Comments of the Messaging Malware Mobile Anti-Abuse Working Group (M^3AAWG) on

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

M^3AAWG welcomes the Contracted Party House's consideration of long overdue changes to the Base gTLDs Registry Agreement (RA) and the Registrar Accreditation Agreement (RAA) related to the pertinent issue of DNS Abuse. While we are happy to see this effort, we would like to note that this necessary step should be part of a coordinated effort to address DNS Abuse now and going forward. Individually, the proposed changes are insufficient to address the challenge of DNS Abuse.

Below, we speak to various concerns voiced by our membership and subject matter experts.

I. In general, contract changes and all relevant requirements must be consistently applied, documented, and actively enforced.

II. Much of the relevant information is currently to be found in supplemental documents. To be properly applicable and enforceable, these documents must either be integrated into the contract documents or clearly and fully referenced as enforceable attachments.

III. The obligations for Contracted Parties, ICANN as a governing body, as well as for ICANN Org and its functional units, must be clearly laid out, either in the contract, or in referenced documents, to be clear, implementable, and enforceable.

IV. The definition of DNS Abuse has been an open discussion for over a decade. However, there is still insufficient agreement on the definition or on practical anti-abuse efforts. Instead of continuing the search for an all-encompassing definition, contracted parties should produce specific measures that deal with DNS Abuse and ensure that they track the evolving nature of DNS Abuse.[1]

Crucially, as cybercrime and abuse are constantly evolving, the list and definition of what constitutes DNS Abuse is constantly in flux. Therefore, this aspect of the contract must be reviewed and updated regularly by a diverse group of experts. We propose a 2-year review turnus. This will provide pragmatic clarity while also avoiding the risk of being locked into outdated definitions or incomplete lists of individually relevant, illicit activities.

V. The role of ICANN compliance has been a critical concern for years. We note that ICANN compliance must be empowered to properly enforce the DNS Abuse provisions of the contract in terms of mandate and resourcing. To enable enforcement, we reiterate that the contract must be written as simply and clearly as possible.

[1] This might include fast and functional processes to respond to abuse notices, fast responses to legitimate requests for WHOIS information, timely takedowns of domains, and so on.

VI. The amendments do not include terms addressing systemic abuse, such as when thousands of similar domain names are registered by the same party for use in a malware attack. While the amendments appear to include obligations to mitigate domains on a one-by-one basis, there is no obligation to take proactive steps that will prevent having other domain names linked to the same abusive party. We recommend that ICANN address this situation now, by issuing guidelines or advisories to the Registrars and the Registry Operators to encourage them to address systemic abuse proactively rather than reactively.

VII. Many registries and registrars are addressing abuse, and many Contracted Parties agree on the basics of anti-abuse, as evidenced by the *DNS Abuse Framework*.[2] We hope that this effort will further what is already established and that tangible changes will result from this effort.

VIII. Comments related to some specific contract terms follow.

We appreciate the opportunity to submit these comments, and we welcome the opportunity to engage as needed to answer any questions during this process. Please address any inquiries to M^{3}AAWG Executive Director Amy Cadagin at comments@m3aawg.org.

Sincerely,
Amy Cadagin
Executive Director, Messaging Malware Mobile Anti-Abuse Working Group
comments@m3aawg.org
P.O. Box 9125 Brea, CA 92822

[2] https://dnsabuseframework.org/

Attachment: Specific Comments on Proposals

Specific Comments on the 2024 Global Amendment to Registrar Accreditation Agreements

3.18.1 Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of DNS Abuse and Illegal Activity.

> We support this requirement. We note that at times, abuse reporting addresses may be subject to routine email anti-malware and anti-spam filtering. That can make it hard or impossible to share samples of malicious or unwanted messages. Thus, we believe that the abuse contact address must be unfiltered in order to ensure that reporting systems are in fact possible.
>
> As a result, the first sentence should be revised as follows:
>
> *"*Registrar shall maintain an abuse contact **configured to receive all reports of abuse…"**

Registrar shall publish an email address or webform to receive such reports on, or conspicuously and readily accessible from, the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time).

