Response to usTLD Registry Management & Maintenance RFI

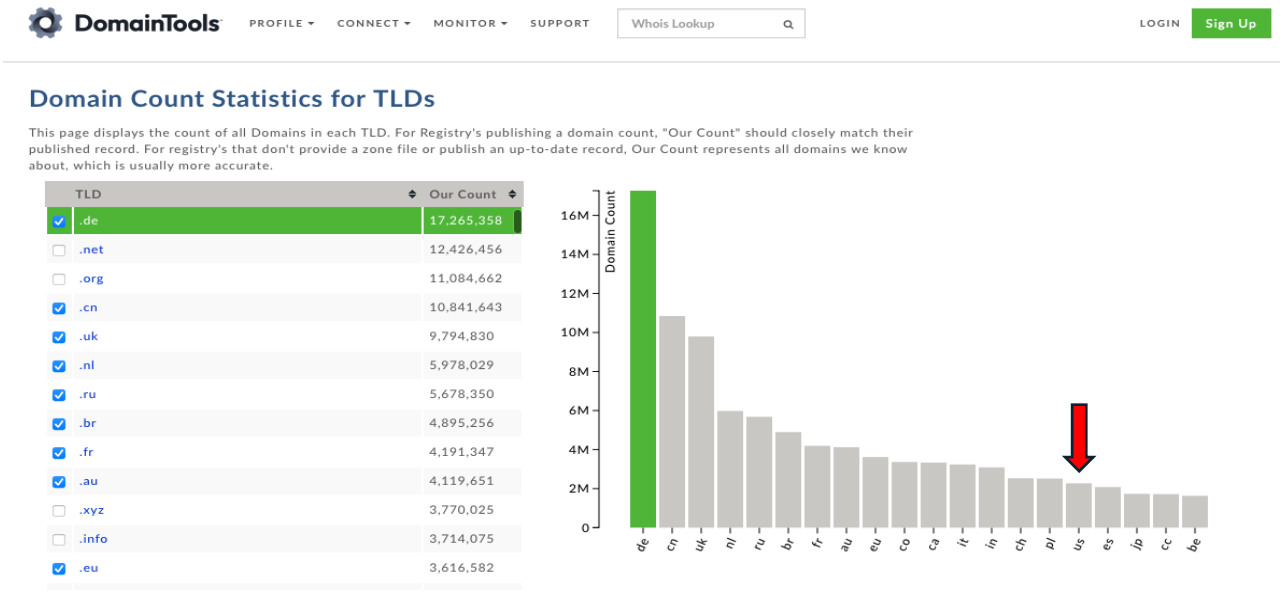
By Michael Palage and Rick Lane

1.0 Executive Summary

The Request for Information (RFI) issued on 17 January 2025, in the waning days of the Biden administration, largely proposed that the United States Government (USG) continue the status quo in connection with its administration of the .US country code top-level domain (ccTLD). For the reasons set forth in this response, it is recommended that the Trump administration expand the scope of the original RFI to make the .US ccTLD best in class and align its operations with the current administration's objective to increase government efficiency. **The .US ccTLD is critical national infrastructure through and the USG has the potential to recognize over one hundred million dollars in new revenue over the course of the next contract.** While the RFI stated that the USG would not directly disclose or distribute information received in response to this RFI, this response has been publicly posted and shared with the Congressional Department of Government Efficiency (DOGE) Caucus and the Senate Inspector General Caucus, and the Senate and House Commerce Committees.

