06 February 2024

RE: At-Large Advisory Committee Advice to ICANN Board on DNS Abuse
Copy: Sarah Deutsch and Jim Galvin, Co-Chairs Board DNS Abuse Caucus

To: Jonathan Zuck
Chair
At-Large Advisory Committee

Dear Jonathan,

I am writing to you regarding the At-Large Advisory Committee (ALAC) Advice to the ICANN Board on DNS Abuse, dated 24 December 2019. The Board would like to thank the ALAC for providing its constructive advice on mitigating DNS Abuse. I would also like to convey the Board's support for several statements expressed in the Advice document, which underscored that DNS Abuse "remains a key factor eroding confidence in a single, trusted, interoperable Internet," that "the status quo is insufficient," and that "suggesting ICANN does not have a role to play is factually incorrect and counterproductive."

The Board shares these concerns and wishes to highlight that it considers the issue of combating and mitigating DNS Abuse to be of strategic importance to ICANN. Indeed, ICANN's Strategic Plan for Fiscal Years (FY) 2021-2025, which feeds the Operating Initiatives in ICANN's annual operating plans, includes a specific strategic objective to "strengthen the security of the Domain Name System and the DNS Root Server System." To that end, ICANN has been strengthening DNS coordination in partnership with relevant stakeholders, as well as establishing and promoting a coordinated approach to effectively identify and mitigate DNS security threats and combat DNS Abuse.

ICANN's response to DNS Abuse has been and will remain multifaceted. ICANN org has consolidated its various efforts related to DNS security threats and DNS Abuse under a coordinated cross-functional program focused on the mitigation of DNS security threats. The program focuses on three pillars, namely: providing research, data, and expertise to help the community conduct fact-based discussions about the topic; providing resources that assist in raising levels of awareness and support in mitigating DNS security threats; and interpreting and enforcing the contractual obligations related

to DNS security threats and abuse generally in gTLD Registry Agreements, Registrar Accreditation Agreements, and ICANN consensus policies.

I would like to share highlights of several pieces of work related to combating and mitigating DNS Abuse that the org has initiated, advanced or deployed since the ALAC provided its written advice on this topic. These efforts are well-aligned with the spirit of the ALAC's Advice. These include:

- Contract amendments concerning DNS Abuse: The contracted parties voluntarily initiated contractual negotiations with ICANN and voted to add obligations to mitigate DNS Abuse in both the base gTLD Registry Agreement and Registrar Accreditation Agreement. As noted in my 22 May 2023 correspondence, these contract updates will aid ICANN's Contractual Compliance team in its enforcement efforts concerning registrars and registry operators who fail to adequately address DNS Abuse.

- Enhancement of ICANN DNS Security Threat Mitigation Program webpage: This webpage can be found at icann.org/dnsabuse and provides information about clearly denoted categories of harmful activity that are within ICANN's remit as defined by the ICANN Bylaws. The contents of the webpage are based upon the current working definition for DNS Abuse that ICANN utilizes in its contracts, projects, and documents. This webpage also features a section on "Enforcing Contractual Obligations with Registries and Registrars" that provides excerpts of all current abuse-related obligations in ICANN's contracts with the contracted parties, including procedures and protocols for responding to DNS Abuse.

- Publication of a DNS Abuse trends report in 2022: This report was based on four years of Domain Abuse Activity Reporting System (DAAR) data. ICANN org has also enrolled more than 20 Country Code Top Level Domains (ccTLDs) to voluntarily participate in DAAR and negotiated contract amendments with the gTLD registry operators that will enable ICANN to extend DAAR-like reporting to the registrar level.

- Creation of the Domain Name Security Threat Information Collection and Reporting (DNSTICR) tool: DNSTICR analyzed domain name registrations related to COVID-19 to identify credible evidence of malware or phishing and

notify the sponsoring registrars to assist in their DNS Abuse-related mitigation efforts.

