Public Comment Summary Report

Amendments to the Base gTLD RA and RAA to Modify DNS Abuse Contract Obligations

Open for Submissions Date:
Monday, 29 May 2023

Closed for Submissions Date:
Thursday, 20 July 2023 (Extended from Thursday, 13 July 2023)

Summary Report Due Date:
Thursday, 31 August 2023 (Extended from Tuesday, 1 August 2023)

Category:
Other

Requester:
ICANN organization (org)

ICANN org Contact(s):
globalsupport@icann.org

Open Proceeding Link:
https://www.icann.org/en/public-comment/proceeding/amendments-base-gtld-ra-raa-modify-dns-abuse-contract-obligations-29-05-2023

Outcome:
This Public Comment proceeding was initially scheduled to remain open from 29 May 2023 through 13 July 2023. The Public Comment proceeding was extended by one week in response to requests for additional time to submit input. ICANN org received thirty-six (36) comments on the proposed amendments to the base generic top-level domain (gTLD) Registry Agreement (Base RA) and the 2013 Registrar Accreditation Agreement (RAA) from groups, organizations, and individuals.

Comments provided general support for the proposed amendments with some offering feedback for ICANN org to consider including in the draft ICANN Advisory and/or the proposed amendments. ICANN org reviewed the feedback and consulted with the Contracted Parties House Negotiating Team (CPH NT). Following the consultation between ICANN org and the CPH NT, the comments confirmed that the proposed amendments met their stated objective of enhancing obligations by requiring registrars and registry operators to promptly take reasonable and appropriate action to stop or otherwise disrupt Domain Name System (DNS) Abuse.

ICANN org appreciates the participation in this proceeding and is grateful to those who provided their feedback.

Section 1: What We Received Input On

ICANN org and members of the CPH NT sought input from the ICANN community on the proposed amendments to the RAA and Base RA, collectively, the "Agreements."

The proposed amendments would enhance obligations by requiring registrars and registry operators to promptly take reasonable and appropriate action to stop or otherwise disrupt DNS Abuse. For the purposes of the proposed 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).

ICANN org and the CPH NT sought input from the ICANN community on the proposed amendments which strengthen the existing provisions in Section 3.18 of the RAA and Specification 6, Section 4 of the Base RA by adding DNS Abuse mitigation and disruption obligations. The proposed revisions include the following:

- Requirements to ensure abuse contacts are readily accessible on the contracted party's (CP) webpage and to produce receipt confirmation for reporters upon receipt of abuse reports
- Possibility for registrars and registry operators to use webforms instead of email as an abuse reporting mechanism
- A definition of DNS Abuse for purposes of the Agreements
- A new requirement to promptly take appropriate mitigation actions against domains for which the CP has actionable evidence demonstrating that the domains are being used for DNS Abuse
- Permission for CPs to exercise reasonable discretion in selecting and implementing the appropriate mitigation actions depending on the circumstances of each case
- Recognition of the different roles of the registrar and registry operator
- A target outcome of stopping or disrupting the use of gTLD domain names for DNS Abuse

In addition, the proposed amendment to the Base RA includes a revision to Section 11.3 (b) to replace the term security threats with DNS Abuse. This clarifies that registry operators must periodically conduct a technical analysis to assess whether gTLD domains are being used to perpetrate DNS Abuse and maintain statistical reports on identified DNS Abuse. A positive benefit of this change is to expand the requirement for registries to include spam as a delivery mechanism for other forms of DNS Abuse as something to include in their periodic analyses and reports.

The proposed amendments do not specify the mitigation actions, or their timing, as such approach may not guarantee the desired outcome in all instances. The negotiation teams discussed a more prescriptive approach but ultimately decided such an approach may unintentionally result in undesirable disproportionate outcomes where DNS Abuse involves compromised domain names or could result in delayed responses in situations where swift action is required. The appropriateness and promptness of the actions will depend on the specific circumstances of each case. The amendments are intended to result in prompt and reasonable mitigation actions that minimize the scope and intensity of the harm and

victimization caused by DNS Abuse while limiting collateral damage caused by CP's actions in response to the DNS Abuse. The proposed amendments contemplate that the best-equipped parties to conduct a thorough review of the matter and take the appropriate, proportionate mitigation actions may vary depending on the circumstances.

