basis for its decision.

31 Cybersecurity and Infrastructure Security Agency. "Requirements for operating a .gov domain." CISA. Accessed on June 1, 2025. <https://get.gov/domains/requirements/>.

Recommendations

OVERVIEW

This section details four recommendations to improve adoption of the .gov domain while simultaneously improving trust online by making .gov use at the sub-federal level simpler and more consistent. The first recommendation is to federate and standardize the local use of .gov. The second recommendation is to narrow allowable domain criteria and cap the number of registrations per jurisdiction. The third recommendation is to promote enrollment among eligible jurisdictions and increase domain digital literacy among the public. And the fourth recommendation is to consider alternative frameworks for .gov governance to mitigate potential problems that could arise from CISA's unilateral control. Each recommendation has applicability for CISA, the U.S. Congress, SLTT-I entities, non-governmental organizations (NGOs), civil society organizations (CSOs), academics, and policy analysts.

1. FEDERATE AND STANDARDIZE LOCAL USE OF .GOV

Congress should update the DOTGOV Act to explicitly allow CISA to federate responsibility for managing local-level .gov use to the states, tribes, and territories. It should do this by requiring eligible local entities to use subdomains beneath a domain managed by their respective higher-level government, rather than registering directly with CISA. A formal exemption or waiver process could accommodate exceptional circumstances in which a standalone domain is necessary at the local level. To facilitate this transition, CISA could publish a transition timeline, provide implementation support, and issue updated domain structure guidelines.

This recommendation would promote a more standardized and consistent domain structure for the nearly 99% of eligible SLTT-I entities that operate at the local level. It would provide the public with a reliable and predictable format for locating official local government websites (such as “mytown.YY.gov,” where “YY” represents the two-letter code for a state or territory). This approach would also help reduce CISA's burden in managing the .gov domain's attack surface, particularly when it comes to authenticating and validating local registrants. States, tribes, and territories are better positioned to verify the legitimacy of their local jurisdictions and can, in theory, perform this validation more effectively than CISA.

While the current text of the DOTGOV Act likely does not allow CISA to mandate subdomain usage (due to its prohibitions on conditioning domain registration based on information sharing or participation in other services), the agency should implement strategic “nudges” to encourage the more localized structure (at least until Congress provides authority). For instance, CISA could offer meaningful services such as preloading, enhanced protections, DNS hosting, or monitoring support exclusively to states, tribes, and territories that require their local governments to adopt standardized subdomains. Congress could reinforce this practice by linking grants to SLTT-I policies that reduce the proliferation of independent .gov domains through formalized subdomain structures.

This recommendation aligns with current White House priorities. President Trump stated in Executive Order 14239, “federal policy must rightly recognize that preparedness is most effectively owned and managed at the State, local, and even individual levels, supported by a competent, accessible, and efficient Federal Government.” The order connects this policy to the prevention of and response to cyber attacks (among other risks).³²

This recommendation also aligns with the second Trump administration’s budget priorities. In a May 2025 budget letter to Senator Collins, the Director of the Office of Management and Budget (OMB) noted that the OMB evaluated federal programs to determine whether their functions could be better performed by state or local governments, or whether they were necessary at all.³³ That same letter recommended a \$491 million reduction in CISA’s budget, reaffirming a federal emphasis on focusing CISA’s role around federal network defense and critical infrastructure protection.

Proactive participation by states, tribes, and territories would further strengthen this model. Higher-level jurisdictions could pre-establish standardized subdomains (e.g., cityname.mo.gov) for local governments and lead the outreach and onboarding process. They can also proactively enact laws requiring standardized .gov subdomain use within their jurisdictions.

Utah passed legislation mandating that all government entities use the .gov TLD, but its implementation allows local jurisdictions to either register directly with CISA or adopt a state-provided subdomain.³⁴ While well-intentioned, this dual-path model falls short of the goals of consistency and standardization. Instead, states should require localities to use subdomains

32 Achieving Efficiency Through State and Local Preparedness. Executive Order 14239. President Donald J. Trump. March 18, 2025. <https://www.federalregister.gov/documents/2025/03/21/2025-04973/achieving-efficiency-through-state-and-local-preparedness>.

33 Letter To the Honorable Susan Collins. Chair of the Senate Appropriations Committee. May 2, 2025. <https://www.whitehouse.gov/wp-content/uploads/2025/05/Fiscal-Year-2026-Discretionary-Budget-Request.pdf>.

34 Utah. “Use of an Authorized Top-Level Domain.” Accessed on May 31, 2025. <https://cybercenter.utah.gov/Requests/>.

unless a waiver is approved through a state technology office, chief information officer, security operations center, or equivalent authority.

2. NARROW ALLOWABLE DOMAIN CRITERIA

CISA should also revise its criteria for domain registration by SLTT-I entities to limit unnecessary domain proliferation. Current CISA policy allows for wide discretion, which leads to patterns of unstandardized and inconsistent use that ultimately undermine trust in the TLD itself. This recommendation is likely consistent with the DOTGOV Act, which states that CISA should “minimize the risk of .gov internet domains whose names could mislead or confuse users.”³⁵

CISA should set a default cap of 12 domains for all SLTT-I entities, with exceptions available through a clearly defined waiver process. SLTT-I entities should host all other functions via subdomains or page structures under a central domain. This cap would allow for up to four domains per branch in three-branch governments. With the exception of the District of Columbia, all tribes and territories already fall within this range, although many states significantly exceed it.

If CISA does not adopt this recommendation, states, tribes, and territories could develop their own standards to limit domain proliferation, whether through internal policy or legislation.