These considerations have informed the Board's approach in its response to the eight Advice items outlined by the ALAC, which you can find in the attached scorecard ("Appendix A"). In summary, the Board accepts Advice item 1 as already fully implemented, accepts Advice item 2 subject to prioritization, and rejects Advice items 3, 4, 5, 6, 7, and 8. In Appendix A, ICANN Org provides an assessment and rationale for why items were not accepted.

The Board recognizes that the discussion and work on DNS Abuse has evolved and will continue to evolve over time. ICANN is committed to continue to work, within its remit, to combat and mitigate DNS Abuse. Reflecting this commitment, ICANN's interim President and CEO's FY 2024 Goals emphasize the need to "continue to enhance how ICANN combats DNS [A]buse across several dimensions, as it is a threat to Internet users' security and safety online."

The ICANN Board looks forward to and greatly appreciates the ALAC's continued collaboration on this important topic.

Sincerely,

Tripti Sinha,
Chair, ICANN Board of Directors

Itemized Board Action/Rationale to At-Large Advisory Committee (ALAC) Advice to the ICANN Board on DNS Abuse
22 January 2024

Advice Item # 1	Advice language: Establish a clear definition of DNS Abuse. The GNSO has already produced consensus definitions of "abuse" and "malicious use of domain names" that are more expansive. According to that definition, "abuse" is an action that: 1) Causes actual and substantial harm, or is a material predicate of such harm; and 2) Is illegal or illegitimate, or is otherwise considered contrary to the intention and design of a stated legitimate purpose, if such a purpose is disclosed. The GNSO also recognized that "malicious use of domain names" include, but are not limited to: 1) spam, 2) malware distribution, 3) online child sexual exploitation and imagery abuse, 4) phishing, 5) botnet command-and-control. ICANN should clarify the purposes and applications of "abuse" before further work is done to define DNS abuse. Once those purposes are identified, ICANN should determine whether abuse definitions used by outside sources can serve as references for the ICANN community, or whether a new, outcomes-based nomenclature could be useful (including impersonation, fraud, or other types of abuse) to accurately describe problems being addressed.

Board action/rationale: [Approved as fully implemented]

The Board acknowledges that DNS abuse[1] is a holistic issue that requires continuous evaluation by the wider ICANN community, including questions around the definitions and scope of DNS security threats that can be considered so long as they are within ICANN's remit.

[1] As used herein, "DNS abuse" with lower case "a" refers to a wider range of abuses within the DNS, some of which may not be within ICANN's remit (e.g. content-based abuse). "DNS Abuse" refers to a subset of abuses that comprise the defined term within the proposed DNS Abuse amendments to the RA and RAA, *to wit*, malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse listed).

The Board approves ALAC Advice item 1 as fully implemented. ALAC Advice item 1 identifies a need for a "clear definition of DNS Abuse." ICANN has developed a baseline definition of "DNS Abuse" as part of its broader efforts to mitigate DNS Abuse and, as such, this Advice is fully implemented.

The Board notes that ALAC Advice item 1 appears to contemplate a definition of "DNS Abuse" that is broader than the definition recently approved by generic top-level domain registries and accredited registrars for incorporation as amendments to the Registrar Accreditation Agreement (RAA) and Base gTLD Registry Agreement (RA). These amendments strengthen obligations on the contracted parties to mitigate DNS Abuse. For the purposes of the contract amendments, DNS Abuse means malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse, namely, malware, botnets, phishing, and pharming) as those terms are defined in Section 2.1 of the Security and Stability Advisory Committee Report on an Interoperable Approach to Addressing Abuse Handling in the DNS (SAC115). This initial definition of DNS Abuse is in line with the Advice's recommendation that "ICANN should clarify the purposes and applications of 'abuse' before further work is done to define DNS abuse." This new definition of DNS Abuse will set the stage for additional community efforts concerning this issue.

Notwithstanding the differences between the new DNS Abuse definition incorporated into the RAA and base RA and the broader view taken by the ALAC, the Board believes this step in amending the agreements implements the ALAC Advice Item 1. It is understood that, following the incorporation of the aforementioned amendments into contracts, the community may determine if policy work focused on evolving the current baseline definition of DNS Abuse would be beneficial, which could include considerations for a suitable approach pertaining to questions around definitions and scope. The Board welcomes further input and discussion with the ALAC on DNS Abuse in the best interests of the DNS community.

