ICANN Business Constituency (BC) Comment on

Proposed Renewal of the Registry Agreement for .COM

5-Nov-2024

Background

This document is the response of the ICANN Business Constituency (BC), from the perspective of business users and registrants, as defined in our Charter. The mission of the BC is to ensure that ICANN policy positions are consistent with the development of an Internet that:

1. Promotes end-user confidence because it is a safe place to conduct business;
2. Is competitive in the supply of registry and registrar and related services; and
3. Is technically stable, secure and reliable.

ICANN should seek community input *before* negotiating registry agreement renewals

In our comments on amendments to .BIZ, .ORG, .INFO, .ASIA, and in the Amendment 3 to the .COM Registry Agreement, the BC said that "ICANN should seek community input before negotiating registry agreement renewals." The BC is not content to merely comment after ICANN has already negotiated and approved contract changes. The BC again asks ICANN to solicit community input *before* it enters negotiations with contracted parties, so that ICANN understands the priority concerns of business users and registrants when it negotiates on behalf of the community. ICANN's failure to do so demonstrates a continuing disregard for community input and is very concerning. Moreover, it is extremely disheartening to community members such as us who are asked to provide public comments, when we know full-well that ICANN has *already* negotiated the terms of the Agreement.

Comment

The BC generally supports the Proposed Renewal of the Registry Agreement for .COM, provided that ICANN and Verisign address questions and suggestions described below.

1. Registrant and user protections from the Base RA

The BC has consistently called for legacy registry renewals to include registrant and user protections from the Base RA. As we said in 2019 regarding the migration of .ORG and .INFO to the Base RA in place at the time:

> In general, the BC supports the proposed renewal agreements negotiated between ICANN and the operators of .ORG and .INFO because they incorporate important Base Registry Agreement provisions that are valuable to BC members, including rights protection mechanisms, dispute resolution processes, the Registry Code of Conduct, and Public Interest Commitments.

The BC reiterates our support for inclusion of those Base RA elements in renewal agreements for all gTLDs, including the proposed .COM RA. This is especially important in light of the large number of domain names that are registered in the .COM registry.

The BC also supports proposed inclusion of specific obligations from the January 2023 Global Amendment to the Base gTLD Registry Agreement, such as:

- **RDAP Compliance:** Adherence to the gTLD Registration Data Access Protocol (RDAP) Profile, including Service Level Requirements for RDAP availability, round-trip and update time.
- **Updated reporting requirements:** Addressing inconsistencies in reporting RDDS queries as advised by SSAC in SAC097.
- **Adjustments to Bulk Registration Data Access (BRDA)**: Allowing ICANN to use BRDA for research purposes.

The BC also supports the proposed continuance of WHOIS for .COM, even though that was not in the Base RA. ICANN notes that "Verisign committed to continue to operate the WHOIS service in parallel with the RDAP for RDDS for .COM and requested to not have the option to sunset the obligations related to the WHOIS protocol."

2. Obligations to address DNS Abuse

The BC worked for years to encourage ICANN Org to adopt Base RA amendments with registry obligations to address DNS Abuse on domains in the TLD. We therefore support the proposed inclusion of obligations from the 2024 Global Amendment to the Base gTLD Registry Agreement related to mitigating DNS Abuse, subject to these suggestions:

2.1 The BC appreciates inclusion of a definition of DNS Abuse. While the current definition of DNS Abuse in the .COM Registry Agreement—addressing phishing, malware, botnets, pharming, and spam (when used to deliver other forms of abuse)—provides a strong foundation, it could benefit from an expanded scope to cover additional forms of abuse that are equally harmful to businesses and individuals:

- **Fraudulent Activities**:
  The current definition of DNS Abuse should include a broader range of fraudulent activities beyond phishing. This would cover domain names used for online scams, misrepresentation, or deceptive practices. For instance, some domains are created to impersonate legitimate organizations or individuals for fraudulent purposes, such as selling counterfeit products, stealing sensitive information, or

tricking users into donating to fake causes. Additionally, registering a domain using someone else's legal name to post derogatory information and personal details without consent could also be considered a form of identity fraud or harassment. These harmful activities should be explicitly recognized as DNS Abuse.