3. PROMOTE .GOV ENROLLMENT AND IMPROVE DOMAIN DIGITAL LITERACY

Once structural reforms are in place, outreach efforts should focus on expanding .gov enrollment and improving digital literacy among constituents. Higher rates of .gov adoption by counties (discussed in Section 1) suggest that county adoption rates increased due to past federal attention on election security issues, which may indicate that targeted outreach can be effective.

³⁵ U.S. House of Representatives. “6 USC 665: Duties and authorities relating to .gov internet domain.” U.S. Code. [https://uscode.house.gov/view.xhtml?req=\(title:6%20section:665%20edition:prelim\)%20OR%20\(granuleid:USC-prelim-title6-section665\)&f=treesort&edition=prelim&num=0&jumpTo=true](https://uscode.house.gov/view.xhtml?req=(title:6%20section:665%20edition:prelim)%20OR%20(granuleid:USC-prelim-title6-section665)&f=treesort&edition=prelim&num=0&jumpTo=true).

By delegating local outreach and onboarding responsibilities to states, tribes, and territories, CISA can reallocate its limited resources toward supporting higher-level jurisdictions. In turn, those higher-level jurisdictions should prioritize outreach based on two criteria:

- Risk of impersonation (e.g., election authorities, public safety); and
- Historically low adoption rates (e.g., school districts).

As documented in the literature review, low digital literacy makes users more vulnerable to cybersquatting and deception that can result in stolen user data, broken trust, and, in the worst cases, damage to national security. Outreach campaigns that teach the public to recognize .gov domains as verified and trustworthy can mitigate these risks. An effective example of one such outreach campaign (although it does not specifically address .gov) is the Take9 campaign, which encourages users to slow down and take nine seconds to critically evaluate content online.³⁶ States, tribes, and territories should work with NGOs and CSOs to lead these efforts as part of a coordinated digital trust-building strategy.

4. CONSIDER ALTERNATIVE FRAMEWORKS FOR .GOV GOVERNANCE

As discussed earlier, CISA retains unilateral authority over the DNS zone file that validates all .gov domains. This centralized control enables CISA to quickly respond to cyber threats but also means that any SLTT-I entity and its constituents are vulnerable to sudden and complete loss of digital access with little recourse.

To address this, Congress and CISA should explore a federated governance model for the .gov TLD. While a degree of centralization is always required due to the technical requirements of DNS, there are various technical and policy approaches that could be enacted to mitigate potentially problematic aspects of CISA’s unilateral authority over the TLD if the benefits outweigh the costs.

Under one such model, a governing council that includes federal and SLTT-I representatives could maintain control of the .gov zone file. Under another approach, Congress could establish a legal framework to adjudicate revocation, and provide streamlined judicial review for decisions that negatively impact a SLTT-I entity. Key questions for further study include whether such models could preserve the agility and speed necessary to respond to malicious

36 “Take 9 seconds before you click, download, or share.” Take9. <https://pausetake9.org/>.

activity without compromising the overall security of the TLD, and whether such approaches could meaningfully improve the willingness of SLTT-I entities to use the TLD.

While CISA could begin exploring this option through policy, the most effective implementation would likely be achieved through congressional legislation following a thorough feasibility study and risk assessment.

Appendix A: State Analysis

As discussed in Section 1, a utilization efficiency metric was calculated for each state by standardizing the number of registered domains using z-scores. This paper defines utilization efficiency as the number of registered domains required to achieve comparable functions. Each state's z-score was calculated using the formula $Z = \frac{\chi - \mu}{\sigma}$, where χ is the state's total domain count. The mean number of domains (μ) was 25.9, and the standard deviation (σ) was 26.50225. This standardized measure indicates how far each state's domain count deviates from the national average. States were then grouped into one of five utilization efficiency categories based on their score: Very High ($z < -0.5$), High ($-0.5 \leq z < 0$), Moderate ($0 \leq z < 1$), Low ($1 \leq z < 2.5$), and Very Low ($z \geq 2.5$). These category thresholds were selected due to the data exhibiting a long tail of low to moderate values with two strong outlier states.

Table A1. Full State Domain Efficiency Analysis

State	Domains	Z-Score	Result
Mississippi	2	-0.90181	Very High
California	3	-0.86408	Very High
Hawaii	4	-0.82634	Very High
Missouri	4	-0.82634	Very High
Utah	4	-0.82634	Very High
Delaware	5	-0.78861	Very High
New Hampshire	6	-0.75088	Very High
Georgia	8	-0.67541	Very High
Minnesota	8	-0.67541	Very High
Kentucky	9	-0.63768	Very High
Washington	9	-0.63768	Very High
Alaska	10	-0.59995	Very High
New Mexico	10	-0.59995	Very High
South Dakota	10	-0.59995	Very High
Connecticut	11	-0.56222	Very High
Rhode Island	11	-0.56222	Very High
Arkansas	12	-0.52448	Very High
Indiana	12	-0.52448	Very High
Vermont	12	-0.52448	Very High
Idaho	13	-0.48675	High