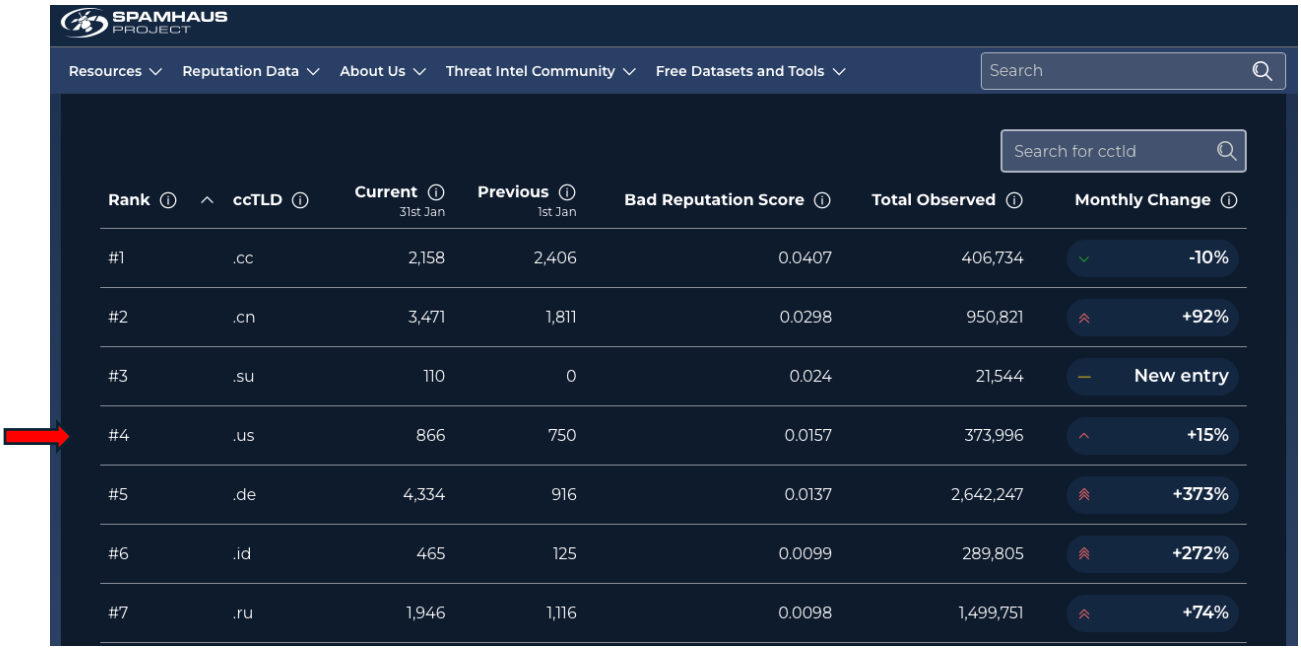
2.0 Current .US ccTLD Metrics

Despite the US being the world's number one economy with a gross domestic product (GDP) in excess of 26 trillion dollars, as illustrated in the chart below the .US ccTLD is only the 16th largest ccTLD trailing behind the likes of China(.CN), Russia (.RU), Brazil(.BR), India (.IN).



Source: DomainTools, https://research.domaintools.com/statistics/tld-counts/ (February 2025)

Sadly, one of the few categories in which the .US ccTLD currently finds itself in the top five is a category that it should not be in. As indicated in the table below, SPAMAUS currently listed the .US ccTLD as the fourth worst ccTLD in connection with illegal phishing activities.



Rank	ccTLD	Current (31st Jan)	Previous (1st Jan)	Bad Reputation Score	Total Observed	Monthly Change
#1	.cc	2,158	2,406	0.0407	406,734	-10%
#2	.cn	3,471	1,811	0.0298	950,821	+92%
#3	.su	110	0	0.024	21,544	New entry
#4	.us	866	750	0.0157	373,996	+15%
#5	.de	4,334	916	0.0137	2,642,247	+373%
#6	.id	465	125	0.0099	289,805	+272%
#7	.ru	1,946	1,116	0.0098	1,499,751	+74%

Source: Shamhaus, https://www.spamhaus.org/reputation-statistics/cctlds/phishing/ (February 2025)

3.0 Base Contract Terms

The outgoing Biden administration proposed retaining the existing fixed-price no cost contract, in which the Contractor would not receive any funding from the USG. The USG has used this contractual framework for the past several decades, however, it ignores current best practices in which Contractors are **PAYING** national governments for the right to operate their ccTLD. While a no-cost contract is good, receiving revenue, potential in excess of one hundred million dollars, is even better. To illustrate the disparity which the USG currently finds itself, consider the .US (United States) and .CO (Colombia) ccTLDs for which GoDaddy Registry Services is the backend registry operator for both TLDs.

In connection with the operation of the .US ccTLD under its current contract with the USG, GoDaddy receives 100% of all of the revenues associated with the over 2.2 million Domains Under Management (DUMs), or over $14 million dollars annually, while the USG receives no financial remuneration. In comparison, the Colombia government has received more than over 500 billion

Colombian pesos ($120 million) in connection with GoDaddy's operation of the .CO ccTLD since 2020.[1] Prior to 2020 contract, the Colombia government only received approximately 6-7% of the revenue associated with domain name registration fees, however, after a competitive tender, than percentage increased to 81%.[2] This trend of Registry Services providers, such as GoDaddy, paying governments for the right to operate their ccTLD for a share of the revenues generated from domain name registration fees is a clearly emerging trend. In 2022, GoDaddy entered into a registry services contract with the government of Tuvalu to operate the .TV ccTLD in which it was reported that the government received well in excess of $5 million annually.[3] Similarly, Identity Digital, another registry service provider, recently announced a partnership with the Anguilla government to commercialize the .AI ccTLD.[4] Simply put, the USG should put out a competitive tender for the .US ccTLD in which **the USG should include a revenue sharing arrangement as part of any future .US RFP**.

Additionally, the proposed terms put forth by the former Biden administration of an initial two-year term followed by 4 two-year renewals is inconsistent with current industry best practices as explained below in greater detail. Additionally, the proposed renewal of the registry agreement every two years is inefficient and represents an administrative burden to the USG.