- **Brand and Reputation Abuse**:
  Another crucial form of abuse that should be addressed is brand and reputation abuse. This involves domains registered to tarnish a brand's image, steal intellectual property, or confuse consumers. For example, practices like cybersquatting or domain spoofing—where a domain is deliberately registered to imitate a well-known brand or individual—can cause significant harm to businesses and reputations. A scenario where someone registers another person's legal name as a domain and posts defamatory content or real personal details would fall under this category. Such actions damage not only the individual's reputation but also erode trust in the DNS ecosystem.

- **Emerging Cybersecurity Threats**:
  As cyberattacks evolve, the definition of DNS Abuse must remain flexible to address new and emerging threats (as the Security and Stability Advisory Committee suggested). For example, ransomware attacks, supply chain attacks, and other advanced forms of exploitation might use domain names in ways not fully covered by existing definitions like malware or botnets but pose equally serious risks. Ensuring the agreement addresses these evolving threats will allow businesses to better protect themselves against both current and future forms of abuse.

2.2 We support the requirement to take the appropriate mitigation actions to stop or otherwise disrupt a registered domain name in .COM from being used for DNS Abuse. However, the BC believes the contract should also require specific measures to mitigate reported DNS Abuse:

- Improvement of response time frames to match the urgency of DNS threat vectors and better time to resolution of situations of abuse;
- Addressing child sexual abuse material (CSAM);
- An affirmative duty for registries to mitigate abuse;
- Documentation to reporter of steps taken against abuse; and
- Requiring WHOIS reveals when there is DNS abuse, particularly when abuse is occurring at scale.

2.3. Establishing Clear Outcomes: Halting DNS Abuse in .COM Domains

As part of the ongoing efforts to maintain a secure and trustworthy online environment, it is crucial to establish clear and measurable outcomes for halting DNS Abuse in .COM domains, particularly in light of the forthcoming renewal of the agreement between ICANN and Verisign. Effective combat against DNS Abuse requires a well-defined framework of actionable outcomes, which will not only enhance the integrity of the .COM domain space but also provide a roadmap for all stakeholders involved in the registration and management of domain names. The following target outcomes aim to protect businesses and consumers from harmful online activities:

a. Defined Takedown Procedures with Standardized Timeframes

The BC recognizes the importance of swift action in addressing DNS abuse across the .COM domain space. While registrars are primarily responsible for suspending abusive domains, we encourage Verisign to play a facilitating role in promoting standardized procedures and target timeframes—such as 24 or 48 hours—for the suspension of confirmed abusive domains. By fostering greater coordination with registrars and ICANN, Verisign can help ensure a more consistent and efficient approach to abuse mitigation.

b. Real-Time Reporting and Mitigation Mechanisms

The BC acknowledges Verisign's efforts to address DNS abuse in the .COM namespace. However, to stay ahead of evolving threats, we encourage Verisign to consider enhancing real-time coordination mechanisms. This approach would offer distinct advantages over the current registrar-managed solutions by fostering registry-level coordination that unifies the efforts of registrars, ICANN, and security experts.

While registrars handle abuse within their domains, Verisign's role as the registry operator allows for a broader view of abuse patterns across the entire .COM namespace. By enabling centralized real-time data sharing, Verisign could provide a platform for registrars and stakeholders to access unified threat intelligence, improving the collective ability to identify and mitigate large-scale threats. This mechanism would complement existing registrar tools by offering faster identification of abuse trends and enhanced collaboration on urgent incidents.

With a unified, real-time reporting system, registrars would benefit from Verisign's broader scope, allowing them to respond more swiftly to abuse

incidents. This solution builds upon and strengthens existing frameworks without duplicating them, ensuring that DNS abuse is addressed more effectively and comprehensively across the entire ecosystem.

c. Establishing Measurable Success Criteria

The BC underscores the importance of establishing clear, measurable success criteria for halting DNS abuse in .COM domains. Setting specific targets, such as the reduction of reported abuse incidents by a defined percentage over a specified timeframe, will create accountability and drive continuous improvement.