BUILDING TRUST

State	Domains	Z-Score	Result
Illinois	14	-0.44902	High
Virginia	16	-0.37355	High
Maryland	18	-0.29809	High
Maine	18	-0.29809	High
Nebraska	18	-0.29809	High
New York	18	-0.29809	High
Pennsylvania	18	-0.29809	High
Oklahoma	19	-0.26036	High
Wyoming	19	-0.26036	High
Michigan	19	-0.26036	High
North Dakota	21	-0.18489	High
Nevada	21	-0.18489	High
Oregon	21	-0.18489	High
Massachusetts	22	-0.14716	High
South Carolina	23	-0.10942	High
Louisiana	24	-0.07169	High
Montana	27	0.041506	Moderate
Wisconsin	31	0.192436	Moderate
West Virginia	37	0.418832	Moderate
Colorado	37	0.418832	Moderate
Texas	38	0.456565	Moderate
Alabama	41	0.569763	Moderate
Tennessee	53	1.022554	Low
New Jersey	57	1.173485	Low
Ohio	58	1.211217	Low
Kansas	64	1.437613	Low
Iowa	67	1.550811	Low
North Carolina	68	1.588544	Low
Florida	102	2.871453	Very Low
Arizona	143	4.41849	Very Low

Appendix B: Local Data

To determine .gov domain utilization at the local level, data from CISA’s domain registrant list and the U.S. Census Bureau’s 2022 Census of Governments were combined, as shown in Table B1.^{37, 38} This table omits territory and tribal locality counts due to jurisdiction-specific nuances regarding local governance. The resulting table is sorted alphabetically by state.

Table B1. Local .gov Domain Use in U.S. States

State	Jurisdiction Type	Jurisdiction Count	Domain Count	Domains-Per-Jurisdiction Percentage
Alabama	County	67	46	68.66%
Alabama	Municipality	462	115	24.89%
Alabama	Special District	541	6	1.11%
Alabama	School District	138	0	0.00%
Alabama	Total	1,208	167	13.82%
Alaska	County	15	5	33.33%
Alaska	Municipality	149	21	14.09%
Alaska	Special District	17	0	0.00%
Alaska	School District	0	0	0.00%
Alaska	Total	181	26	14.36%
Arizona	County	15	22	146.67%
Arizona	Municipality	91	87	95.60%
Arizona	Special District	326	9	2.76%
Arizona	School District	242	1	0.41%
Arizona	Total	674	119	17.66%
Arkansas	County	75	68	90.67%
Arkansas	Municipality	500	68	13.60%
Arkansas	Special District	753	11	1.46%
Arkansas	School District	234	0	0.00%
Arkansas	Total	1,562	147	9.41%
California	County	57	85	149.12%
California	Municipality	482	359	74.48%

³⁷ Cybersecurity and Infrastructure Security Agency. “Official list of .gov domains” GitHub. Accessed on April 10, 2025. <https://github.com/cisagov/dotgov-data>.

³⁸ Census Bureau. “2022 Census of Governments - Organization.” Last revised April 23, 2025, <https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html>.

BUILDING TRUST

State	Jurisdiction Type	Jurisdiction Count	Domain Count	Domains-Per-Jurisdiction Percentage
California	Special District	2,949	111	3.76%
California	School District	1,006	6	0.60%
California	Total	4,494	561	12.48%
Colorado	County	62	62	100.00%
Colorado	Municipality	272	88	32.35%
Colorado	Special District	3,201	44	1.37%
Colorado	School District	180	1	0.56%
Colorado	Total	3,715	195	5.25%
Connecticut	Municipality	179	129	72.07%
Connecticut	School District	17	1	5.88%
Connecticut	Special District	433	5	1.15%
Connecticut	County	0	1	0.00%
Connecticut	Total	629	136	21.62%
Delaware	County	3	3	100.00%
Delaware	Municipality	57	12	21.05%
Delaware	Special District	255	0	0.00%
Delaware	School District	19	0	0.00%
Delaware	Total	334	15	4.49%
Florida	County	66	141	213.64%
Florida	Municipality	412	184	44.66%
Florida	Special District	1,374	28	2.04%
Florida	School District	95	1	1.05%
Florida	Total	1,947	354	18.18%
Georgia	County	152	111	73.03%
Georgia	Municipality	537	174	32.40%
Georgia	Special District	510	3	0.59%
Georgia	School District	180	0	0.00%
Georgia	Total	1,379	288	20.88%
Hawaii	County	5	9	180.00%
Hawaii	Municipality	1	2	200.00%
Hawaii	Special District	17	1	5.88%
Hawaii	School District	0	0	0.00%
Hawaii	Total	21	12	57.14%
Idaho	County	44	29	65.91%
Idaho	Municipality	199	35	17.59%

B U I L D I N G T R U S T

State	Jurisdiction Type	Jurisdiction Count	Domain Count	Domains-Per-Jurisdiction Percentage
Idaho	Special District	807	5	0.62%
Idaho	School District	118	0	0.00%
Idaho	Total	1,168	69	5.91%
Illinois	County	102	118	115.69%
Illinois	Municipality	2,720	206	7.57%
Illinois	Special District	3,218	24	0.75%
Illinois	School District	890	0	0.00%
Illinois	Total	6,930	348	5.02%
Indiana	County	91	29	31.87%
Indiana	Municipality	1,571	77	4.90%
Indiana	School District	290	3	1.03%
Indiana	Special District	696	4	0.57%
Indiana	Total	2,648	113	4.27%
Iowa	County	99	64	64.65%
Iowa	Municipality	940	69	7.34%
Iowa	Special District	445	2	0.45%
Iowa	School District	342	0	0.00%
Iowa	Total	1,826	135	7.39%
Kansas	County	103	46	44.66%
Kansas	Municipality	1,891	75	3.97%
Kansas	School District	306	1	0.33%
Kansas	Special District	1,468	2	0.14%
Kansas	Total	3,768	124	3.29%
Kentucky	County	118	68	57.63%
Kentucky	Municipality	417	81	19.42%
Kentucky	Special District	601	5	0.83%
Kentucky	School District	171	0	0.00%
Kentucky	Total	1,307	154	11.78%
Louisiana	County	60	25	41.67%
Louisiana	Municipality	304	47	15.46%
Louisiana	Special District	101	4	3.96%
Louisiana	School District	69	0	0.00%
Louisiana	Total	534	76	14.23%
Maine	County	16	16	100.00%
Maine	Municipality	484	80	16.53%