For more information, please read the draft ICANN Advisory that would come into effect if the proposed amendments are approved. The draft Advisory further explains the new requirements, provides guidance, and sets out expectations for action by CPs to establish compliance. The draft Advisory also elaborates upon terms like "mitigation actions," "appropriate," "stop" (contributing to stopping), and "disrupt" (contributing to disruption). Additionally, the draft Advisory contains examples of DNS Abuse, actionable evidence, and corresponding appropriate and prompt mitigation actions, considering the circumstances of each case.

Section 2: Submissions

Organizations and Groups:

Name	Submitted by	Initials
Governmental Advisory Committee	Fabien Betremieux	GAC
iQ Global AS (iQ)	Steinar Grøtterød	iQ
Non-Commercial Stakeholder Group	Mesumbe Tomslin Samme-Nlar	NCSG
Internet Infrastructure Coalition	i2Coalition Staff	i2C
Tucows	Sarah Wyld	
Registries Stakeholder Group	RySG	RySG
Association française pour le nommage Internet en coopération	Lucien Castex	AFNIC
The Messaging, Malware and Mobile Anti-Abuse Working Group	Amy Cadagin	M3AAWG
Japan Publisher's Manga Anti-Piracy Conference	Tatsuo Ninoseki	JPMAC
Amazon	Gregory DiBiase	
Registrar Stakeholder Group	Zoe Bonython	RrSG
Nominet UK	Nick Wenban-Smith	
TLD Registry Limited OY	Steinar Grøtterød	
Internet and Jurisdiction Policy Network	Bertrand De La Chapelle	
Brazilian Association of Software Companies (ABES), AR-TARC, Governance Primer	Brazilian Association of Software Companies (ABES), AR-TARC, Governance Primer	
Security and Stability Advisory Committee	SSAC Staff	SSAC
Forum of Incident Response and Security Teams	Peter Lowe	FIRST
Namecheap, Inc.	Owen Smigelski	
At-Large Advisory Committee	ALAC Policy staff	ALAC
Safer Internet Association	Yuichi Moritomo	SIA
Technology Verification Team, Working-Level Forum for Anti-Piracy of Japan	George Shishido	
African Regional At-Large Organization (AFRALO)	Julius Kirimi	AFRALO
eco – Association of the Internet Industry	Lars Steffen	ECO
DNS Abuse Institute	Graeme Bunton	DNSAI
Cross-Community Working Party on ICANN and Human Rights	Ephraim Percy Kenyanito	CCWP-HR
ICANN Business Constituency	Business Constituency	BC
International Trademark Association	Lori Schulman	INTA
Intellectual Property Constituency	Brian King	IPC

Individuals:

Name	Affiliation (if provided)	Initials

Jeffrey Bedser	CleanDNS Inc	JB
YUKI HIRAI	Interested Lawyers	YH
Prince Andrew Livingstone Zutah		PZ
James Olorundare	Civil Organization, User, Non-Commercial User, Researcher, End User	JO
Matthias Pfeifer		MP
MD IMRAN HOSSEN		MIH
KEN AKAMATSU		KA
Nobuhisa Nishigata	Ministry of Internal Affairs and Communications of Japan	NN

Section 3: Summary of Submissions

ICANN org thanks all the contributors for their valuable input and feedback to the proposed DNS Abuse amendments. All comments have been thoroughly reviewed, discussed with the CPH NT, and a categorized summary of the comments received is provided below.

1. The definition of DNS Abuse in the proposed amendments and ICANN's remit

Internet and Jurisdiction Policy Network, Association française pour le nommage Internet en coopération (AFNIC), Tucows, i2Coalition, CleanDNS, Brazilian Association of Software Companies (ABES), DNS Abuse Institute (DNSAI), eco association and topDNS (ECO) submitted comments which support the addition of the definition of DNS Abuse and clarified scope. These organizations and the Governmental Advisory Committee (GAC) support the terminology that is used in the definition which focuses on forms of abuse within ICANN's remit. The Registrar Stakeholder Group (RrSG) commented that the definition will assist CPs and those reporting abuse in clearly delimiting the scope of these new contractual obligations, enhancing predictability regarding types of DNS Abuse that can be addressed by the ICANN community. Safer Internet Association (SIA) supports the proposed amendments and explains that it is very important to encourage registries and registrars, which play an important role in the use of the Internet, to fulfill their responsibilities.