ICANN org assessment:

ALAC Advice item 1 proposes an approach to establish a clear definition of DNS Abuse, i.e. "ICANN should clarify the purposes and applications of 'abuse' before further work is done to define DNS Abuse. Once those purposes are identified, ICANN should determine whether abuse definitions used by outside sources can serve as references for the ICANN community, or whether a new, outcomes-based nomenclature could be

useful". The Advice item also asks ICANN org to consider as part of an expansive evaluation, i.e. "action that causes actual and substantial harm, or is a material predicate of such harm; and is illegal or illegitimate, or is otherwise considered contrary to the intention and design of a stated legitimate purpose, if such a purpose is disclosed."

Per ICANN org's evaluation, the suggested scope of this Advice item could include much more broadly defined forms of "abuse", which may go beyond ICANN's remit, as well as its visibility and competencies.

As highlighted in the ICANN blog posting dated 13 December 2023, the contracted parties voluntarily initiated contractual negotiations with ICANN and voted to add obligations to mitigate DNS Abuse in both the base gTLD Registry Agreement and Registrar Accreditation Agreement. A critical aspect of the contract amendment language is to strengthen existing abuse-related obligations and to arrive upon a definition of the forms of DNS Abuse that falls within ICANN's mandate.

For the purposes of the contract amendments, DNS Abuse means malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse, namely, malware, botnets, phishing, and pharming) as those terms are defined in Section 2.1 of the Security and Stability Advisory Committee Report on an Interoperable Approach to Addressing Abuse Handling in the DNS (SAC115).

It is understood that this definition is neither an exhaustive list nor a criteria-based definition, and one that might be subject to further development as the work and dialogue on DNS Abuse progress, subject to ICANN's remit. At the same time, the definition brings together a set of agreed-upon DNS Security Threats for which policy and mitigation work within ICANN can take place immediately, while or if definitions continue to be debated.

ICANN org notes that the community continues its discussions over DNS abuse mitigation, which include questions around the definitions and scope of DNS security threats that can be considered as within ICANN's remit. ICANN will continue to support such discussions in the years to come.

Advice Item # 2	Advice language: Cease rate limiting WHOIS (eventually RDAP) or simplify the process of whitelisting, so that it can report on the registration ecosystem. Adopt a uniform and timely access framework for publicly available registrant data.

Board action/rationale: [Approved subject to prioritization]

The Board notes that ALAC Advice item 2 overlaps with SAC 101v2 Advice 2A and 2B, which it has already considered and resolved on 23 June 2019.

Therefore, the Board approves this Advice item subject to prioritization with the understanding that no further action is required, other than for ICANN org to continue to provide regular updates as its evaluation of SAC101v2 Advice item 2B progresses.

ICANN org assessment:

ICANN org notes that ALAC Advice item 2 overlaps with SAC 101v2 Advice 2A and 2B which suggest that: “the ICANN Board should direct the ICANN Organization to work with the ICANN Community to: A) develop policy with clearly defined uniform purposes for RDDS rate-limiting and corresponding service level agreement requirements, and B) clarify current expectations for the use of rate limiting under existing policy and agreements.”

On 23 June 2019, the ICANN Board considered and resolved SAC101v2 Advice items 2A and 2B:

- The Board referred Advice item 2A to the GNSO Council for consideration for inclusion in the EPDP Phase 2 work.

  In its rationale the Board stated, "Advice item 2A suggests that the Board direct ICANN org to work with the community to 'develop policy with clearly defined uniform purposes for RDDS rate-limiting and corresponding service level agreement requirements.' As policy is developed by the community and this topic is in the work plan for the EPDP Phase 2, the Board notes this Advice and refers to the GNSO Council as the manager of PDPs. In taking this action, the Board also notes that in the Annex to the Temporary Specification for gTLD Registration Data, the Board asked that the topic of rate limiting be discussed and resolved by the community as quickly as possible."