.EU (EURid)

The European Registry for Internet Domains (EURid) was appointed as the ccTLD manager of the .EU ccTLD by the European Commission (EC) following a competitive tender process in 2003.[5] EURid's administration of the TLD includes the provision of technical registry services. The first service contract expired in 2009[6] and was renewed in 2014 for an additional 5 years after an EC call for expression of interest.[7] In 2019 EURid extended the then current services contract for 3 years until 2022.[8] EURid signed a new services contract in 2022 with an additional 5 year term, with the option for an additional 5 years.[9]

.AU (auDA)

The .au Domain Administration (auDA) is the ccTLD Manager that administers the .AU ccTLD which is currently the 10th largest TLD with 4.3 million Domains Under Management (DUMs).[10] However, auDA has always contracted out the technical backend registry infrastructure to a third-party RSP. The last two public RFP tenders that auDA has undertaken in 2017 and 2023 have both included the following provision:

> Initial Term of 4 years with an option for auDA to extend for a further two years. Upon the expiry or termination of the Registry Services Agreement, auDA also has the right to require the Registry Operator to comply with the agreement for a further period of up to 12 months following the expiry or termination.[11]

---

[1] https://www.larepublica.co/economia/dominio-co-entre-los-mas-grandes-de-america-latina-con-ingresos-por-mas-de-medio-billon-3906627 (Spanish)
[2] https://www.financecolombia.com/neustar-subsidiary-wins-renewal-of-co-domain-registrar-contract-with-colombian-government/
[3] https://www.abc.net.au/pacific/programs/pacificbeat/tuvalu-tv-deal/13704112
[4] https://www.winnmediaskn.com/the-government-of-anguilla-forges-a-partnership-with-digital-identity/
[5] https://eurid.eu/en/welcome-to-eurid/eu-timeline/
[6] https://icannwiki.org/EURid
[7] https://eurid.eu/en/welcome-to-eurid/eu-timeline/
[8] https://eurid.eu/en/news/eurid-ec-service-concession-contract-extended/
[9] https://eurid.eu/en/news/eurid-signs-contract-with-ec/
[10] https://dnib.com/articles/the-domain-name-industry-brief-q3-2024
[11] https://assets.auda.org.au/a/2023-05/rft_-_auda_registry_operator_procurement_2023_release_version_-_1_may_2023.pdf?VersionId=zr9OqhXKsG3qOfhzf5M_aiKsAhNk6VvA

.FR (Afnic)

Afnic is the ccTLD Manager that administers both operational and technical operations of the .FR ccTLD. There does not appear to be any formal tender process, however, the French government does appear to make a periodic decree every 5 years.[12]

.IN (NIXI)

The National Internet Exchange of India (NIXI) is the government agency responsible for overseeing the .IN ccTLD. Traditionally, NIXI contracted with a third party to provide administrative and technical operations. In 2017, RFP NIXI proposed an initial 5-year term with the ability to seek an extension.

> **RECOMMENDATION**: The baseline contractual term for the .US ccTLD should be five (5) years, with an option for an additional five (5) years provided that agreed upon technical Service Level Agreements (SLAs); financial benchmarks (e.g. revenue sharing goals); and policy objectives (e.g. minimizing abuse, data accuracy/access, etc.) are met.

4.0 DNS Abuse

NTIA in the RFI stated that it is considering "**enhancing**" the .US Statement of Work (SOW) to include DNS Abuse. However, according to the .US website DNS Abuse is currently defined as including, but not limited to phishing, pharming, dissemination of malware, fast flux hosting, botnetting, malicious hacking; SPAM (as a mechanism for DNS Abuse); illegal sale of pharmaceuticals online; and Child Sexual Abuse Material (CSAM).[13] However, the ICANN definition cited in the RFI for DNS Abuse actually represents a **substantial weakening** of consumer safeguards and protections. ICANN's current definition of DNS Abuse **ONLY** includes phishing pharming botnets, malware and spam when it serves as a delivery mechanism for DNS Abuse. It is disappointing that the Biden administration in the RFI would tout potential "enhancing the SOW to include more rigorous requirements" when in fact this ICANN definition actually represents a substantial weaking of safeguards in the .US namespace.

NTIA specifically cites the recent ICANN contractual amendments with Registrars and Registries as a basis for the **purported** enhancements and more rigorous DNS Abuse requirements. However, NTIA choose to ignore more comprehensive definitions put forth by both the private and public sectors. From a private sector perspective, the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) in their response to the .US RFI cites their previous work entitled DNS Abuse Prevention, Remediation, and Mitigation Practices for Registrars and Registries which identifies best practices in this area.[14] Whereas the European Union adopted a much more expansive definition of DNS Abuse that includes "any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity" and which aligns more closely with the current .US DNS Abuse definition.[15]

---

[12] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000026078782, https://www.afnic.fr/en/observatory-and-resources/news/afnic-continues-as-the-registry-for-the-fr-tld-2/, and https://www.afnic.fr/en/observatory-and-resources/news/afnic-renewed-as-registry-for-fr/

[13] https://www.about.us/policies/usTLD-Statement-to-Combat-Domain-Name-Abuse

[14] https://www.m3aawg.org/sites/default/files/dns_abuse_prevention_remediation_and_mitigation_practices_for_registrars_and_registries.pdf

[15] https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1#:~:text=Domain%20Name%20System%20(DNS)%20abuse%20is%20any%20activity%20that%20makes,out%20harmful%20or%20illegal%20activity.