> While allowing flexibility in implementation is normally a positive, here email should always be present as a reporting mechanism. In addition, webform content and layout should be standardized. If the text were to remain as stated, every registrar might implement a different approach to accepting abuse reports. Without standardization, reporters will either find it difficult to submit reports at scale, or may be deterred from reporting at all.
>
> In addition, M^{3}AAWG recommends that the following sentence be added after the first sentence in order to ensure that the webforms are able to handle the high volumes that are often associated with malware attacks, and to ensure that the reporters have the ability to submit screenshots and other evidence to support the request.
>
> "…(or in another standardized place that may be designated by ICANN from time to time)**. Where a webform is used, the webform must not impose unreasonable rate limits on submissions, and must allow users to submit attachments up to a reasonable file size limit."**

Upon receipt of such reports, Registrar shall provide the reporter with confirmation that it has received the report.

> In the case of email-based reports, we expect that this confirmation would likely be in the form of a confirmation email. Given that email apparent senders can be spoofed, this means report confirmations can be used as a reflected attack on innocent third parties. Therefore, we recommend allowing submission via an authenticated API in a standardized format, in addition to any other also-allowed ad hoc reporting channel.

Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse.

> What constitutes "reasonable," "prompt" and "appropriate" must be more clearly defined in the contract. While we understand that examples may have been provided elsewhere as to what is

considered "reasonable," sufficiently prompt, or "appropriate," those examples are not formally part of the contract, and hence are informative rather than determinative, at best.

As a result, we recommend the following revisions:

"Registrar shall take reasonable and prompt steps **(within 3 business days, with the speed proportional to the abuse risk)** to investigate**, mitigate (where DNS Abuse is detected),** and respond appropriately to any **acts** of abuse."

For the purposes of this Agreement, "DNS Abuse" means malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse listed in this Section) as those terms are defined in Section 2.1 of SAC115 (<https://www.icann.org/en/system/files/files/sac-115-en.pdf>).

The quoted typology of abuse includes many common ills that deserve action and remediation, but is far from complete or sufficiently flexible in a changing abuse environment. For example, this definition excludes spam per se, not as a distribution measure or component of another criminal or abusive enterprise. Domain registrations involving fake point of contact information are also excluded, alongside distributed denial-of-service (DDoS) and problematic content such as Child Sexual Abuse Materials (CSAM), terrorism-promoting content/terrorism funding solicitations, the online sale of controlled substances without a valid prescription, and other illegal behaviors. The current policy fails to make all of these other abuses actionable.

As stated previously, we therefore believe the definition of "DNS Abuse" needs to be enlarged to encompass a broader range of criminal and abusive behaviors that may leverage the DNS.[3] We also urge that (bi-yearly) reviews, and, if necessary, updates to this definition are performed going forward.

As a result, we recommend that this text be revised as follows to add the following two sentences:

"…SAC 115. **In addition, 'DNS Abuse' includes DDoS, Child Sexual Abuse Materials (CSAM), terrorism-promoting content, terrorism funding solicitations, the online sale of controlled substances without a valid prescription, general spam (not referenced in the prior sentence), and the online sale of counterfeit goods."**

"Relevant definitions of DNS abuse and descriptions of relevant abusive activities must be reviewed, and, if necessary, updated every two (2) years."

3.18.2 When Registrar has actionable evidence that a Registered Name sponsored by Registrar is being used for DNS Abuse, Registrar must promptly take the appropriate mitigation action(s) that are reasonably necessary to stop, or otherwise disrupt, the Registered Name from being used for DNS Abuse. Action(s) may vary depending on the circumstances, taking into account the cause and severity of the harm from the DNS Abuse and the possibility of associated collateral damage.