As a result, implementation of this Advice item was not directed and this item is now formally closed.

- The Board accepted Advice item 2B in SAC101v2 relating to clarifying expectations for the use of rate-limiting under existing policy and agreements, and directs the ICANN President and CEO, or his designee(s), to work with the community to clarify existing contractual obligations relating to rate limits.

  Following completion of the Operational Design Phase (ODP) for the System for Standardized Access/Disclosure (SSAD) and subsequent work related to the Registration Data Request System (RDRS), ICANN org and the Board continue to consider this advice.

Advice Item # 3	Advice language: Direct ICANN Org to establish low thresholds for identifying bad actors. Direct ICANN Org to publish more actionable Domain Abuse Activity Reporting (DAAR) data: identifying the operators with high concentrations of abuse against whom onward action ought to be contemplated. There are a number of metrics that DAAR already offers. One is "cumulative count of abuse domains over 365 days". Data is available showing which registries and registrars exhibit "register, use, discard, repeat" - which is the same behavior that criminals use with burner mobile phones. The phone is used once and then it is abandoned. The domain is used for a single campaign or attack, and then it is abandoned. Basically, all the data counted per registry, per registrar, can be used to formulate many metrics.

Board rationale/action: [Rejected]

ALAC Advice item 3 envisions that ICANN establish specific thresholds of abuse, which when met and surpassed would trigger “onward action” from Contractual Compliance. However, the Board notes that ICANN Contractual Compliance’s role is to bring contracted parties into compliance with their ICANN contractual obligations, regardless of whether or not a specific complaint threshold has been triggered.

The Board supports the recent work by ICANN org and Contracted Parties to enhance the existing obligations related to DNS Abuse via contract amendments, and agrees with the Org that these will create a new standard of behavior that ICANN org can use to hold contracted parties accountable to, in line with the spirit of this Advice item.

The Board also concurs with ICANN org's assessment that careful consideration is required to distinguish between reported cases of DNS Abuse and evidenced cases of DNS Abuse, and that engagement with the community could be helpful in designing a procedure that supports positive outcomes. For those reasons, ALAC Advice item 3 is rejected.

The Board encourages ICANN org to continue in its efforts to report security threat activity to the ICANN community and continue the dialogue with the contracted parties to support their actions in combating DNS Abuse, which may include further improving its DNS Abuse analysis and reporting efforts, as intended by this Advice item.

ICANN org assessment:

ALAC Advice item 3, which overlaps with Competition, Consumer Trust, and Consumer Choice (CCT) Recommendation 15, envisions that ICANN establish a low threshold of abuse, which when met would trigger "onward action" from Contractual Compliance. Setting such generalized abuse thresholds on registries and registrars implies that compliance inquiries will be triggered by the volume of possible abuses rather than their severity and context, which is the principle at the core of any action in this area.

ICANN Contractual Compliance's role is to bring registry operators and registrars into compliance with their ICANN contractual obligations regardless of whether or not a specific complaint threshold has been triggered. The recent work conducted by ICANN and the Contracted Parties to advance amendments in the RAA and RA related to combating DNS Abuse will provide ICANN's Contractual Compliance with appropriate remit to hold registrars and registrars accountable for enhanced obligations to take appropriate mitigation actions against well-evidenced DNS Abuse.

ICANN org also notes that domain names and volumes that appear as suspected cases of broader DNS abuse are not necessarily equivalent to those that are confirmed and evidenced.

When it comes to the possible publication of reports that identify registries and registrars as “bad actors”, careful consideration must be given to distinguish between reported cases of broader DNS abuse which might be sourced via Reputation Block List (RBL) feeds or via complaints provided to ICANN Compliance, and evidenced cases of DNS Abuse which would result from investigations by contracted parties or Law Enforcement and Investigations (LEI) agencies. It is worth noting that ICANN org does not have full visibility of all evidenced DNS Abuse cases. Furthermore, before publishing reports that identify registries and registrars it could be helpful for ICANN org to engage in a dialogue with the community to design a procedure that supports positive outcomes.