Moreover, it is crucial to regularly review these metrics to assess the effectiveness of the implemented measures and adjust strategies as necessary. By adopting a results-oriented approach, stakeholders can ensure that efforts to combat DNS abuse are not only effective but also adaptable to the evolving landscape of cyber threats. This commitment to measurable outcomes will reinforce the integrity of the .COM domain and foster greater trust among businesses and consumers.

d. Adherence to a standard Incident Response Plan (IRP)

We appreciate efforts by Verisign to develop best practices and educate the internet community regarding DNS abuse. We also encourage Verisign to enforce an Incident Response Plan that could be adopted across the .COM namespace. It is our belief that every DNS attack should be addressed in a consistent manner with sufficient attention. DNS abuse incidents, regardless of the damage they cause, should have root cause analysis, a structured approach to containment and recovery, and minimized damage and downtime.

3. Additional security obligations recommended by SSAC in SAC074

The BC supports the proposed security reporting obligations in the .COM RA and the amended LOI:

- An obligation for Verisign to disclose security incidents that may significantly jeopardize the Registry's systems. This new obligation is the result of work ICANN and Verisign undertook as part of Amendment 1 to the binding Letter of Intent between ICANN and Verisign.
- A commitment by Verisign to work with ICANN to determine the appropriate process for ICANN to publish statistics concerning security incident disclosures to ICANN based on the recommendations in SAC074.

4. Definitional limits on Security and Stability for Consensus policy purposes

Both the current and proposed .COM RA and Base RA treat "Security" and "Stability" as defined terms for purposes of operating the registry databases. But when describing Consensus Policy Development that is binding on all contractual parties, the Base RA uses the terms security and stability *without definitions*, which could allow more flexibility for the PDP process to develop consensus policies to address emerging threats.

In our Mar-2023 comments on .NET renewal, we said that using defined terms for Security and Stability might limit consensus policy obligations for the .NET registry operator. The BC requested that the .NET RA match the Base RA by using *undefined* security and stability terms for consensus policy purposes.

The BC was glad to see the .NET renewal RA updated to use "security" and "stability" for applicability of consensus policies. And we note approvingly that the proposed .COM RA does the same:

> "Consensus Policies shall relate to one or more of the following: (1) issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet or DNS." (p.3)

5. Cooperation With ICANN Economic Studies

In this request for Public Comment, ICANN stated that the renewal proposal *"incorporates important concepts from the Base RA, including both recent amendments to the Base gTLD Registry Agreement (Base RA), bringing these enhanced obligations to the largest TLD"*.[1]

However, one of the key features of the Base RA is inclusion at Section 2.15, of a provision requiring the registry to reasonably cooperate with an economic study if initiated or commissioned by ICANN.[2]

Given that one of the express purposes of the proposed renewal is to incorporate important concepts from the Base RA, we are concerned with this omission. Cooperation with any such

[1] See: https://www.icann.org/en/public-comment/proceeding/proposed-renewal-of-the-registry-agreement-for-com-26-09-2024

[2] See: https://www.icann.org/en/registry-agreements/base-agreement

economic study would be all the more crucial for the .COM registry given that it accounts for the overwhelming majority of domain name registrations overseen by ICANN. Any economic study missing .com registration data would be of substantially less utility and we therefore call upon ICANN to include a provision consistent with Section 2.15 of the Base RA in the proposed renewed Agreement.