We support this new section and suggest that it may be improved to ensure that the abusive domain name can no longer be used for DNS Abuse. The proposed language is limited to situations where the domain name is currently being used for DNS Abuse. Yet we observe that domain names are

[3] A helpful list of potentially relevant DNS abuse types can be found at https://international.eco.de/download/205700/

sometimes being used for DNS Abuse over longer periods of time. During that time period, hosting providers sometimes take down content while the domain remains active. In order to prevent the abuse from the domain name to jump to another hosting provider to continue the abuse, we recommend that this section be amended as follows:

"When Registrar has actionable evidence that a Registered Name sponsored by the Registrar is being **or has been used** for DNS abuse**, or if the Registrar has actionable evidence that a Registrant is using multiple names for DNS abuse…."**

Including this new language would help mitigate the risk that anti-abuse actors are moving from one provider to another at high speed, forcing anti-abuse actors to play whack-a-mole.

3.18.3 Registrar shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored twenty-four (24) hours a day, seven (7) days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the Registrar is established or maintains a physical office.

We recommend rewriting this requirement for clarity and ease of comprehension. The current wording is unclear and not explicit and can thus be understood in a variety of ways. In the event this section is not rewritten in its entirety, at a minimum, we would recommend clarifying the use of "Illegal Activity" in that sentence.

We also urge the explicit adoption of a requirement that at least one universally supported/mandatory language be set in addition to any locally supported alternatives. Following the lead of International Civil Aviation Organization (ICAO) and the International Maritime Organization (IMO),[4] we recommend that all registrars be required to accept DNS abuse reports made in English (as well as any other languages of their choice). In the absence of such a requirement, we believe registrars would be free to require reports to be made exclusively in one language. Many abuse reporting parties may be unable to satisfy such requirements.

Well-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by the Registrar to take necessary and appropriate actions in response to the report.

As currently stated, the Illegal Activity report must be reviewed within twenty-four (24) hours. Instead, we urge requiring and setting deadlines for actions that must be taken in response to a verified complaint, and giving deficient complaints the opportunity to be cured and made well-founded if a minor deficiency exists.

3.18.4 Registrar shall publish on its website a description of its procedures for the receipt, handling, and tracking of abuse reports.

We agree that transparency is useful but would like to note that personal identifiable information (PII) should be redacted from these reports.

[4] See https://www.icao.int/safety/lpr/Documents/A38.8.pdf and https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/A.918(22).pdf.

Registrar shall document its receipt of and response to all such reports.

> We urge explicit transparent public disclosure, keeping in mind privacy concerns. As much detail as possible should be provided at all stages, with the exception of the identities of reporters and other actors, which should be withheld to prevent potential retribution against reporters and victimization of other relevant parties.

Registrar shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period, shall provide such records to ICANN upon reasonable notice.

> We believe this retention schedule is too short. Official investigations by law enforcement, for example, may routinely take three (3) or more years. This retention schedule would lead to data being deleted too early.

3.18.2 When Registrar has actionable evidence that a Registered Name sponsored by Registrar is being used for DNS Abuse, Registrar must promptly take the appropriate mitigation action(s) that are reasonably necessary to stop, or otherwise disrupt, the Registered Name from being used for DNS Abuse. Action(s) may vary depending on the circumstances, taking into account the cause and severity of the harm from the DNS Abuse and the possibility of associated collateral damage.

> We support this new section and suggest that it may be improved to ensure that the abusive domain name can no longer be used for DNS Abuse. The proposed language is limited to situations where the domain name is currently being used for DNS abuse. Yet, we observe that domain names are sometimes being used for DNS abuse over longer periods of time. During that time period, hosting providers sometimes take down content, while the domain remains active. Including this new language would help mitigate the risk that anti-abuse actors are moving from one provider to another at high speed, with anti-abuse actors forced to play "whack-a-mole". In order to prevent the abuse from the domain name to jump to another hosting provider to continue the abuse, we recommend that this section be amended as follows:
>
> "When a Registrar has actionable evidence that a Registered Name sponsored by the Registrar is being or has been used for DNS abuse, or if the Registrar has actionable evidence that a Registrant is using multiple names for DNS abuse."