The DNSAI, ECO, CleanDNS, and Cross-Community Working Party on ICANN and Human Rights (CCWP-HR) expressed support noting that the proposed amendments remain within ICANN's bylaws and remit by excluding website content related abuse issues. Specifically, the CCWP-HR explained that the only modification that should be made to Specification 11 of the Base RA should be the inclusion of a disclaimer: "ICANN will not encourage Contracted Parties to broadly interpret its obligations to include items beyond ICANN's mandate, such as content or any other issues beyond the scope of ICANN Bylaws."

Conversely, the SIA, International Trademark Association (INTA), Technology Verification Team, Working-Level Forum for Anti-Piracy of Japan, MIC-Japan, Intellectual Property Constituency (IPC), Japan Publisher's Manga Anti-Piracy Conference (JPMAC), ICANN Business Constituency (BC), and individual commenters want the definition of DNS Abuse in the proposed amendments to be expanded to include illegal activities such as: internet piracy, copyright infringement, cybersquatting, typosquatting, trademark infringement, child sexual abuse material (CSAM), counterfeiting, domain hopping, domain spoofing, illegal content distribution, one-click scams, lottery scams, and e-commerce, and fraud. The ICANN Business

Constituency (BC) explains that over the long term the definition of DNS Abuse included in the proposed amendments is insufficient since the definition does not include other well-known forms of damaging behavior. The BC explains that this definition should not remain static and must be subject to periodic community review. The BC suggests a regular independent review of the definition of DNS Abuse, with an eye toward incorporating reasonably anticipated changes in sources of abuse. JPMAC, the GAC, CCWP-HR and individuals submitted comments regarding registrants right to due process, requiring registries or registrars to proactively disclose the policies that govern their relationships with registrants and be accountable to registrants when making any and all decisions that impact them.

The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) likewise offered that the definition of what constitutes DNS Abuse is constantly in flux. Therefore, the M3AAWG believes this aspect of the contract must be reviewed and updated regularly by a diverse group of experts. M3AAWG states this would provide pragmatic clarity while also avoiding the risk of being locked into outdated definitions or incomplete lists of individually relevant, illicit activities.

The SSAC clarified that Section 2.1 of SAC115 does not fully contain SSAC's definitions of abuse, and the proposed contract definitions of abuse are not endorsed by SSAC. SAC115 Section 2.1 quoted, for discussion and illustration purposes, definitions from the Contracted Parties' DNS Abuse Framework and the Internet and Jurisdiction Policy Network's "Operational Approaches, Norms, Criteria, Mechanisms" document. SAC115 stated a qualification about those definitions:

"To be clear there are additional abuses that are worthy of discussion. SSAC finds some of the specific definitions [in section 2.1] limited, and the above do not provide a general definition of abuse that may accommodate the evolving natures of abuse and cybercrime over time." Additionally, the SSAC explained that SAC115 Section 2.1 states that spam is "unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content."

The new contractual language therefore could be interpreted to define spam in two different ways and could thus be confusing.

The Non-Commercial Stakeholder Group (NCSG), M3AAWG, and individual commenters are generally not supportive of the proposed amendments and believe they are insufficient to address the challenge of DNS Abuse. The NCSG and Cross-Community Working Party on ICANN and Human Rights (CCWP-HR) believes "DNS abuse" is an ambiguous term and should not replace "security threat" and are concerned with the direction that ICANN and the CPs are going in doing bilateral negotiations to resolve complex and complicated policy issues.

ICANN org and the CPH NT acknowledge the time and dedication that the IPC and BC took to provide redlines to the proposed amendments and draft Advisory. ICANN org is also grateful to those who provided suggested language to the amendments which was valuable feedback for our consideration.