BUILDING TRUST

State	Jurisdiction Type	Jurisdiction Count	Domain Count	Domains-Per-Jurisdiction Percentage
Maine	Special District	227	0	0.00%
Maine	School District	101	0	0.00%
Maine	Total	828	96	11.59%
Maryland	County	23	24	104.35%
Maryland	Municipality	157	74	47.13%
Maryland	Special District	162	0	0.00%
Maryland	School District	0	0	0.00%
Maryland	Total	342	98	28.65%
Massachusetts	County	5	5	100.00%
Massachusetts	Municipality	351	268	76.35%
Massachusetts	Special District	415	10	2.41%
Massachusetts	School District	85	0	0.00%
Massachusetts	Total	856	283	33.06%
Michigan	County	83	58	69.88%
Michigan	Municipality	1,773	380	21.43%
Michigan	Special District	437	6	1.37%
Michigan	School District	567	0	0.00%
Michigan	Total	2,860	444	15.52%
Minnesota	County	87	67	77.01%
Minnesota	Municipality	2,633	241	9.15%
Minnesota	Special District	579	20	3.45%
Minnesota	School District	330	0	0.00%
Minnesota	Total	3,629	328	9.04%
Mississippi	County	82	44	53.66%
Mississippi	Municipality	298	55	18.46%
Mississippi	Special District	437	0	0.00%
Mississippi	School District	150	0	0.00%
Mississippi	Total	967	99	10.24%
Missouri	County	114	102	89.47%
Missouri	Municipality	1,226	147	11.99%
Missouri	Special District	1,927	18	0.93%
Missouri	School District	529	1	0.19%
Missouri	Total	3,796	268	7.06%
Montana	County	54	50	92.59%
Montana	Municipality	128	24	18.75%

B U I L D I N G T R U S T

State	Jurisdiction Type	Jurisdiction Count	Domain Count	Domains-Per-Jurisdiction Percentage
Montana	Special District	736	4	0.54%
Montana	School District	310	1	0.32%
Montana	Total	1,228	79	6.43%
Nebraska	County	93	80	86.02%
Nebraska	Municipality	878	43	4.90%
Nebraska	Special District	1,303	0	0.00%
Nebraska	School District	267	0	0.00%
Nebraska	Total	2,541	123	4.84%
Nevada	County	16	16	100.00%
Nevada	Municipality	19	11	57.89%
Nevada	Special District	135	0	0.00%
Nevada	School District	17	0	0.00%
Nevada	Total	187	27	14.44%
New Hampshire	County	10	10	100.00%
New Hampshire	Municipality	234	143	61.11%
New Hampshire	Special District	128	9	7.03%
New Hampshire	School District	166	2	1.20%
New Hampshire	Total	538	164	30.48%
New Jersey	County	21	21	100.00%
New Jersey	Municipality	564	157	27.84%
New Jersey	Special District	222	9	4.05%
New Jersey	School District	521	2	0.38%
New Jersey	Total	1,328	189	14.23%
New Mexico	County	33	16	48.48%
New Mexico	Municipality	105	46	43.81%
New Mexico	Special District	769	2	0.26%
New Mexico	School District	96	0	0.00%
New Mexico	Total	1,003	64	6.38%
New York	County	57	77	135.09%
New York	Municipality	1,525	441	28.92%
New York	Special District	1,189	22	1.85%
New York	School District	676	0	0.00%
New York	Total	3,447	540	15.67%
North Carolina	County	100	106	106.00%
North Carolina	Municipality	552	158	28.62%

BUILDING TRUST

State	Jurisdiction Type	Jurisdiction Count	Domain Count	Domains-Per-Jurisdiction Percentage
North Carolina	Special District	313	9	2.88%
North Carolina	School District	0	1	0.00%
North Carolina	Total	965	274	28.39%
North Dakota	County	53	19	35.85%
North Dakota	Municipality	1,661	19	1.14%
North Dakota	Special District	683	0	0.00%
North Dakota	School District	173	0	0.00%
North Dakota	Total	2,570	38	1.48%
Ohio	County	88	104	118.18%
Ohio	Municipality	2,234	246	11.01%
Ohio	Special District	952	21	2.21%
Ohio	School District	665	1	0.15%
Ohio	Total	3,939	372	9.44%
Oklahoma	County	77	35	45.45%
Oklahoma	Municipality	592	103	17.40%
Oklahoma	Special District	632	6	0.95%
Oklahoma	School District	539	0	0.00%
Oklahoma	Total	1,840	144	7.83%
Oregon	County	36	37	102.78%
Oregon	Municipality	240	107	44.58%
Oregon	Special District	1,029	58	5.64%
Oregon	School District	223	2	0.90%
Oregon	Total	1,528	204	13.35%
Pennsylvania	County	66	69	104.55%
Pennsylvania	Municipality	2,559	195	7.62%
Pennsylvania	Special District	1,712	8	0.47%
Pennsylvania	School District	514	2	0.39%
Pennsylvania	Total	4,851	274	5.65%
Rhode Island	Municipality	39	42	107.69%
Rhode Island	Special District	84	3	3.57%
Rhode Island	County	0	0	0.00%
Rhode Island	School District	4	0	0.00%
Rhode Island	Total	127	45	35.43%
South Carolina	County	46	29	63.04%
South Carolina	Municipality	271	62	22.88%