While NTIA has a been a staunch advocate of the multistakeholder model over the past several decades, it is worth noting that the cited ICANN contractual amendments with its Registry and Registrar contracting parties did not follow the multistakeholder Policy Development Process (PDP) model enshrined in the ICANN bylaws. Instead, these changes occurred through private bilateral contractual negotiations between ICANN and the Registrars and Registries. While ICANN and its contracting parties have touted these changes as evidence of the multistakeholder model working, history provides a much starker reality.

In 2019 at the Global Domains Division (GDD) Summit in Bangkok, Thailand, there were two sessions held on May 9th where the topic of "DNS Abuse and Consumer Safeguards" were discussed.[16] These recorded sessions make crystal clear that the contracting parties had no intention of utilizing the PDP to address DNS Abuse or Consumer safeguards. During these sessions, ICANN staff expressed the concern about national legislation defining DNS Abuse like the European General Data Protection Regulation (GDPR) defining basic privacy rights. Over the next several years ICANN and the contracting parties engaged in private negotiations which excluded large segments of the ICANN multistakeholder community. Attempts to obtain some of these communications between ICANN and the contracting parties through ICANN's Documentary Information Disclosure Policy (DIDP)[17] were declined by ICANN's legal office.[18]

While ICANN's narrow definition of DNS Abuse accommodates the business objectives of its Registrars and Registries, it does not address the legitimate concerns of Internet users that are harmed by this illegal activity within the .US namespace. Therefore, the USG should propose a more expansive definition of the current .US DNS Abuse definition to include facilitating the sale and/or distribution of goods and/or services that infringe intellectual property rights. As the current Trump administration looks to revitalize US manufacturing, it should provide corresponding safeguards to protect these investments.

> **Recommendation**: The .US SOW should include metrics by which Contractor address and mitigate DNS Abuse including but not limited to 1) phishing; 2) pharming; 3) botnets; 4) malware; 5) Child Sexual Abusive Material (CSAM); 6) facilitating the distribution of illegal/unauthorized pharmaceutical products; 7) facilitating the sale and/or distribution of goods and/or services that infringe intellectual property rights; and 8) spam (when spam serves as a delivery mechanism for the foregoing abusive activities).

5.0 Third-Party Data Access to Registration Data and Data Accuracy

Third Party Data Access to Registration Data

Protecting the privacy of .US registrants from unwanted spam and commercial solicitations is a legitimate concern. Unfortunately, under the Biden administration, NTIA appeared to prioritize this perspective above the concerns of US businesses, law enforcement, cybersecurity organizations, consumer protection agencies, and child safety advocates that were calling for more timely access to accurate domain name registrations data. Having timely access to this data is vitally important to aid both criminal and civil investigations involving online illegal activity occurring within the .US namespace.

---

[16] https://www.icann.org/resources/pages/gdd-summit-session-recordings-2019-05-08-en
[17] https://www.icann.org/resources/pages/didp-2023-01-24-en
[18] DIDP Request 20230815-1 (Request #3), https://www.icann.org/resources/pages/didp-20230815-1-palage-request-2023-09-18-en

After the GDPR went in effect, access to most generic top-level domain (gTLD) registrant registration data went "dark." This is why US businesses and citizens expressed their concern when NTIA and GoDaddy began circulating ideas to restrict access to domain name registration data.[19] Free and open access to domain name registration data has been a hallmark of the .US ccTLD operation since its conception. The importance of timely access to domain name registration data has not only been reiterated by the private sector, but by several USG agencies.

> "HSI views WHOIS information, and the accessibility to it, as critical information required to advance HSI criminal investigations, including COVID-19 fraud. Since the implementation of GDPR, HSI has recognized the lack of availability to complete WHOIS data as a significant issue that will continue to grow. If HSI had increased and timely access to registrant data, the agency would have a quicker response to criminal activity incidents and have better success in the investigative process before criminals move their activity to a different domain."
> **Source**: U.S. Homeland Security Criminal Investigations Letter to Congress (July 2020)[20]

> "Access to WHOIS information has been a critical aspect of FDA's mission to protect public health. Implementation of the E.U. General Data Protection Regulation (GDPR) has had a detrimental impact on FDA's ability to pursue advisory and enforcement actions as well as civil and criminal relief in our efforts to protect consumers and patients."
> **Source**: FDA Letter to Congress Regarding Criminal Case Investigations[21]

> "Before the GDPR took effect in May 2018, the FTC and other consumer protection and law enforcement agencies routinely relied on the publicly-available registration information about domain names in WHOIS databases to investigate wrongdoing and combat fraud. The FTC uses this information to help identify wrongdoers and their locations, halt their conduct, and preserve money to return to defrauded victims. Our agencies may no longer rely on this information because, in response to the GDPR, ICANN developed new policies that significantly limit the publicly available contact information relating to domain name registrants."
> **Source**: FTC Letter to Congress on Consumer Protection Investigations[22]

GoDaddy as the world's largest domain name Registrar has long promoted the use of Privacy/Proxy Services which mask the identity of the beneficial registrant/user of a domain name. In fact, GoDaddy in the early 2000s were providing privacy/proxy services for .US domain name registrations in violation of the .US contractual requirements. One of GoDaddy's registrant customers, Robert Peterson, sued NTIA alleging a First Amendment right to have his registration data withheld from public disclosure. The Court of Appeals for the Fourth Circuit affirmed the district court's denial of the registrant's request for a temporary restraining order and upheld NTIA's prohibition of privacy and proxy services in the .US namespace.[23]