2. Provide additional clarity related to the terminology used in the proposed amendments

Comments submitted by individuals, i2Coalition, CleanDNS, At-Large Advisory Committee (ALAC), JPMAC, Amazon, eco association all are very supportive of the addition of obligations

for CPs to promptly take appropriate mitigation actions against domains involved in DNS Abuse. Many expressed support that this is generally considered a positive step to protect users and maintain the integrity of the Internet ecosystem. Also, many commented that they support that the proposed amendments acknowledge that appropriate action may vary depending on the severity of the harm and potential collateral damage.

ICANN org also received comments submitted by M3AAWG, the GAC, and INTA that terms used in the proposed amendments should be further defined, such as: “actionable evidence”, “appropriate mitigation action(s)”, “appropriate,” “prompt,” “respond appropriately to any reports of abuse."

3. How to address systemic abuse

M3AAWG, ABES, BC, INTA, and IPC commented that the proposed amendments should include reference to when there is actionable evidence that the domain name “was used” for DNS Abuse to allow for greater ability to stop systematic abuse. Additionally, comments received called for enforcement against registrars and registries that intentionally harbor abuse with truly out of the curve, unacceptably high, rates of malicious domain name registrations. Furthermore, comments stated to proactively prevent abuse by mitigating abuse at the “party” or “account” level, with the capability of addressing broad swaths of abuse at one time.

4. Abuse report handling

Individuals, Internet and Jurisdiction Policy Network, Tucows, i2Coalition, CleanDNS, ABES, DNSAI, eco association and topDNS support requiring accessible abuse contacts and offering webforms for reporting. Many of these individuals and organizations stated that webforms will streamline the process and improve response times. The RrSG commented that the authorization for registrars to collect reports of abuse through a webform will help registrars process abuse reports faster and more efficiently. The RrSG further explained that webforms can ensure that all reports are properly evidenced and are provided in a standardized format; webforms also help protect registrar abuse queues against spam. Amazon also is supportive of the amendments providing CPs with additional flexibility in how they ingest and process abuse reports, allowing for greater efficiency in mitigating abuse.

Additionally, individuals, Internet and Jurisdiction Policy Network, and AFNIC were grateful to see that confirmation of receipt were added to the proposed amendments.

M3AAWG, iQ Global AS (iQ), BC, the International Trademark Association (INTA), and IPC commented that webforms should adhere to reasonable standards for word/character limits or size limits, the ability to provide attachments in a variety of common formats (like .jpeg and .pdf), include a ticketing number in combination with the reported domain name(s) in the subject field, and send a confirmation of the form submission that includes the content of the report by email to the submitter.

TLD Registry Limited OY and iQ commented that there should be obligations on the registrar to forward received abuse reports to the “best-positioned” entity for DNS Abuse mitigation. M3AAWG, BC, INTA, and IPCR expressed that the Base RA should require the registry to take mitigation action if after referring an abuse report to the registrar, the registrar fails to adequately act to mitigate the reported abuse.

M3AAWG, Brazilian Association of Software Companies, BC, INTA, IPC expressed that service-level agreements guarantee timely reactions to abusive behavior (e.g., within 48 hours of receipt

of a credible DNS Abuse report; no more than two business days to confirm receipt of reports, and no more than 10 calendar days to respond substantively to non-LEA reports).

BC, INTA, IPC commented that CPs should be required to clearly document to the abuse reporter the specific steps taken (or in some instances, not taken) to address reported abuse. If determined no action is appropriate in a particular case, CPs should have an obligation to report this to the abuse reporter and identify what other options the reporter has for addressing the reported abuse.

5. ICANN Contractual Compliance enforcement of the obligations

The GAC, INTA, and ALAC requested the inclusion of what concrete actions ICANN Contractual Compliance might take against registrars or registry operators who are found to not be in compliance with the new terms in the Agreements.

6. Suggested additional reporting requirements and data collection

TLD Registry Limited OY, iQ, ALAC, and individuals stated that expanding obligations for registry operators to conduct technical analyses and maintain statistical reports on DNS Abuse is commendable and a significant improvement in addition to clarifying the registry operator obligations. These comments explained that these measures enable ongoing monitoring and timely resolution.

African Regional At-Large Organization (AFRALO) and other organizations listed below in this section commented that ICANN org and the CPs should include enhanced reporting requirements and data collection related to DNS Abuse.