6. Agreed Restrictions on domain prices and vertical integration

The Base RA does not impose price controls for domain names. However, the US Government (NTIA) and Verisign have a Cooperative Agreement that imposes price caps on .COM names. Amendment 35 to that Cooperative Agreement stated that "Verisign and ICANN may agree to amend Section 7.3(d)(i)(Maximum Price) of the .com Registry Agreement" to increase prices by 7% per year" for four out of every six years starting in 2020 for both new registrations and renewals.[3] In the proposed .COM RA, ICANN allows the maximum price permitted under the Cooperative Agreement, i.e. 7% "in the final four Pricing Years of every six year period" (p. 19 of redlined version).[4]

In our 2016 and 2019 comments on Proposed Amendments to Base New gTLD Registry Agreement, the BC said, "it is not ICANN's role to set and regulate prices". However, as we stated in our Mar-2023 comments on .NET renewal, the BC continues to support price caps that are willingly agreed to by Verisign and ICANN.

For this proposed renewal of .COM, the BC requests that ICANN explain and justify its decision to allow Verisign the maximum annual increase of 7% in years 3 through 6. We understand that the NTIA Cooperative Agreement allows a maximum of 7% annual increases in years 3 through 6, but we want to understand ICANN's rationale for adopting that maximum, instead of limiting Verisign to a lower percentage increase.

Regarding vertical integration, the BC continues to support restrictions agreed by Verisign and ICANN, even though such restrictions are not part of the Base RA:

> (c) Restrictions on Acquisition of Ownership or Controlling Interest in Registrar. Registry Operator shall not acquire, directly or indirectly, control of, or a greater than fifteen percent ownership interest in, any ICANN-accredited registrar for the TLD. (p.16)

[3] https://www.ntia.doc.gov/files/ntia/publications/amendment_35.pdf

[4] https://itp.cdn.icann.org/en/files/global-domains-division-gdd-operations/redline-of-the-proposed-and-2012-com-registry-agreement-as-amended-26-09-2024-en.pdf

7. Adoption of Thick WHOIS Consensus Policy

The adoption of the updated EU Directive on Network and Information Security Services in 2022 (NIS2) may have established the legal basis for the maintenance of a thick registry. NIS2, which now carries the effect of binding law, imposes obligations on registries that can be met through the maintenance of thick WHOIS records.

As a result, one of the impediments for implementing the Thick WHOIS consensus policy has been removed, and the BC recommends that the .COM agreement include commitments from Verisign to implement the Thick WHOIS policy by a specific date. No further work is needed by the ICANN Community for Verisign to implement Thick WHOIS in .COM, since the current policy as modified by the GNSO Council on Jan 21, 2021 states that:

> *The GNSO Council determines that the Recommendation #7 language, "must be transferred from registrar to registry provided an appropriate legal basis exists and data processing agreement is in place" should be included in the Registration Data Policy in order to conform with the intent of the EPDP Phase 1 Team's policy recommendation and the subsequent GNSO Council adoption.*

Moreover, the current registration data Consensus Policy requires data protection agreements between ICANN, the Registry, and Registrars:

> Data Protection Agreement
>
> ICANN, gTLD Registry Operators, and accredited Registrars MUST enter into required data protection agreements with each other and with relevant third party providers contemplated under this Policy where applicable law requires. The terms may include legal bases for processing Registration Data.
>
> Where such agreements between Registry Operator or Registrar and ICANN are required to comply with applicable law, ICANN MUST upon request and without undue delay, enter into data protection agreement or agreements with Registry Operator or Registrar as implemented pursuant to this Policy.
>
> If the Registry Operator or Registrar determines that such agreements are required by applicable law, it MUST make the request without undue delay pursuant to this policy.

The BC recommends that ICANN evaluate and determine whether NIS2 establishes "an appropriate legal basis" as called for in the consensus policy now in effect. If so, the BC requests that ICANN, the .COM registry operator, and .COM registrars quickly negotiate the "necessary data processing agreements" to enable Thick WHOIS in .COM "without undue delay pursuant to this policy."

The BC also recommends that the .COM agreement include commitments to adopt Thick WHOIS and negotiate data processing agreements to enable the transition to THICK WHOIS as soon as possible.

This comment was drafted by Steve DelBianco, Mason Cole, Zak Muscovitch, Alan Woods Asteway Negash, and Segunfunmi Olajide.

It was approved in accord with our charter