---

[19] https://www.ntia.gov/blog/2023/proposal-more-privacy-domain-name-personal-data (A Proposal for More Privacy in Domain Name Personal Data) and https://www.about.us/policies/ustld-stakeholder-council/ustld-privacy-recommendation (usTLD Recommendation for Privacy Plan).
[20] https://secureandtransparent.org/wp-content/uploads/2020/09/20-02497-ICEs-Signed-Response-to-Representative-Latta.pdf
[21] https://secureandtransparent.org/wp-content/uploads/2020/09/2020-2860-RESPONSE.pdf
[22] https://secureandtransparent.org/wp-content/uploads/2020/09/2020.07.30-FTC-to-Rep.-Latta-WHOIS.pdf
[23] https://caselaw.findlaw.com/court/us-4th-circuit/1487811.html

Data Accuracy

Unfortunately, NTIA only references data accuracy in passing in the RFI. Current data accuracy requirements within the .US TLD are contained in the WHOIS Data Reminder Policy.[24] Sadly, these data accuracy requirements largely mirror those imposed by ICANN on its contracting parties. Specifically, Registrars must "validate" email, telephone, and postal data fields, e.g. emails contain an @ symbol, US telephone numbers have 8 digits +1.XXX.XXXX, and postal data complied with the S42 address templates. Registrars are only required to operationally "verify" either the email **OR** the telephone number ONCE. After the initial registration, the "Registrar is not required to perform the above validation and verification procedures above, if Registrar has already successfully completed the validation and verification procedures on the identical contact information and is not in possession of facts or knowledge of circumstances that suggest that the information is no longer valid."[25] Therefore, a domain name that has been registered and renewed for multiple terms (years) is only required to be operationally verified once unless that registrar is in possession of additional facts or knowledge.

Because the Registrar are **only** required to verify the operation of either the registrant's email address OR the telephone number, this represents an incredibly low bar to data accuracy. Criminals can comply with these data accuracy requirements by merely using a disposable email address from any free provider (e.g. Gmail) provided that the other data fields are syntactically correct (validated). The insanity of this definition of "accuracy" was discussed in greater detail in this white paper through the actual registration of the domain name icannsdefinitionofaccuracyisajoke.com.[26] The European Union in connection with its national cybersecurity directive (NIS 2.0) established a standing body, the Cooperation Group, to proposed various policies regarding data accuracy.[27] Notably, these recommendations require the syntactical validation of data fields and the operational verification of email and telephone at the time of initial registration and on an annual ongoing basis.

The .US Contractor is required to "perform random verifications of Registered Name Holder's data" throughout the year.[28] In December of 2022, Representatives Robert Latta and Jan Schakowsky submitted a bipartisan letter to the NTIA raising concerns about NTIA and GoDaddy's proposal to modify the contractual obligations regarding .US domain name registration data, as well as requesting "copies of the annual WHOIS Accuracy and the Security Audit Data annual reports conducted by the .US Contracted Parties (Neustar and GoDaddy), as required under the same .US Contract."[29] Upon information and belief, these document have not yet been produced and they do not appear to be publicly available on the .US website.

Recommendations:

1) The USG shall continue to prohibit the use of Privacy and Proxy services in connection with the registration of .US domain names, consistent with the legal principles articulated by the 4th Circuit Court of Appeals in 2007.

---

[24] https://www.about.us/documents/policies/WHOIS_Data_Reminder_Policy.pdf
[25] https://www.about.us/documents/policies/WHOIS_Data_Reminder_Policy.pdf (Page 4).
[26] https://circleid.com/pdf/NIS-WhitePaper-Final-1.0 (Section 3.0 Case Study, Page 2)
[27] https://ec.europa.eu/newsroom/dae/redirection/document/108437
[28] https://www.about.us/documents/policies/WHOIS_Data_Reminder_Policy.pdf (Page 5)
[29] https://secureandtransparent.org/wp-content/uploads/2022/12/12.14.22-Letterhead-NTIA-US-WHOIS-Latta-Schakowsky.pdf

2) Contractor shall require all .US Registrants (both existing and future) to identify themselves as either a natural or legal person and indicate their appropriate .US Nexus Code[30] and such information shall be publicly available via WHOIS/RDDS. Existing Registrants will have 60 days after the commencement of the new SOW to make that designation or have their domain name suspended.
3) Contractor shall require all .US Registrants to validate and verify an operational email and telephone number at the time of initial registration, and on an annual ongoing basis.

6.0 Nexus Requirements

In theory nexus requirements are a legitimate safeguard incorporated into the operation of several ccTLD, e.g. Canada (.CA), Australia (.AU), England (.UK), Europe (.EU), and France (.FR). However, there are other ccTLD Registry Operators which seek to operate their ccTLD as a hybrid gTLD, e.g. Colombia (.CO), Tuvalu (.TV), Montenegro (.ME), and Anguilla (.AI). Unfortunately, the current Registry Operator does not appear to make any metrics available regarding Nexus challenges for there to be any objective analysis as to whether the current policy is working. In theory, .US Nexus Code 31 (foreign entity or organization that has a bona fide presence in the US) or 32 (foreign entity that has an office or other facility in the US) seem sufficient and in line with the current Trump administration's efforts to stimulate investing in US manufacturing.