The SSAC observes that measurement against goals requires data collection and reporting, and that these implementation issues will be critical to the success of this initiative. The SSAC would appreciate the community being kept up-to-date on implementation of these amendments and how ICANN org will measure progress against overall goals.

The GAC suggests that ICANN org provide the community with the ability to monitor how compliance is enforced, and to link future work on DNS Abuse with the review of such data. The GAC also suggests the parties consider how to enhance the proposed reporting requirements with a view to promoting transparency of the CPs' policies and how they respond to DNS Abuse reports.

The Technology Verification Team, Working-Level Forum for Anti-Piracy of Japan requests that ICANN publish transparency reports that can verify effective compliance of registries and registrars with the Agreements. The Technology Verification Team, Working-Level Forum for Anti-Piracy of Japan explains that despite the importance of Domain Abuse Activity Reporting (DAAR) project, it is unable to measure the incidents and trends of DNS abuse on a per-registry or per-registrar basis. Therefore, the Technology Verification Team, Working-Level Forum for Anti-Piracy of Japan requests that the DAAR include the number of DNS abuse incidents per-registry and per-registrar in the report.

Section 4: Analysis of Submissions

ICANN org and the CPH NT appreciate the feedback to the proposed amendments and thank all the contributors for the valuable input. In general, the proposed amendments and the contractual obligations for DNS Abuse received strong support across the industry and ICANN

community. Support was also received for the addition of an obligation to provide confirmation of receipt of an abuse report. Many comments encourage the CPs to approve and implement the proposed amendments which they stated would be a significant achievement of the multistakeholder model. NameCheap Inc., i2Coalition, and the RrSG, strongly support the proposed amendments to the Agreements, the draft ICANN Advisory, and encourage that they be adopted in their current form.

Regarding comments that the proposed amendments are insufficient to address the challenge of DNS Abuse, ICANN org acknowledges the comments and reminds the community that the ICANN community will have the opportunity to discuss these obligations and determine if further obligations are required. If so, that should likely take place through the Generic Names Supporting Organization's (GNSO's) open, transparent multistakeholder policy development process. Defining specific improvements to the existing obligations in the Agreements is intended to become an important building block in further combating DNS Abuse. We believe taking firm practical steps aligns with the recommendations made by the GNSO Small Team on DNS Abuse. ICANN org and the CPH NT support the comments from the GAC which stated that after the proposed amendments are adopted, work should include Policy Development Processes (PDPs) to further inform the updated Base RA and RAA.

1. The definition of DNS Abuse in the proposed amendments and ICANN's remit

Several groups and individuals submitted comments that the proposed amendments should expand the definition of DNS Abuse to include content-related matters. ICANN org acknowledges the comments on this topic. It is important to remember that the proposed amendment resulted from the November 2022 proposal the CPH sent to ICANN org to collaborate and enhance the existing contracts by creating clear obligations to stop or otherwise disrupt DNS Abuse. This proposal came with certain guideposts, including to not include matters pertaining to website content. It is equally important to remember that while the new obligations are specific to DNS Abuse as defined in the amendments, they do not negate the existing obligations in Section 3.18 of the RAA. Section 3.18.1 of the RAA requires that registrars take reasonable and prompt steps to investigate and respond appropriately to **any** (emphasis added) report of abuse. This obligation remains in effect and will continue to be enforced.

The security and stability of the DNS are core to ICANN's mission. However, staying within ICANN's technical remit is necessary. Core to the issue is what is within the ICANN remit. It is clear that the items listed in the proposed definition of DNS Abuse within the amendments are within ICANN's remit. It is in line with the ICANN Bylaws (Sections 1.1 and 1.2.) as well as ICANN's Strategic Plan, which states that a "coordinated approach is necessary to effectively identify and mitigate DNS security threats and combat DNS abuse." However, many other examples of abuse discussed in some sectors of the community and the Public Comments, while malicious, are deemed outside of ICANN's remit as they pertain to content, such as certain forms of fraud, copyright or trademark infringement, and scams perpetrated through websites. These harms often require legal expertise and due process to the registrant. Intellectual property disputes are complex, involving considerations such as fair use, free speech, and laws from multiple jurisdictions, and CPs are not the proper venue to adjudicate these disputes. Other frameworks exist to address some forms of intellectual property infringement. For example, ICANN's Uniform Domain-Name Dispute Resolution Policy (UDRP) is designed specifically to deal with trademark infringement in domain names, and is binding on all registered second level names in gTLDs. Further, the Uniform Rapid Suspension System (URS) is a rights protection mechanism that complements the UDRP by offering a lower-cost,