B U I L D I N G T R U S T

State	Jurisdiction Type	Jurisdiction Count	Domain Count	Domains-Per-Jurisdiction Percentage
South Carolina	Special District	271	4	1.48%
South Carolina	School District	78	0	0.00%
South Carolina	Total	666	95	14.26%
South Dakota	County	66	12	18.18%
South Dakota	Municipality	1,207	15	1.24%
South Dakota	Special District	478	0	0.00%
South Dakota	School District	149	0	0.00%
South Dakota	Total	1,900	27	1.42%
Tennessee	County	92	92	100.00%
Tennessee	Municipality	345	134	38.84%
Tennessee	School District	14	1	7.14%
Tennessee	Special District	451	15	3.33%
Tennessee	Total	902	242	26.83%
Texas	County	254	89	35.04%
Texas	Municipality	1,225	419	34.20%
Texas	Special District	2,984	32	1.07%
Texas	School District	1,070	1	0.09%
Texas	Total	5,533	541	9.78%
Utah	County	29	31	106.90%
Utah	Municipality	254	156	61.42%
Utah	Special District	308	91	29.55%
Utah	School District	41	2	4.88%
Utah	Total	632	280	44.30%
Vermont	County	14	5	35.71%
Vermont	Municipality	277	69	24.91%
Vermont	Special District	162	1	0.62%
Vermont	School District	121	0	0.00%
Vermont	Total	574	75	13.07%
Virginia	County	95	80	84.21%
Virginia	Municipality	228	104	45.61%
Virginia	Special District	198	9	4.55%
Virginia	School District	1	0	0.00%
Virginia	Total	522	193	36.97%
Washington	County	39	39	100.00%
Washington	Municipality	281	122	43.42%

B U I L D I N G T R U S T

State	Jurisdiction Type	Jurisdiction Count	Domain Count	Domains-Per-Jurisdiction Percentage
Washington	Special District	1,275	17	1.33%
Washington	School District	295	1	0.34%
Washington	Total	1,890	179	9.47%
West Virginia	County	55	33	60.00%
West Virginia	Municipality	231	53	22.94%
West Virginia	Special District	298	3	1.01%
West Virginia	School District	55	0	0.00%
West Virginia	Total	639	89	13.93%
Wisconsin	County	72	58	80.56%
Wisconsin	Municipality	1,850	583	31.51%
Wisconsin	Special District	703	15	2.13%
Wisconsin	School District	437	0	0.00%
Wisconsin	Total	3,062	656	21.42%
Wyoming	County	23	24	104.35%
Wyoming	Municipality	99	24	24.24%
Wyoming	Special District	643	2	0.31%
Wyoming	School District	55	0	0.00%
Wyoming	Total	820	50	6.10%

Appendix C: Tribal Data

CISA’s domain list includes all domains attributed to both federally- and state-recognized tribes. To calculate a total domain count per tribe, entries associated with the same tribe — but listed under different domain names — were consolidated. Because the dataset only included the organization name submitted during registration, and not necessarily the tribe’s official or commonly recognized name, manual interpretation was often required. Additionally, CISA’s list did not differentiate between federal and state recognition, so this analysis independently verified each tribe’s status by cross-referencing official lists of federally- and state-recognized tribes. Some inaccuracies may remain due to the scale of the dataset, the diversity of tribal governance structures, and limited familiarity with jurisdiction-specific naming conventions. Minor normalization was applied to the registrant names, such as removing leading articles (e.g., “The”) and omitting references to specific tribal offices (e.g., “Housing Authority”). The resulting tables are sorted alphabetically by tribal nation.

Table C1. Federally-Recognized Tribal Nation Domain Count

Tribe	Domains	State
Absentee-Shawnee Tribe of Indians of Oklahoma	1	OK
Agua Caliente Band of Cahuilla Indians	2	CA
Ak-Chin Indian Community	1	AZ
Akiak Native Community	1	AK
Arctic Village	1	AK
Aroostook Band of Micmacs	1	ME
Augustine Band Of Cahuilla Indians	2	CA
Bad River Band Of Lake Superior Tribe Of Chippewa Indians	1	WI
Baranof Island	1	AK
Barona Band of Mission Indians	1	CA
Bear River Band of the Rohnerville Rancheria	1	CA
Big Valley Rancheria	1	CA
Bishop Paiute Tribe	2	CA
Blue Lake Rancheria	1	CA
Bois Forte Reservation	1	MN
Burns Paiute Tribe	1	OR
Cabazon Band of Mission Indians	1	CA
Cahto Tribe	1	CA

BUILDING TRUST

Tribe	Domains	State
Cahuilla Band of Indians	1	CA
California Valley Miwok Tribe	1	CA
Campo Kumeyaay Nation	1	CA
Catawba Indian Nation	1	SC
Cayuga Nation	2	NY
Central Council Tlingit & Haida Indian Tribes of Alaska	2	AK
Chemehuevi Indian Tribe	1	CA
Cherokee Nation	2	OK
Cheyenne and Arapaho Tribes	1	OK
Chickaloon Native Village	1	AK
Chickasaw Nation (Shawnee)	8	OK
Chico Rancheria	1	CA
Chilkat Indian Village Tribal Government	1	AK
Chilkoot Indian Association	1	AK
Chitimacha Tribe of Louisiana	1	LA
Cocopah Indian Tribe	1	AZ
Coeur d' Alene Tribe	1	ID
Cold Springs Rancheria	1	CA
Colorado River Indian Tribes	1	AZ
Colusa Indians	1	CA
Comanche Nation	1	OK
Confederated Salish and Kootenai Tribes	1	MT
Confederated Tribes and Bands of the Yakama Nation	1	WA
Confederated Tribes of the Chehalis Reservation	1	WA
Confederated Tribes of Warm Springs	1	OR
Cow Creek Band of Umpqua Tribe of Indians	1	OR
Coyote Valley Tribe	1	CA
Crow Nation	1	MT
Delaware Nation	1	OK
Eastern Band of Cherokee	3	NC
Eastern Shawnee Tribe of Oklahoma	1	OK
Elk Valley Rancheria, California	1	CA
Ewiiapaayp Band of Kumeyaay Indians	1	CA
Flandreau Santee Sioux Tribe of South Dakota	1	SD
Forest County Potawatomi Community	2	WI
Fort Sill Apache Tribe	1	OK

