**Before the United States Department of Commerce**

**Washington, DC**

**Top Level Domain Registry Management & Maintenance of the .US Domain**

---

**Introduction**

Thank you for the opportunity to provide input on this important matter.

**About the ICANN Business Constituency**

The Business Constituency (BC) is the representative voice of business users of the internet and their customers as their concerns relate to governance of the domain name system (DNS). Our constituency is chartered by the Internet Corporation for Assigned Names and Numbers (ICANN), the multistakeholder body charged with maintaining a secure and stable DNS.

The BC is replying to this Request for Information (RFI) in its capacity as a party interested in the effective and safe management of the global domain name system (DNS), including the dot US top-level domain (usTLD). Our organization will not be soliciting the award of a contract to manage the usTLD namespace. Our objective is to provide the Department of Commerce information critical to a thorough examination of a potential administrator of the usTLD.

**I. Key Issue Areas as documented in Statement of Work Synopsis**

We offer our input on the following key issue areas as identified by the Department:

***DNS Abuse*: NTIA is considering enhancing the SOW to include more rigorous requirements to prevent, mitigate, and disrupt malicious activity within usTLD, including "DNS Abuse," which has been recently defined in ICANN contracts as phishing, pharming, botnets, malware, and spam (when spam serves as a delivery mechanism for the foregoing abusive activities).**

We support the Department's consideration of more stringent requirements for mitigation of DNS abuse, a persistent and rapidly growing problem for all internet users. In the United States alone, DNS abuse costs the businesses represented by the Department of Commerce millions of dollars annually.[1] Our members are victims of these increased rates of DNS abuse and are eager to find meaningful solutions.

[1] See, for example: https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

We believe that the usTLD registry should be the global leader among ccTLDs in combating fraud and abuse. Unfortunately, the operation of the usTLD has not yet met this aspirational standard. Security researcher Brian Krebs' article *Why is .US Being Used To Phish So Many of Us?* raises concerns regarding the high levels of phishing emanating from domain names in the usTLD. Krebs highlights Interisle's reports that "significant numbers of .US domains were registered to attack some of the United States' most prominent companies, including Bank of America, Amazon, Apple, AT&T, Citi, Comcast, Microsoft, Meta, and Target."

While domain name registries and registrars have taken *some* proactive steps through the ICANN contracts to curb this negative behavior, these measures have fallen short of the ultimate objective of keeping to a minimum the disruption and damage inflicted by bad actors on businesses, internet users, intellectual property rights holders, law enforcement, cybersecurity authorities, and others with a stake in the safe operation of the DNS.

Accordingly, we do not believe that the usTLD registry should adopt the strict definition of DNS abuse in recently updated ICANN contracts. This definition is not sufficient to encompass other existing types of abuse that leverage the DNS. In fact, ICANN's own Security and Stability Advisory Committee (SSAC), in its 2021 publication of SAC115, advised the ICANN Board of Directors (emphasis added):

> "These categories have been adopted within the ICANN realm in specific contracts, **but do not represent all forms of DNS abuse that exist, are reported, and are acted upon by service providers**. New types of abuse are commonly created, and their frequency waxes and wanes over time. Thus, **no particular list of abuse types will ever be comprehensive**."

The DNS research community generally supports a broader definition of DNS abuse. For example, a 2022 study on DNS abuse sponsored by the European Commission advances the following definition:

> **Domain Name System (DNS) abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity.** (Emphasis added)

We strongly recommend that the Department consider a provider for usTLD oversight that has embraced or will embrace not only an expanded definition of DNS abuse (including, for example, business and governmental impersonation, intellectual property theft, CSAM, the sale of illicit/counterfeit drugs, etc.) but provides enhanced capability for cooperation with businesses, cybersecurity authorities and law enforcement agencies to combat persistent abuse.

The Department should also consider the European Union's Cooperation Group's Guidelines on Domain Names and Registration Data published in September 2024 that describes a risk-based approach to verify the accuracy of WHOIS information (Section 3.2). It recommends that:

- A risk-based method approach should be adopted based on best practices, including taking account of the state of the art of predictive algorithms techniques;
- All registrations that present a medium to high risk of malicious registration should undergo identity verification; and
- In case of domain names used for malicious purposes, prompt actions should be taken to remove or de-activate the domain names.