Recommendation: Contactor shall provide annual metrics regarding Nexus challenges and any compliance activities as part of it's annual Stakeholder Council Reports.[31]

7.0 KIDS.US

To fully understand the dynamics, it is helpful to take a historical BIG picture perspective of the Dot Kids Implementation and Efficiency Act of 2002. In the early 2000's the US government was still attempting to take a light touch approach toward regulating internet activity. In May 2002, then Representative Mike Pence from Indiana, introduced the Truth in Domains Act (H.R.4658) which sought to prohibit knowingly using a misleading domain name with the intent to attract a minor into viewing a visual depiction of sexually explicit conduct on the Internet. At this time known typo squatters were registering misspelling of popular children's websites and directing users to pornographic content. It is also worth noting that during this time the domain name WHITEHOUSE.COM resolved to a pornographic website.[32] While the initial Truth In Domains Act was not adopted in that Congress, provisions of that Bill were included in the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003 ("PROTECT Act") which were signed into law by then President Bush.

The Dot Kids Implementation and Efficiency Act of 2002 was signed into law on December 4, 2002, and directed NTIA to require the Registry Operator of .US to delegate and operate a KIDS.US namespace. Earlier discussions of this Bill called for the introduction of a .KIDS generic top-level domain (gTLD). While the USG at this time had the legal authority to add the .KIDS TLD to the Internet Root Zone, such an action would have undermined ICANN's legitimacy on the global stage, so the delegation and operation of the .KIDS.US was a compromise. Section 157(i) of the Dot Kids provided NTIA the authority "on its own review or upon a good faith

[30] https://www.about.us/documents/policies/usTLD_Nexus_Codes.pdf
[31] https://www.about.us/stakeholders/stakeholder-council-reports
[32] https://www.computerworld.com/article/1323850/porn-site-whitehouse-com-domain-name-up-for-sale.html

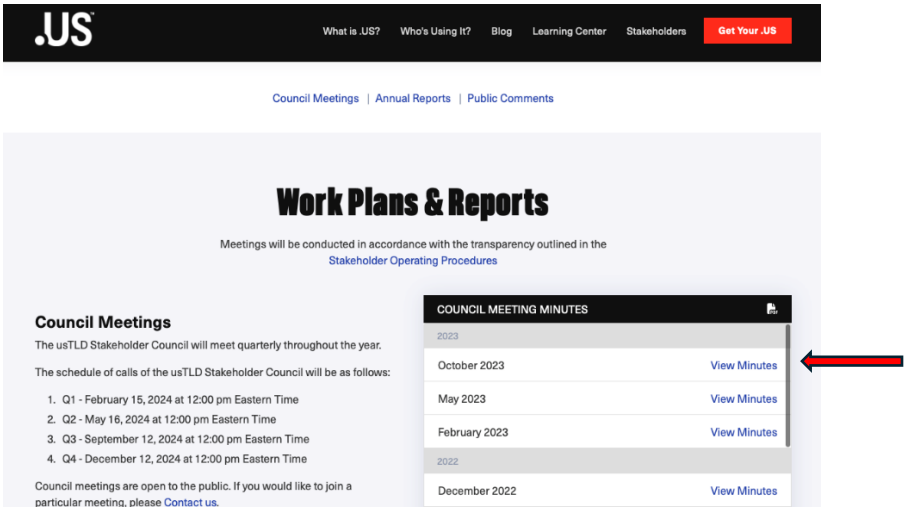
petition by the registry" to suspend the KIDS.US domain if the "new domain is not serving its intended purpose."[33] On July 27, 2012 the KIDS.US namespace was indefinitely suspended.[34] In light of the delegation of the .KIDS TKD in 2022, it makes little sense for KIDS.US to be referenced in any future SOW.[35]

> **Recommendation**: There should be no future obligations imposed in the SOW regarding the KIDS.US namespace until a clearly defined use of kids.us is provided.

8.0 Multistakeholder Approach

There has been a lot of recent discussion about the genesis and success of the multistakeholder model, so it is rather timely that NTIA has included this topic in the RFI. For those not fully immersed in this multistakeholder concept and its complex 25 plus year legacy, it would be informative to read competing viewpoints by Milton Muller and Alex Klimburg on CircleID.[36] While there is merit in Muller's assessment that multistakeholderism is a "muddied distinction between governance by state actors and non-state actors", there is equal merit in Klimburg's statement about how this concept has help preserve a free and open internet over the past several decades. The USG has traditionally advocated a light-weight regulatory approach toward internet governance, instead advocating for private sector led solutions. Unfortunately, the stark reality is we live in a world where more governments, including the USG, have identified the domain name system as critical national infrastructure and have begun regulating it accordingly. These recent legislative actions by the US, Australian, European Union, Russian and Chinese governments raise serious questions about the continued viability of the multistakeholder model. To help inform the USG in this analysis it is important to look at the current short comings of multistakeholder model in the administration of the .US ccTLD.