The Domain Abuse Activity Reporting (DAAR) project measures reported concentrations of security threat (DNS Abuse) reports in domain names within the gTLD space in an aggregated and anonymous manner, and provides coverage of those ccTLDs that have voluntarily joined the project. In a 5 May 2021 blog posting, ICANN org outlined current and planned evolution of the DAAR project based on the input received which includes project documentation, report coverage and data visualization, among others. The methodology at the core of the DAAR project has been developed, peer reviewed, and previously made available for public review and comment in order to address specific goals pertaining to the reporting of security threat concentrations to the ICANN community.

Enhancing the transparency and accountability of any DNS Abuse analysis and reporting, as intended by ALAC Advice item 3, remains a key objective for ICANN org. Research is ongoing within ICANN org on possible ways of further increasing transparency around DNS Abuse-related data within ICANN’s remit to guide the future evolution of the DAAR project.

Advice Item # 4	Advice language: Provide an explicit mandate to ICANN Contractual Compliance to regularly use the audit function to root out “systemic” abuse; not to regulate content, but to proactively exercise enforceability.

Board rationale/action: [Rejected]

The Board concurs with ICANN org’s assessment that multiple tools and approaches are necessary to holistically respond to DNS Abuse, while remaining within the

constraints of ICANN's Bylaws, the contractual obligations set forth in ICANN's policies and agreements, including the Registry Agreement (RA) and the Registrar Accreditation Agreement (RAA), and local law and regulatory requirements.

The Board is not opposed to Contractual Compliance audits in the area of DNS Abuse, however disagrees that audits, irrespective of whether they are conducted with greater frequency and targeted to a wider sample of Contracted Parties, will be an effective standalone mechanism to root out broader DNS abuse and proactively exercise enforcement of the RA and RAA.

A multi-faceted approach should be employed in this regard, and the Board emphasizes that Compliance's objectives must equally include and efficiently address third-party complaints, proactive enforcement of contractual obligations, and registry and registrar audits against their contractual obligations. As a result, the Board rejects ALAC Advice item 4.

ICANN org Assessment:

ALAC Advice item 4 highlights the specific opportunity to "regularly use the audit function to root out systemic abuse" by proactively exercising enforceability of contractual provisions.

While ICANN org has conducted audits specifically focused on existing anti-abuse provisions, ICANN org believes that the premise of a time-defined audit, i.e. having a predefined start and end date, aimed at a subset of contracted parties is insufficient as a tool to root out broader DNS abuse (including undefined 'systemic' abuse) through proactive enforcement. Furthermore, such an approach is inconsistent with the overall function of the audit program to "enhance community transparency through fact based and measurable reporting while proactively addressing any potential deficiencies".

ICANN org believes it is necessary to complement any regularly implemented audit program with a thorough investigation of identified cases of alleged violations of applicable ICANN consensus policies pertaining to DNS Abuse, and pursuit of enforcement actions against any non-compliant contracted parties, as appropriate.

It is also worth noting that ICANN Compliance robustly addresses abuse complaints. Over the duration of calendar years 2021 and 2022, for instance, ICANN Compliance

received and evaluated more than 7,500 abuse complaints. During the same time period, ICANN Compliance issued 13 breach notices to registrars, which included notices either for failures to publish on the relevant registrar's website an email address to receive abuse reports, a description of the registrar's procedures for the receipt, handling and tracking of abuse reports, or both.

As highlighted in the ICANN blog posting dated 13 December 2023, the contracted parties voluntarily initiated contractual negotiations with ICANN and voted to add obligations to mitigate DNS Abuse in both the base gTLD Registry Agreement and Registrar Accreditation Agreement. ICANN Compliance will enforce these obligations against contracted parties' failures to mitigate and disrupt DNS Abuse.