faster path to relief for rights holders experiencing the most clear-cut cases of infringement. Additionally, Specification 11.3 (a) of the Base RA and similar provisions in .COM, .NET and other legacy TLD RAs requires that the registry operators include a provision in its Registry-Registrar Agreement that requires registrars to include in their Registration Agreements a provision prohibiting registrants 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 consequences for such activities including suspension of the domain name.

Some comments call for contracted parties to disclose the policies that govern their relationships with registrants and remain accountable to registrants while making any and all decisions that impact them. Throughout ICANN's policies and agreements, there are multiple requirements related to ensuring information is provided to registrants. These requirements are, and will continue to be, enforced. For example, the requirements in RAA Section 3.7.7 et seq. for registrars and registrants to enter into registration agreements that set forth the terms and conditions applicable to each domain name registration. Another example includes the registrars' obligation to comply with the Registrants' Benefits and Responsibilities Specification of the RAA, including by providing registrants with information about how to raise concerns and resolve disputes with the registrar (see Section 3.7.10 of the RAA). Further, Section 3.7.11 of the RAA requires that registrars make available to registrants a description of the customer service handling processes, including a description of the processes for submitting complaints and resolving disputes regarding registrar services. Section 3.18.3 of the RAA also requires registrars to publish on their website a description of its procedures for the receipt, handling, and tracking of abuse reports. Registrars must also document its receipt of and response to all abuse reports. ICANN org does not believe that additional language is needed in this regard.

To the point raised by the SSAC regarding Section 2.1 of SAC115 not containing the SSAC's definitions of abuse, ICANN org would like to clarify that the elements of abuse are what are defined in Section 2.1 of SAC115. ICANN org is using the definition of the terms malware, botnets, phishing, pharming, and spam (when spam is used as a delivery mechanism for any of the other four types of DNS Abuse) as defined by the SSAC and as further explained in the draft Advisory. ICANN org is not stating that this is the SSAC's definition of DNS Abuse. We also thank you for your comments regarding spam. ICANN org recognizes the definition of spam in the amendments is leveraged from SSAC115 with an added qualifier to include spam in the definition of DNS Abuse when it is used as a delivery mechanism. ICANN org nor the CPH NT believe this creates confusion regarding what SPAM is considered DNS Abuse.

2. Provide additional clarity related to the terminology used in the proposed amendments

To address comments that ask for terms like "actionable evidence," "appropriate" or "prompt" to be further defined, please refer to the draft Advisory which explains why the proposed amendments do not specify what mitigation actions are appropriate and prompt. Defining these terms may not always guarantee the desired outcome and may even result in undesirable outcomes in some instances. What is appropriate, prompt, or actionable will greatly depend on the specific circumstances of each case. This is why the draft Advisory provides illustrative examples with specific facts tied to specific actions and timing. This is also why the draft Advisory indicates that whenever ICANN Contractual Compliance initiates an investigation, registrars and registry operators will be asked to provide evidence demonstrating compliance with the relevant RAA and Base RA requirements considering the specific circumstances of the

case. Further, the draft Advisory is not meant to be a static document, and over time, may be updated as additional insight is gained through the enforcement of the new obligations.

3. How to address systemic abuse
ICANN org recognizes that more work needs to be done in this area to address systemic abuse on the Internet. ICANN org and the CPH NT note that there is no consensus definition of what systemic abuse is and see these proposed amendments as needing to be meaningful and enforceable to raise the floor and expediently close the gap in the current contracts. We believe this is a good area for the ICANN community to further discuss and consider what is systemic abuse and how best to address systemic abuse. ICANN org will continue to provide or enable sharing of good practices on combating DNS abuse. For example, the upcoming Day of DNS Abuse Discussions in Da Nang Vietnam, see please the agenda for more information.