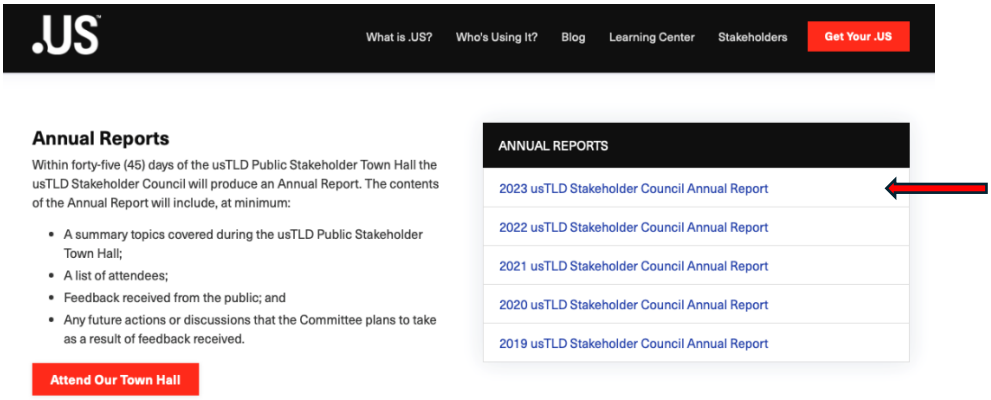
Objectively speaking the output of the .US Stakeholder Council is underwhelming. Until February 4th the most recent Council Meeting Minutes on the website were from October 2023.



[33] https://www.congress.gov/107/plaws/publ317/PLAW-107publ317.pdf
[34] http://kids.us
[35] https://www.iana.org/domains/root/db/kids.html
[36] See Muller, M., (November 2024), *Why We Need to Discard the Word "Multistakeholder"*, CircleID, https://circleid.com/posts/why-we-need-to-discard-the-word-multistakeholder and Klimburg, A., (December 2024), *Multistakeholderism and Its Discontents*, CircleID, https://circleid.com/posts/multistakerholderism-and-its-discontents-a-reply

Source: https://www.about.us/stakeholders/stakeholder-council-reports (3 February 2025)

The .US Town Hall was held on 31-October-2024.[37] However, despite a requirement to produce an Annual Report within forty-five (45) days of the such Town Hall, as of 3-February-2025 no such annual report has been posted.



Source: https://www.about.us/stakeholders/stakeholder-council-reports (3 February 2025)

On February 4th, the annual 2024 usTLD Stakeholder Council Annual report was posted on the usTLD Stakeholder Council website. However, now only the two most recent annual reports are publicly posted with user required to contact the Registry Operator to obtain these archived reports.

Despite other ccTLDs which have implemented a host of consumer and security safeguards to respond to emerging threats and regulatory requirements over the past several years, the .US Stakeholder Council has engaged in minimum public policy discussion as evidenced by table of Public Comment Period and Reports maintained on the .US Stakeholder Council website.

Public Comment Periods

COMMENT PERIOD	OPEN DATE	CLOSE DATE	STATUS & REPORTS
2021			
usTLD Privacy Recommendation	26 Feb 2021	5 Apr 2021 (extended)	Closed |View Comments
Closed in 2017			
usTLD Privacy Service Plan	15 Dec 2016	15 Jan 2017	Closed |View Comments
usTLD Premium Domain Name Plan	15 Dec 2016	15 Jan 2017	Closed |View Comments
Closed in 2015			
Suspension of Kids.us Namespace	14 May 2015	13 Jun 2015	Closed |View Comments
usTLD Stakeholder Council Operating Procedures	15 Dec 2014	14 Jan 2015	Closed |View Comments
usTLD Stakeholder Council Work Plan	15 Dec 2014	14 Jan 2015	Closed |View Comments

[37] https://www.about.us/stakeholders

Source: https://www.about.us/stakeholders/stakeholder-council-reports (3 February 2025)

In fact, one of the only substantive policies that the .US Stakeholder Council has considered over the past several years is usTLD Privacy Recommendation (see above). While the protecting the privacy of .US registrants from unwanted spam and commercial solicitations is a fair and valid concern, it should not override the legitimate interests of other parties such as law enforcement, consumer/child protection and cybersecurity entities, and intellectual property owners trying to investigate illegal activity online. While NTIA, under the prior Biden Administration, appeared to proactively support enhanced privacy protections in connection with domain name registrant data[38], this view appears to conflict with the view of other USG agencies such as the Federal Trade Commission (FTC) and the Food and Drug Administration (FDA), and Homeland Security which placed the accuracy and access of registrant data over privacy concerns.[39]

Perhaps the most disappointing aspect of the lack of any meaningful activities over the past several years is the fact the current Contractor specifically requested a $0.50 per domain name fee per year to fund usTLD Stakeholder Council activities.