These are practical solutions to reduce the amount of malicious domain names in the usTLD.

***Third party access to .us registration data, and registrant data privacy: The current SOW requires the Contractor to "maintain a publicly-accessible, accurate, and up-to-date registration (WHOIS) database for all usTLD registrations." At present, the registration information of .us registrants (e.g., name, email, physical address, and phone numbers) is published openly on the global Internet. NTIA has long supported access to .us registration data by legitimate parties who make legitimate requests. NTIA is exploring ways to enhance registrant data privacy within a registration data access system.***

We believe that access to a complete, accurate and verified database of registration data (commonly referred to as "WHOIS") is warranted and should not be undermined or otherwise artificially restricted.

There exists significant risk in closing yet another namespace. While anecdotal evidence may exist regarding the potential harms identified in the question above, there is significant, well-established and ongoing research documenting that:

- Abuse of the domain name system (DNS) and related infrastructures – including phishing, malware, pharming, impersonation and other harms – has, over time, become a rapidly growing problem;
- WHOIS is a key investigatory tool for pursuing accountability relating to criminal or abusive behavior; and
- WHOIS is critical to proactively preventing additional DNS abuse by the same bad actors.

WHOIS is a public interest tool that should be made available as efficiently as possible. Indeed, the US Government should consider requiring complete, accurate, and verified WHOIS information in the usTLD, in a manner similar to the approach taken by the European Union in its Network and Information Security Directive[2].

It is worth noting that the US government has consistently and clearly emphasized the criticality of accurate and accessible WHOIS data, both historically and in recent times. In 2006, when WHOIS-related policy development began to mature, the Federal Trade Commission established its position as solidly in favor of an open and accurate WHOIS database. Commissioner Jon Liebowitz stated:

> "**The FTC believes that the Whois databases, despite their limitations, are nevertheless critical to the agency's consumer protection mission, to other law enforcement agencies around the world, and to consumers**. The use of these databases to protect consumers is at risk as a result of the Generic Names Supporting Organization's ("GNSO") recent vote to define the purpose of Whois data as technical only. The FTC is concerned that any attempt to limit Whois to this narrow purpose will put its ability to protect consumers and their privacy in peril." (Emphasis added)

and:

> FTC investigators and attorneys have used Whois databases for the past decade in multiple Internet investigations. Whois databases often are one of the first tools FTC investigators use to identify wrongdoers. Indeed, **it is difficult to overstate the importance of quickly accessible Whois data to FTC investigations**. (Emphasis added)

Further to the FTC's interest in WHOIS policy, in comments raised in reply to the FTC's proposed Trade Regulation Rule on Impersonation of Government and Businesses, commentors were clear in their advocacy for an open WHOIS database as a means of combating impersonations of businesses and governments.

In its July 2022 letter to ICANN, the Food and Drug Administration expressed its frustration with the accessibility of WHOIS as it relates to enforcement capability. The letter reads, in part:

> "…since personal contact information within WHOIS records became unavailable to U.S. investigators under ICANN's implementation of the European General Data Protection Regulation (GDPR) in 2018, the issue regarding WHOIS access for public health and law enforcement agencies is still unresolved some four years later."

[2] See Article 23, and Recitals 109-112, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Over the last decade, NTIA also recognized the importance of the availability of WHOIS access through its participation in ICANN's Governmental Advisory Committee (GAC) discussions on WHOIS. See:

> NTIA statement to the GAC, March 13, 2018:
>
> "…I just wanted to provide some views from the United States with respect to the GDPR and how WHOIS is going to be dealt with in light of that as well as what ICANN has asked of the GAC, so if that's a good time I'm happy to carry on. So, **from the U.S. perspective maintaining access to WHOIS is very important**." (Emphasis added)
>
> NTIA statement to the GAC, March 10, 2019 (after the imposition of the European Union's General Data Protection Regulation (GDPR)):
>
> "…**we strongly believe there's a lot of urgency to making sure there are predictable, efficient ways in which to request and get access to redacted information**." (Emphasis added)

In summary, our position mirrors the position historically articulated by NTIA, as well as other governmental authorities with a stake in a safe internet namespace: that an accessible WHOIS database that permits investigatory efforts is more likely to *prevent* DNS abuse than it is to enable other types of harm.