BUILDING TRUST

Tribe	Domains	State
Gila River Indian Community	1	AZ
Grand Portage Band of Lake Superior Chippewa	1	MN
Grand Traverse Band of Ottawa and Chippewa Indians	1	MI
Gun Lake Tribe (Match-e-be-nash-she-wish Band of Pottawatomi Indians of Michigan)	2	MI
Habematolel Pomo of Upperlake	1	CA
Hannahville Indian Community	1	MI
Havasupai Tribe	1	AZ
Hoopa Valley Tribal Council	1	CA
Hopi Tribe	1	AZ
Hualapai Tribal Nation	1	AZ
Igiugig Village Council	1	AK
Inupiat Community of the Arctic Slope	1	AK
Iowa Tribe of Oklahoma	1	OK
Jackson Rancheria Band of Miwuks	1	CA
Jamul Indian Village	1	CA
Kaibab Band of Paiute Indians	1	AZ
Kalispel Tribe of Indians	1	WA
Kaw Nation	1	OK
Kayenta Township	1	AZ
Keweenaw Bay Indian Community	2	MI
Kickapoo Tribe in Kansas	1	KS
Klamath Tribe	1	OR
La Jolla Band of Luiseno Indians	1	CA
Lac Courte Oreilles Tribal Government	1	WI
Lac Vieux Desert Band of Lake Superior Chippewa Indians	1	MI
Lipay Nation of Santa Ysabel	2	CA
Little River Band of Ottawa Indians Tribal Government	1	MI
Little Traverse Bay Bands of Odawa Indians	1	MI
Lummi Indian	3	WA
Manzanita Band of Diegueno Mission Indians	1	CA
Mashantucket Pequot Tribal Nation	3	CT
Mashpee Wampanoag Tribe	2	MA
Mattaponi	1	VA
Mechoopda Indian Tribe of Chico Rancheria	1	CA
Menominee Indian Tribe of Wisconsin	1	WI

BUILDING TRUST

Tribe	Domains	State
Mesa Grande Band of Mission Indians	1	CA
Miccosukee Tribe of Indians of Florida	1	FL
Middletown Rancheria	1	CA
Mille Lacs Band of Ojibwe	2	MN
Mississippi Band of Choctaw Indians	1	MS
Monacan Indian Nation	1	VA
Mooretown Rancheria of Maidu Indians	1	CA
Morongo Band of Mission Indians	2	CA
Muckleshoot Indian Tribe	1	WA
Muscogee (Creek) Nation	2	OK
Nansemond Indian Tribe	1	VA
Native Village of Barrow	1	AK
Native Village of Eklutna	1	AK
Native Village of Eyak	1	AK
Navajo Nation	2	AZ
Ninilchik Tribe	1	AK
Nisqually Tribal Council	1	WA
Nooksack Indian Tribe	1	WA
North Fork Rancheria	3	CA
Nottawaseppi Huron Band of the Potawatomi	2	MI
Oglala Sioux Tribe	1	SD
Oneida Tribe of Indians of Wisconsin	1	WI
Organized Village of Kake	1	AK
Osage Nation (Shawnee)	3	OK
Ottawa Tribe of Oklahoma	1	OK
Paiute Indian Tribe of Utah	1	UT
Pascua Yaqui Tribe	1	AZ
Paskenta Band Of Nomlaki Indians	1	CA
Passamaquoddy	1	ME
Pauma Band of Mission Indians	1	CA
Pechanga Tribal Government	1	CA
Penobscot Nation	1	ME
Picayune Rancheria of the Chukchansi Indians	2	CA
Pinoleville Pomo Nation	1	CA
Pit River Tribe	1	CA
Poarch Band of Creek Indians	2	AL

BUILDING TRUST

Tribe	Domains	State
Pokagon Band of Potawatomi Indians	1	MI
Ponca Tribe of Nebraska	1	NE
Ponca Tribe of Oklahoma	1	OK
Prairie Island	1	MN
Pueblo of Isleta	1	NM
Pueblo of Laguna	4	NM
Pueblo of Santa Ana	3	NM
Puyallup Tribe of Indians	1	WA
Quapaw Nation	1	OK
Quartz Valley Indian Reservation	1	CA
Ramona Band of Cahuilla	1	CA
Red Cliff Band of Lake Superior Chippewa	1	WI
Redding Rancheria	1	CA
Resighini Rancheria	1	CA
Rincon Band of Luiseno Indians	1	CA
Robinson Rancheria	1	CA
Roebud Sioux Tribe	2	SD
Sac & Fox Nation	1	OK
Sac & Fox Tribe of the Mississippi in Iowa	1	IA
Saginaw Chippewa Indian Tribe of Michigan	1	MI
Saint Regis Mohawk	2	NY
Salt River Pima-Maricopa Indian Community	1	AZ
Samish Indian Nation	1	WA
San Carlos Apache Tribe	2	AZ
San Juan Southern Paiute Trive	1	AZ
San Manuel Band of Mission Indians	1	CA
Santa Rosa Band of Cahuilla Indians	2	CA
Santa Rosa Indian Community of the Santa Rosa Rancheria	2	CA
Santa Ynez Band of Chumash Indians	1	CA
Scotts Valley Band of Pomo Indians	2	CA
Seminole Nation of Oklahoma	1	OK
Shawnee Tribe	1	OK
Shinnecock Nation	1	NY
Shoalwater Bay indian Tribe	1	WA
Shoshone-Bannock Tribe	1	ID
Sisseton Wahpeton Oyate	1	SD