> The maximum wholesale fee to Registrars of $6.00 for a usTLD second-level domain name has only changed once over the last decade with the addition of the usTLD Stakeholder Council Fee of $0.50 per domain name per year introduced in 2014.
>
> Source: Solicitation Number: 1331L5-19-R-1335-0001 (Volume 1 Technical Capabilities)[40]

Over the past several years, Registry Services, LLC (GoDaddy) has collected millions of dollars in fees from .US registrants with little to show from a Return on Investment (ROI) perspective. Sadly, this lack of meaningful activity is eerily familiar to activities of the International Foundation for Online Responsibility (IFFOR) which was responsible for policy and advocacy in connection with the .XXX gTLD. Shortly after GoDaddy's acquisition of ICM Registry (the Registry Operator of .XXX) in 2021[41], GoDaddy and ICANN began negotiating for the removal of IFFOR from the registry agreement along with several enumerated obligations outlined in the original registry agreement,

The inactivity of the usTLD Stakeholder Council may be attributable to its composition. As of February 3rd, over 40% (3 out of 7) of the Council's members are associated with ICANN accredited registrars. On February 4th, Lauren Price from DigiCert was added as the newest member to the Council.

> **Recommendation(s):**
>
> The usTLD Stakeholder Council should be disbanded similar to how GoDaddy collaborated with ICANN to remove the International Foundation for Online Responsibility (IFFOR) from the .XXX Registry Agreement. Instead, the over **1 million dollars collected from .US registration fees should be reallocated to enhance safety and security measures, including but not limited to enhanced registrant verification and data accuracy; combating CSAM; and trusted**

---

[38] https://www.ntia.gov/blog/2023/proposal-more-privacy-domain-name-personal-data

[39] FTC's proposed Trade Regulation Rule on Impersonation of Government and Business (2022), https://www.federalregister.gov/documents/2022/10/17/2022-21289/trade-regulation-rule-on-impersonation-of-government-and-businesses and FTC communication to ICANN regarding accessibility of registrant data (July 2022), https://www.icann.org/en/system/files/correspondence/hermsen-to-marby-15jul22-en.pdf

[40] https://www.ntia.gov/files/ntia/publications/technical_proposal_volume_1.pdf (Page 9)

[41] https://domainnamewire.com/2021/04/07/godaddy-to-acquire-mmx-club-design/

notifier programs to mitigate online intellectual property rights infringement and the distribution of illegal pharmaceutical products, such as fentanyl.

The USG should be the primary source of policy for ensuring the safe and secure operation of the .US ccTLD, and the USG should align the best practices it has implemented in .GOV.

The USG shall require the .US Contractor to hold a hybrid Town Hall event (in-person and online) in connection with the annual US Internet Governance Forum (US IGF) to solicit community feedback in connection with the operation of the .US ccTLD. The Contractor shall also maintain an online mechanism where proposals can be submitted for consideration, along with a corresponding public comment forum when appropriate to help inform the USG.

If the usTLD Stakeholder Council is not disbanded, all future meetings and .US Town Halls shall be recorded and made publicly available on YouTube to provide a historical record of these meetings which will continue to exist historically independent of the current Contractor or their current contractual term,

9.0 Security

There is a growing recognition amongst national governments that the domain name system and top-level domains constitute critical national infrastructure. Therefore, it should be of paramount importance to ensure that GoDaddy is implementing best in class security safeguards in the operation of this critical infrastructure. However, as illustrated from the representative sampling of news clippings below, there is a genuine reason to be concerned about the internal security safeguards at GoDaddy:

- "Proposed order will prohibit GoDaddy from misleading customers about its security protections and require it to establish a robust information security program"
  FTC, *FTC Takes Action Against GoDaddy for Alleged Lax Data Security for its Website Hosting Services*, January 15, 2025, https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-godaddy-alleged-lax-data-security-its-website-hosting-services

- "[T]he world's largest domain name registrar, recently addressed an authentication weakness that cybercriminals were use to blast out spam through legitimate, dormant domains."
  Brian Krebs, *Cooks Continue to Exploit GoDaddy Hole*, Krebs on Security, February 4, 2019, https://krebsonsecurity.com/2019/02/crooks-continue-to-exploit-godaddy-hole/

- "In the particular case of CreamFinance and PancakeSwap, the public DNS GoDaddy was compromised. The GoDaddy DNS CNAME record had been corrupted and was not pointing to their hosting IP."
  How Hackers use DNS Hijacking Attacks to Steal Funds and Clone Websites, CERTIK, September 4, 2023, https://www.certik.com/resources/blog/6f48zdQwiqzPVF2OM8sxzc-how-hackers-use-dns-hijacking-attacks-to-steal-funds-and-clone-websites

- “Two companies that say GoDaddy unfairly clawed back domains they won at expired domain auctions have refiled lawsuit.” Andrew Allemann, *Companies refile expired domain clawback lawsuit against GoDaddy*, Domain Name Wire, December 2, 2024, https://domainnamewire.com/2024/12/02/companies-refile-expired-domain-clawback-lawsuit-against-godaddy/

Recommendation:

USG shall require Contractor that all Registrars implement mandatory non-phishable multi-factor authentication (MFA) in their systems to prevent the unauthorized transfer or manipulation of .US domain name registration data.