***Nexus Requirement: The usTLD is intended to serve the Internet community of the United States and does so through a United States nexus requirement. NTIA is exploring enhancing the enforcement of the nexus requirement.***

The BC supports this requirement and its enforcement.

***Kids.us Statutory Obligation: The Dot Kids Act of 2002 (the Act) is "[a]n act to facilitate the creation of a new, second-level Internet domain within the United States country code domain that will be a haven for material that promotes positive experiences for children and families using the Internet, provides a safe online environment for children, and helps to prevent children from being exposed to harmful material on the Internet, and for other purposes." NTIA is exploring how to identify and develop potential uses of the kids.us domain that are consistent with its objective of providing a safe space on the Internet for children.***

We support this initiative.

***Multistakeholder consultation on usTLD policy: NTIA is considering requiring enhanced transparency and other adjustments to the current SOW requirement for multistakeholder community engagement in the management of the usTLD, including policy development.***

While robustly supporting transparency in DNS governance, we are concerned that, at present, the ICANN multistakeholder model does not support full transparency in policy decision-making. Further, the lack of balanced outcomes from ICANN processes has caused us concern for some time. ICANN's inability to update the WHOIS policy to restore access for businesses seeking to mitigate fraud and abuse demonstrates the limitations of the multistakeholder model.

Were the Department to invite multistakeholder participation in usTLD policy development, stakeholders on both sides of various issues should be properly heard. For example, equal bearing should be given to those who utilize WHOIS records to advance the public interest and the security and stability of the DNS vs. those who prefer to keep identities hidden.

***Security*: NTIA is considering updates and modernization of the current security commitments including cyber incident reporting.**

We support this consideration.

## II. Answers to solicitation of specific information

High level description of the Respondent's advice on how to meet and/or exceed the objectives described in the attached Statement of Work Synopsis.

With regard to overall governance of the usTLD, the BC urges the Department of Commerce to partner with its existing or new provider to:

- carefully weigh the needs of all usTLD stakeholders;
- recognize DNS abuse as the persistent and serious threat that it is; and
- strike a reasonable balance between the public interest and WHOIS access.

Further, at a high level, we urge adoption of the approach taken by the European Commission in Article 28 of its NIS2 Directive. This Directive focuses on improving responses to significant cyber-enabled nefarious activity by permitting WHOIS access for investigations, mitigation and enforcement. This data is collected and managed by registrars and, in most cases, registries as well.

Identification of specific work products or deliverables the Respondent has either produced, or is aware of, to address the key issue areas of interest as described in the attached Statement of Work Synopsis.

There are multiple studies regarding the impact of DNS abuse on the health of the DNS. We refer you to the most informative and timely:

- Interisle Consulting Group study on the cybercrime supply chain: https://interisle.net/insights/cybercrimesupplychain2024

- Internet Crime Complaint Center (IC3) 2023 Annual Report: https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

- Anti-Phishing Working Group 3rd Quarter 2024 Phishing Trends Report: https://docs.apwg.org/reports/apwg_trends_report_q3_2024.pdf

- DNS Research Federation - Why are European ccTLD abuse Rates so low? https://dnsrf.org/blog/habits-of-excellence--why-are-european-cctld-abuse-rates-so-low-/index.html

- DNS Research Federation - Privacy/Proxy Services - a Safe Haven for Cyberccriminals: https://dnsrf.org/blog/privacy-proxy-services---a-safe-haven-for-cybercriminals-/index.html

- M3AAWG Best Practices on DNS Abuse Prevention and Mitigation Practices for Registrars and Registries: https://www.m3aawg.org/sites/default/files/dns_abuse_prevention_remediation_and_mitigation_practices_for_registrars_and_registries.pdf

The extent to which the Respondent is familiar with existing markets for services to address aspects of the requirement.

We are very familiar with the market and, while not pursuing a contractual relationship with the Department, we believe it will be necessary to incorporate the factors enumerated here to ensure a safe namespace for usTLD.

The risks are considered significant for contractor performance.

Our position is that the greatest risk to contractor performance is in further reducing transparency in the usTLD to a point that nefarious actors have greater latitude to carry out abusive practices.

Any additional information the government should include in any potential solicitation to provide industry with sufficient knowledge to respond to a future solicitation.

N/A