Advice Item # 5	Advice language: Do not process registrations with "third party" payments, unless they have been approved prior to the request. Much of the POC data regarding mainly "persons" and fewer "organizations" was falsely composed. Organizations (any registrar that is not a natural person), should only accept payment methods authorized by the registrant organization. Organizations would benefit by having the ability to impose a single payment method and a focused anti-fraud measures program.

Board rationale/action: [Rejected]

The Board is committed to ICANN org's enforcement of all contractual obligations.

The requirement within the 2013 RAA to ensure reasonable assurance of payment prior to activation does not restrict accredited registrars from implementing more stringent payment restrictions, such as those outlined in this Advice item regarding third-party payments.

However, recognizing that the Advice item requires changes to contractual obligations and considering both the lack of clarity on the scale of the issue and value of mandating that all accredited registrars implement such a restriction, the Board rejects this Advice item.

The community may determine, as appropriate, if policy work would be beneficial to further combat DNS Abuse, and the extent to which preventative measures such as those outlined in this advice should feature in future ICANN policy.

ICANN org assessment:

ICANN org understands ALAC to advise for the prohibition of ICANN accredited registrars from processing registrations where the payor is, or the method of payment belongs to,
an individual or entity other than the registrant, unless such payment methods have been
approved in advance of registration. The Advice item suggests that such a prohibition would be beneficial to registrar organizations "by having the ability to impose a single payment method and a focused anti-fraud measures program".

ICANN org notes an existing requirement within the 2013 RAA (Section 3.7.4), mandating that "registrars shall not activate any registered name unless and until it is satisfied that it has received a reasonable assurance of payment of its registration fee". The envisioned incremental restriction regarding third-party payments, which represents one of many possible edge cases operationally, is not expressly forbidden under the current contract language should any registrars wish to voluntarily implement this.

It is also worth noting that this advice calls for changes to the RAA relating to the pre-approval of acceptable payment methods, which in some cases may be a matter of commercial law in the jurisdictions that ICANN accredited registrars operate.

Lastly, no supporting data has been shared with ICANN org indicating the scale of the issue, nor the desirability of its envisioned benefits. As such, it would be presumptive for ICANN org to specifically mandate such a restriction before the community has had a chance to further discuss these topics.

Advice Item # 6	Advice language: Adopt an "anti-crime, anti-abuse" Acceptable Use Policy (AUP) and include enforcement.

Board rationale/action: [Rejected]

The Board supports a number of observations by ICANN org that support rejection of this Advice item, i.e. that ICANN has contracted parties numbering in the thousands that are dispersed geographically and thus subject to a wide variety of international, national, and local legal obligations; and that contracted parties face a lack of consistency in the definition of the regulatory framework as to what constitutes "illegal and/or criminal conduct" pertaining to the use of the DNS.

Further, this Advice item's language encompasses a much broader, undefined concept of "abuse" as compared to DNS Abuse, which could go beyond ICANN's remit, visibility, and competencies, and thus complicates the Advice item's intent of formulating a wholesale "anti-crime, anti-abuse" Acceptable Use Policy (AUP). While contracted parties may choose to voluntarily employ a broader definition as to what constitutes abusive, malicious, or illegal conduct in the registration of domain names, and for as long as these are compliant with ICANN's contracts, ICANN has neither the authority to mandate nor to enforce the incorporation of provisions extending beyond its remit.

Setting aside the noted limitations relating to both scope and scale which leads the Board to reject ALAC Advice item 6, the Board welcomes further input and discussion on this topic. Following the incorporation into contracts of amendments that add obligations to mitigate DNS Abuse, the community may determine if the adoption of standardized AUP language, for as long as these are strictly within ICANN's remit, might be beneficial additions to future ICANN policy.