While there is no consensus definition of what constitutes systemic abuse, there is also nothing in the amendments that prevents ICANN Contractual Compliance from enforcing the new DNS Abuse obligations against CPs that exhibit a pattern of allowing registration of large volumes of abusive names. The proposed amendments empower ICANN org to address all instances of evidenced DNS Abuse, whether they involve a single domain name or thousands. The obligations will be enforced against all domain names within a given case arising from external complaints, proactive enforcement or through the ICANN Audit Program.

Additionally, the RAA and the Base RA provide consequences for CPs who are repeatedly found to be in breach of their respective agreements. Specifically, ICANN org may terminate (Section 5.5.6 of the RAA) or suspend for up to twelve months (5.7.1 of the RAA) a registrar's accreditation when such a registrar has been in fundamental and material breach of its RAA obligations (abuse-related obligations or others) at least three (3) times within a twelve (12) month period. Similarly, in accordance with Section 5.2.3 of the RAA, a registrar's accreditation will not be renewed when such a registrar has been given notice by ICANN org of three (3) or more material breaches of this RAA within the two (2) years preceding the Expiration Date or the date of expiration of any successive five (5) year term thereafter. Article 4.2 (a) (ii) of the Base RA describes the instances in which a RA will not be renewed, including when a registry operator has been found by an arbitrator or a court of competent jurisdiction on at least three (3) separate occasions to have been in (A) fundamental and material breach (whether or not cured) of Registry Operator's covenants set forth in Article 2 or (B) breach of its payment obligations under Article 6 of this Agreement.

ICANN org is not suggesting that the existing or proposed contractual requirements explicitly define or address "systemic abuse," or that the community should not discuss how to define and address systemic abuse. Rather, the current Agreements and the proposed amendments provide enforceable obligations to mitigate and disrupt all instances of DNS Abuse.

4. Abuse report handling

In response to comments that request service-level agreements be added to the proposed amendments, as explained in the draft Advisory, the appropriate mitigation action to stop or disrupt an instance of DNS Abuse will vary depending on the specific circumstances of each case. Consequently, the appropriate amount of time to investigate and take action will also vary, making it impossible to prescribe a fixed amount of time for an action to be considered "prompt." Instead, registrars and registry operators must demonstrate an ongoing attentiveness to allegations of sponsored names being used for DNS Abuse. The attentiveness should be commensurate with the potential harm that DNS Abuse causes victims. The examples within the

draft Advisory illustrate reasonable mitigation actions promptly taken to stop or contribute to stopping the Registered Name from being used for DNS Abuse. As explained in the draft Advisory, in response to an inquiry by ICANN Contractual Compliance, registrars and registry operators will be required to explain how the actions were prompt considering the specific circumstances. ICANN Contractual Compliance will then review the explanation and the relevant circumstances to make a case-by-case determination as to whether the actions were reasonably prompt.

ICANN org and the CPH NT thank all for comments which call for CPs to document to the abuse reporter the specific steps taken (or in some instances, not taken) to address reported abuse. ICANN and the CPH NT appreciate the spirit of the suggestion and request. However there remain concerns about the burdens this could place on the CPs to manage status of reports, especially those receiving a large volume of reports, that could detract resources from combatting DNS Abuse. ICANN org believes this is a matter for the community to further discuss and consider the best path forward rather than delay progress on what has been agreed to already in these amendments.

Some comments call for elaboration of best practices for formatting webforms. The use of webforms is intended to facilitate submission of actionable evidence in correspondence with the DNS Abuse complaints. ICANN org believes the language in the proposed amendments is adequate, and the concerns regarding webform restrictions are still enforceable with the current language; particularly, if the restrictions prevent the reporter from submitting complete reports. For example, it would not be considered compliant if the registrar did not act on an abuse report for lack of actionable evidence if the absence of actionable evidence was due to webform restrictions and failure of the registrar to seek such information. Further, the Advisory is not meant to be a static document, and over time, may be updated as additional insight is gained through the enforcement of the new obligations, including insight respective to webform formatting issues.

In response to comments that stated the proposed amendments should require registry operators to take mitigation action if the registrar fails to adequately act to mitigate the reported abuse, in Section 4 of Specification 6 of the proposed amendment to the Base RA, registry operators have the ability of taking direct action where the registry operator deems appropriate.