BUILDING TRUST

Tribe	Domains	State
Sitka Tribe of Alaska	1	AK
Skokomish Health Center	1	WA
Soboba Band of Luiseno Indians	1	CA
Sokaogon Chippewa Community	1	WI
Southern Ute Indian Tribe	1	CO
St. Croix Chippewa Indian of Wisconsin	1	WI
Stockbridge-Munsee Band of Mohican Indians	1	WI
Susanville Indian Rancheria	1	CA
Swinomish Indian Tribal Community	1	WA
Sycuan Band of the Kumeyaay Nation	2	CA
Taos Pueblo	1	NM
Tejon Indian Tribe	1	CA
Texas Band of Yaqui Indians	1	TX
Tohono O'odham Nation	3	AZ
Tolowa Dee-ni Nation	2	OR
Torres-Martinez Desert Cahuilla Indians	2	CA
Tulalip Tribes	6	WA
Tule River	1	CA
Twenty-Nine Palms Band of Mission Indians	3	CA
United Keetoowah Band of Cherokee Indians in Oklahoma	1	OK
Upper Sioux Community	2	MN
Upper Skagit Indian Tribe	1	WA
Viejas	2	CA
Village of Dot Lake	1	AK
Wakpamni Lake Community	1	SD
Wampanoag Tribe of Gay Head (Aquinnah)	1	MA
White Earth Reservation Tribal Council	1	MN
Wilton Rancheria	1	CA
Wyandotte Nation	1	OK
Yakama Nation Fisheries Resource Management	1	WA
Yerington Paiute Tribe	1	NV
Yocha Dehe Wintun Nation	2	CA
Ysleta Del Sur Pueblo	1	TX

Table C2. State-Recognized Tribal Nation Domain Count

Tribe	Domains	State
Hassanamisco Nipmuc Band	1	MA
Piqua Shawnee Tribe	1	AL
Upper Mattaponi Tribe	1	VA

References

- Achieving Efficiency Through State and Local Preparedness. Executive Order 14239.
President Donald J. Trump. March 18, 2025. <https://www.whitehouse.gov/wp-content/uploads/2025/05/Fiscal-Year-2026-Discretionary-Budget-Request.pdf>.
- Alter, Adam L., and Daniel M. Oppenheimer. “Uniting the Tribes of Fluency to Form a Metacognitive Nation.” *Personality and Social Psychology Review* 13, no. 3 (2009). <https://doi.org/10.1177/1088868309341564>.
- Census Bureau. “2022 Census of Governments - Organization.” Last revised April 23, 2025. <https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html>.
- Chen, Zhanhao, and Janos Szurdi. “Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers.” Unit 42, September 1, 2020. <https://unit42.paloaltonetworks.com/cybersquatting/>.
- Cybersecurity and Infrastructure Security Agency. “CISA Announces Transfer of the .Gov Top-Level Domain from U.S. General Services Administration.” 2021. CISA. March 8, 2021. <https://www.cisa.gov/news-events/news/cisa-announces-transfer-gov-top-level-domain-us-general-services-administration>.
- Cybersecurity and Infrastructure Security Agency. “Official list of .gov domains” GitHub. Accessed on April 10, 2025. <https://github.com/cisagov/dotgov-data>.
- Cybersecurity and Infrastructure Security Agency. “Requirements for operating a .gov domain.” CISA. Accessed on June 1, 2025. <https://get.gov/domains/requirements/>.
- David, Anne, Tan Yigitcanlar and R.Y. M., et al. “Understanding Local Government Digital Technology Adoption Strategies: A PRISMA Review.” *Sustainability* 15, 9645 (2023): 1-43. <https://doi.org/10.3390/su15129645>.
- Internet Assigned Numbers Authority. “Root Zone Database.” Internet Assigned Numbers Authority. <https://www.iana.org/domains/root/db>.
- Keller, Kevin Lane. “Conceptualizing, Measuring, and Managing Customer-Based Brand Equity.” *Journal of Marketing* 57, no. 1 (1993), pages 7-8. <http://www.jstor.org/stable/1252054>.
- Koenig, Alexa and Jonathan Stein. “Federalism and the State Recognition of Native American Tribes: A Survey of State-Recognized Tribes and State Recognition Processes across the United States.” *Santa Clara Law Review* 48, no. 1 (2008), page 83. Accessed at <https://digitalcommons.law.scu.edu/lawreview/vol48/iss1/2>.
- Letter To the Honorable Susan Collins, Chair of the Senate Appropriations Committee. May 2, 2025. <https://www.whitehouse.gov/wp-content/uploads/2025/05/Fiscal-Year-2026-Discretionary-Budget-Request.pdf>.