ICANN org assessment:

ALAC Advice item 6 calls for ICANN org to "adopt an anti-crime, anti-abuse Acceptable Use Policy (AUP) and include enforcement", asserting that "the vague language in the existing contracts that require only that the parties 'have a policy' is obviously insufficient in some cases". ICANN org remains fully supportive of any community work to enhance DNS Abuse safeguards, however, recommends the Board reject this Advice item based on the following considerations:

First, any "anti-crime, anti-abuse" AUP must conform with the wide variety of international, national, and local legal obligations to which gTLD registry operators and registrars are subject. Considering ICANN's current contracted party base is composed of more than 1,400 distinct gTLD registry operators and registrars operating across a minimum of 84 countries, attempting to put forth a wholesale "anti-crime, anti-abuse"

AUP would be complicated by a lack of consistency in the definition of the regulatory framework across countries as to what constitutes “illegal and/or criminal conduct” pertaining to the use of the DNS.

Second, as is also noted in ICANN org’s evaluation of ALAC Advice item 1, this Advice item suggests adopting an AUP with a much broader, undefined concept of “abuse”, as compared to DNS Abuse, which could go beyond ICANN’s remit, visibility, and competencies. While ICANN org is aware that contracted parties often do utilize AUPs with broad-based specifications as to what constitutes abusive, malicious, or illegal conduct in the registration of domain names and which are compliant with their ICANN contracts, ICANN has neither the authority to mandate nor to enforce the incorporation of provisions extending beyond ICANN’s remit.

Lastly, as a multi-jurisdictional organization and with an understanding that the definition of crime is not consistent across jurisdictions, ICANN’s contracts clearly advocate that contracted parties develop policies that abide by applicable laws and regulatory requirements. Examples of these are outlined in: Section 3.7.2 of the 2013 RAA covering Business Dealings, Including with Registered Name Holders, which states that “Registrar[s] shall abide by applicable laws and governmental regulations.”, and Specification 11.3A of the base gTLD registry agreement covering Public Interest Commitments, which states “Registry Operator[s] will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.”

Advice Item # 7	Advice language: Compel industry-wide good behavior: for eg. by increasing per domain transaction fees for registrars that continually demonstrate high abuse rates.

Board rationale/action: [Rejected]

The Board believes that continuous education developed at registry, registrar and registrant levels, as well as constructive dialogue and enhanced cooperation with all the interested parties, will be key components in the fight against DNS Abuse.

The Board agrees with ICANN org's assessment that linking a financial incentive/penalty to 'high abuse rate' thresholds would place undue focus on the volume of possible abuse cases rather than their severity and context, which is the principle at the core of actions in this area. In its 10 September 2023 resolution, the Board underscored in its rationale to the CCT Recommendation item 15 that "ICANN Contractual Compliance's role is to bring registrars into compliance with the Registrar Accreditation Agreement (RAA) regardless of whether or not a specific 'complaint threshold' has been reached."

The Board also concurs that careful consideration is required to distinguish between reported cases and evidenced cases of DNS Abuse. The ability to collect independently verifiable metrics demarcating evidenced cases of DNS Abuse should be a critical aspect for implementing this Advice item, and it must be noted that ICANN org does not have full visibility of all evidenced DNS Abuse cases.

Furthermore, the Board supports the work by ICANN org and Contracted Parties that enhanced the existing obligations related to DNS Abuse via contract amendments, and believes that these will create a new standard of behavior that ICANN org can hold contracted parties accountable to, in line with the spirit of this Advice item. The Board encourages the Org and community to continue consideration of additional ways to combat DNS Abuse.

Ultimately, the Board believes that there are other ways to ensure a healthy DNS environment rather than increasing registration fees for registrars that may have high abuse rates, and rejects this Advice item.

ICANN org assessment:

ALAC Advice item 7 directs ICANN org to compel Contracted Parties to adhere to industry-wide good behavior, for example, by increasing per-domain transaction fees for registrars that continually demonstrate high abuse rates. Implementation of this Advice item would cause ICANN org to enter into voluntary negotiations with Contracted Parties regarding pricing and industry best practices.