To address comments suggested that registrars be obligated to forward received abuse reports to the “best-positioned” entity for DNS Abuse mitigation, we recognize that in some instances a third-party entity such as the web-hosting provider, the content delivery network, or others might be best positioned, and sometimes it may a combination of all. ICANN org would expect the registrar to refer the complainant to the appropriate party, but we cannot reasonably require registrars to communicate with a third-party entity. The registrar may not have contact information, interaction or relationship with the “best-positioned” entity and registrar action will depend on the specific circumstances of each case.

5. ICANN Contractual Compliance enforcement of the obligations

ICANN Contractual Compliance enforces all obligations with ICANN’s CPs in a fair and consistent manner. Failure to cure any instances of non-compliance, including with the proposed DNS Abuse obligations, may result in the suspension or termination of a CP’s agreement with ICANN org as explained below.

ICANN Contractual Compliance will follow its established process to enforce the new obligations, should they be approved. The process comprises two stages: an informal and formal resolution stage. The informal resolution stage (through which most investigations are resolved and closed) generally entails, at a minimum, three notifications and two phone calls to the CP. These communications include an itemized list of information and records needed to evaluate compliance.

In the event a CP continues to demonstrate non-compliance following exhaustion of the informal resolution stage, ICANN Contractual Compliance issues a formal notice of breach. If the CP does not cure all areas of non-compliance identified in the formal notice by the specified deadline, ICANN Contractual Compliance may suspend (registrars only – see Section 5.7.1 of the RAA) or initiate termination proceedings of the CP's accreditation with ICANN org (see Section 5.5.4 of the RAA and Article 4.3 of the Base RA.) Additionally, compliance with contractual obligations is a requirement, with certain conditions, for a CP to renew its RAA or RA with ICANN org or assign it to another entity (see Section 5.2 of the RAA and 4.2 of the Base RA, and Sections 7.3 of the RAA and 7.5 of the Base RA supplemented by the information at https://www.icann.org/resources/assignments).

The Contractual Compliance process is published, and the consequences of non-compliance are clearly described in the respective agreements. The draft Advisory helps provide additional detail as to ICANN org's expectations for CP compliance. ICANN org does not believe that additional language is needed in the Agreements to clarify what actions ICANN Contractual Compliance will take against registrars or registry operators that are found non-compliant with the new requirements. With respect to the compliance enforcement process itself, ICANN org may include in the draft Advisory a link to the suspension and termination provisions in the relevant agreements as well as to ICANN Contractual Compliance's established process for added clarity.

6. Suggested additional reporting requirements and data collection

The goal of the proposed amendments is to enhance the existing obligations by requiring registrars and registry operators to promptly take reasonable and appropriate action to stop or otherwise disrupt DNS Abuse. The targeted amendments do not focus on enhancing data reporting and data collection requirements. The proposed amendments will require significant work to be conducted by registrars. Enhanced reporting requirements and data collection can be part of a voluntary framework, and this is a good area of discussion for the ICANN community to align on proactive monitoring and obligations in a potential PDP. ICANN org does not believe this work should impede the progress of the proposed amendments and their adoption by the CPs.

7. Out of scope for amendments

Many organizations and individuals called for enhanced registrant data accuracy verification obligations and for the definition of DNS Abuse in the proposed amendments to be expanded to include website content abuses. However, as explained in the 4 November 2022 letter from the CPH, which ICANN org agreed to, matters pertaining to website content abuses and access to registration data would not be included in the amendments. ICANN org and the CPH NT respected the agreed upon guideposts for the potential amendments during negotiations.

Section 5: Next Steps

Following the completion of the Public Comment process, ICANN org will facilitate a vote by all eligible registrars and registries to approve or reject the proposed amendments. In order for the proposed amendments to be approved, the following thresholds must be met, respectively: (i) for the RAA, approval of registrars accounting for 90 percent of the total registered domain names under management and (ii) for the RA, approval of registry operators whose payments to ICANN account for two-thirds of total fees paid in the prior year and approval of a majority of registry operators (one vote per TLD). Following an approval vote, the proposed amendments will be sent to the ICANN Board for consideration. If these approvals are obtained, the amendments will become effective following notice from ICANN org. If the proposed amendments do not reach the necessary thresholds, the negotiating teams will discuss next steps.