- Menon, Theo and William T. Alder. “More Election Offices are Adopting Verified, .gov Websites.” Bipartisan Policy. July 19, 2024. <https://bipartisanpolicy.org/blog/more-election-offices-are-adopting-verified-gov-websites/>.
- Metzger, Miriam J., and Andrew J. Flanagin. “Psychological Approaches to Credibility Assessment Online” in *The Handbook of the Psychology of Communication Technology*, First Edition, edited by S. Shyam Sundar (John Wiley & Sons, Inc., 2015).
- National Association of Counties. “America’s County Governments: A Primer on County-Level Election Administration.” November 4, 2024. <https://www.naco.org/resource/americas-county-governments-primer-county-level-election-administration>.
- National Center for Interstate Compacts. “NCIC Database.” Last updated April 7, 2025. <https://compacts.csg.org/database/>.
- National Conference of State Legislatures. “Federal and State Recognized Tribes.” Archived by the Internet Archive on September 1, 2022. <https://web.archive.org/web/20220901061023/https://www.ncsl.org/legislators-staff/legislators/quad-caucus/list-of-federal-and-state-recognized-tribes.aspx>.
- Native Nations Institute at the University of Arizona. “Governance Under State Recognition.” Accessed April 19, 2025. <https://nni.arizona.edu/our-work/research-policy-analysis/governance-under-state-recognition>.
- Obermiller, Carl. “Varieties of Mere Exposure: The Effects of Processing Style and Repetition on Affective Response.” *Journal of Consumer Research* 12, no. 1 (1985), pages 18–19. <http://www.jstor.org/stable/2489378>.
- Ramesh, Reethika, and Zhanhao Chen. “IRS-themed Domains Used for CAPTCHA-Style Paste Hijacking Pages” GitHub. April 15, 2025. <https://github.com/PaloAltoNetworks/Unit42-timely-threat-intel/blob/main/2025-04-15-IOCs-for-IRS-themed-domains-used-in-CAPTCHA-style-paste-hijacking.txt>.
- Szurdi, Janos. 2021. “A Peek into Top-Level Domains and Cybercrime.” Unit42. November 11, 2021. <https://unit42.paloaltonetworks.com/top-level-domains-cybercrime/>.
- Take9. “Take 9 seconds before you click, download, or share.” Take9. <https://pausetake9.org/>.
- U.S. Government. “Federally recognized American Indian tribes and Alaska Native entities.” Last modified March 25, 2025. <https://www.usa.gov/indian-tribes-alaska-native/>.
- U.S. Government. “Requirements for the registration and use of .gov domains in the federal government.” Digital.gov. <https://digital.gov/resources/requirements-for-the-registration-and-use-of-gov-domains-in-the-federal-government>.
- U.S. House of Representatives. “6 USC 665: Duties and authorities relating to .gov internet domain.” U.S. Code. [https://uscode.house.gov/view.xhtml?req=\(title:6%20section:665%20edition:prelim\)%20OR%20\(granuleid:USC-prelim-title6-section665\)&f=treesort&edition=prelim&num=o&jumpTo=true](https://uscode.house.gov/view.xhtml?req=(title:6%20section:665%20edition:prelim)%20OR%20(granuleid:USC-prelim-title6-section665)&f=treesort&edition=prelim&num=o&jumpTo=true).

- Utah. "Use of an Authorized Top-Level Domain." Accessed on May 31, 2025. <https://cybercenter.utah.gov/Requests/>.
- Wineburg, Sam, and Sarah McGrew. "Lateral Reading and the Nature of Expertise: Reading Less and Learning More When Evaluating Digital Information" *Teachers College Record*, (2018). https://stacks.stanford.edu/file/druid:yk133ht86o3/Wineburg%20McGrew_Lateral%20Reading%20and%20the%20Nature%20of%20Expertise.pdf.
- Zucker, Lynne G. "Production of trust: Institutional sources of economic structure, 1840–1920." *Research in Organizational Behavior* 8, (1986), pages 53-111. <https://digicoll.lib.berkeley.edu/record/70599>.

Acknowledgments

ChatGPT was leveraged for initial brainstorming, guidance on statistical technique selection, and light editing to improve grammar, clarity, and structure.

I would like to thank the UC Berkeley Center for Long-Term Cybersecurity (CLTC) for the opportunity to conduct and publish this research, and for the opportunity to present its key findings at the 2025 Cyber Civil Defense Summit in Washington, D.C.

In particular, I would like to thank CLTC's Shannon Pierson for her support and guidance throughout the process and Chuck Kapelke for improving the quality of the final draft.

I am grateful to all CLTC's funders for their support, with particular thanks to Craig Newmark Philanthropies, Okta for Good, and Google.org.

Finally, I am grateful to my wife, Kelsey, for her unwavering support of all my initiatives and wild ideas. This paper could not have been completed without all the support described above.

About the Author

Chris Babcock, Major, U.S. Air Force, is a cyber defense analyst whose experience spans across all levels of operations and strategy. A graduate of the U.S. Air Force Cyber Weapons School and certified GIAC Network Forensic Analyst (GNFA) with over a decade of experience, he specializes in cyber incident response, threat mitigation, and resilience planning. He has led and scaled teams defending national security operational technology systems and crafted organization-wide cybersecurity and defense strategies. He has directed complex, multi-organization incident response efforts against advanced persistent threats and advised senior leaders on risk mitigation strategies. An advocate for elevating diverse perspectives and improving risk communication, he has designed and implemented training programs reaching thousands of cybersecurity professionals annually. Passionate about building proactive security frameworks, he is committed to developing high-performing teams capable of defending against the world's most sophisticated cyber threats.



CLTC

Center for Long-Term
Cybersecurity

UC Berkeley