ICANN org notes that ALAC Advice item 7 complements ALAC Advice item 3 and the CCT Recommendation 15, all of which suggest the creation of generalized abuse thresholds and triggering specific actions (i.e. “onward action” from Contractual Compliance or presumption of contracted parties to be in default of their agreement in the case of ALAC Advice item 3 and CCT Recommendation 15, respectively, or seeking higher per-domain transaction fees in the case of ALAC Advice item 7) based on the volume of possible abuses rather than their severity and context, which is the principle at the core of actions in this area.

ICANN org also notes that the feasibility of implementing this Advice item is complicated by the fact that domain names and volumes that appear as suspected cases of broader DNS abuse are not necessarily equivalent to those that are confirmed and evidenced. It is worth reiterating that ICANN org does not have full visibility of all evidenced DNS Abuse cases.

Furthermore, this Advice item calls for changes to contracted party agreements. In the recently concluded contract amendment process with the gTLD Registries and Registrars to add a clearly defined obligation to mitigate or disrupt DNS Abuse in each agreement, the Contracted Parties proposed and ICANN agreed to keep the scope purposefully focused on mitigation obligations, and to only subsequently engage in wider community discussions, including possible policy development regarding additional obligations. Therefore, it would be procedurally and substantively out of scope for ICANN org to attempt to design and add anti-abuse incentives before the community has had a chance to consider what concrete behaviors or outcomes should be incentivized.

ICANN org will continue to remain vigilant on possible actions that might be introduced to support any contracted party in their fight against DNS Abuse.

Advice Item # 8	Advice language: Implement the above (Advice items) in agreements/contracts, with clear enforcement language for ICANN Contractual Compliance to adopt. Convene a discussion between the Contracted Parties and ICANN Compliance to finally resolve what additional tools might be needed by Compliance

Board action/rationale: [Rejected]

The Board has provided its comprehensive response and rationale for proposed actions to each of the items noted in the ALAC Advice on DNS Abuse. As a number of Advice items are being rejected, Advice item 8, which assumes the implementation of all other Advice items within contracted party agreements, is also necessarily being rejected.

Furthermore, the Board reiterates the Registry Stakeholder Group's views, as expressed in the public comment on the SSR2 Final Report, that any recommendations (or advice items) related to ICANN Contractual Compliance should be connected to specific contractual terms and tied to a specific problem statement.

The Board supports the recent work by ICANN org and Contracted Parties that enhanced the obligations related to DNS Abuse via contract amendments, and believes that these will create a new standard of behavior to which ICANN org can hold contracted parties accountable. Following the incorporation of these amendments into contracts, the community may determine, as appropriate, if policy work would be beneficial to further combat DNS Abuse. ICANN Contractual Compliance enforces the contractual obligations set forth in ICANN's policies and agreements, and further progress in the community's work to enhance DNS Abuse safeguards will support ICANN Compliance's efforts to enforce obligations against contracted parties' failures to mitigate and disrupt DNS Abuse.

ICANN org assessment:
ICANN org understands ALAC to advise the ICANN Board to direct ICANN org to enter into voluntary contract negotiations with Contracted Parties to implement the above advice items, and to include clear enforcement language to facilitate ICANN Contractual Compliance to enforce these. ICANN org further understands ALAC to advise the ICANN Board to direct ICANN org to ensure that ICANN Contractual Compliance has the tools it will need to enforce the output of any relevant Consensus Policy and/or voluntary contract negotiations.

ICANN org has evaluated and provided a response on the feasibility of implementing each of the items noted in the ALAC Advice on DNS Abuse, leading to a recommendation to reject several among these. Accordingly, Advice item 8 which assumes the acceptance of all prior items, must necessarily be rejected.

ICANN's response to DNS Abuse reflects the need to address abuse within the constraints of ICANN's Bylaws and policies as defined by the ICANN community, and by obeying local law and regulatory requirements. ICANN Contractual Compliance has the ability to enforce the output of any relevant Consensus Policy and/or voluntary contract negotiations.

ICANN org notes that the community continues its discussions over DNS Abuse mitigation. ICANN will continue to support such discussions in the years to come and ICANN Contractual Compliance will continue to enforce the output of any resulting Consensus Policy and/or outcomes of voluntary contract negotiations.