Specific Comments on the 2024 Global Amendment to Registry Agreements

4.1. Abuse Contact. Registry Operator shall provide to ICANN and publish on its website its accurate contact details including a valid email address or webform and mailing address as well as a primary contact for handling reports related to malicious conduct in the TLD, including DNS Abuse, and will provide ICANN with prompt notice of any changes to such contact details. Upon receipt of such reports, Registry Operator shall provide the reporter with confirmation that it has received the report.

For the purposes of this Agreement, "DNS Abuse" is defined as malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse listed in this Section) as those terms are defined in Section 2.1 of SAC115 (<https://www.icann.org/en/system/files/files/sac-115-en.pdf>).

Please refer to the comments that treat analogous sections of the RAA above. For the reasons described there, we recommend the following revisions to this text:

> **“**Registry Operator **shall maintain an abuse contact configured to receive all reports of abuse and** shall provide to ICANN and publish on its website its accurate contact details including a valid email address or webform and mailing address as well as a primary contact for handling reports related to malicious conduct in the TLD, including DNS Abuse, and will provide ICANN with prompt notice of any changes to such contact details. **(Where a webform is used, the webform must not impose unreasonable rate limits on submissions, and must allow users to submit attachments up to a reasonable file size limit.)** Upon receipt of such reports, Registry Operator shall provide the reporter with confirmation that it has received the report.**”**
>
> **“…**SAC 115. In addition, ‘DNS Abuse’ includes DDoS, Child Sexual Abuse Materials (CSAM), terrorism-promoting content, terrorism funding solicitations, the online sale of controlled substances without a valid prescription, general spam (not referenced in the prior sentence), and the online sale of counterfeit goods. Relevant definitions of DNS abuse and descriptions of relevant abusive activities must be reviewed, and if necessary, updated every two years.”

4.2 DNS Abuse Mitigation. Where a Registry Operator reasonably determines, based on actionable evidence, that a registered domain name in the TLD is being used for DNS Abuse, Registry Operator must promptly take the appropriate mitigation action(s) that are reasonably necessary to contribute to stopping, or otherwise disrupting, the domain name from being used for DNS Abuse. Such action(s) shall, at a minimum, include: (i) the referral of the domains being used for the DNS Abuse, along with relevant evidence, to the sponsoring registrar; or (ii) the taking of direct action, by the Registry Operator, where the Registry Operator deems appropriate. Action(s) may vary depending on the circumstances of each case, taking into account the severity of the harm from the DNS Abuse and the possibility of associated collateral damage.

> We observe that this text contains significantly fewer definitive obligations for Registry Operators. We suggest that the language be tightened, tracking the language applicable to Registrars. We note that there are times when Registry Operators may need to step in, such as when there is a non-compliant registrar, or when the laws applicable to the Registry Operator may be different than those applicable to the Registrar in a way that prevents action by the Registrar. We also note that if the Registrar does not act, the current proposed language does not include an obligation for the Registry to act, since it will have fulfilled its obligations by merely “referring” the domain to the sponsoring Registrar.
>
> As a result, we recommend the following revisions, which tracks the Registrar language above:
>
> “**Where a Registr**y Operato**r has** actionable evidence that a registered domain name in the TLD is being **or has been** used for DNS Abuse, Registry Operator must promptly take the appropriate mitigation action(s) that are reasonably necessary to **stop or otherwise disrupt** the **domain name from being used for DNS Abuse.”**
>
> **“**Such action(s) shall, at a minimum, include: (i) the referral of the domains being used for the DNS Abuse, along with relevant evidence, to the sponsoring registrar; or (ii) the taking of direct Action, by the Registry Operator, where the Registry Operator deems appropriate. **Where the Registry**

Operator refers the domains being used for the DNS Abuse under Section 4.2 (i), along with relevant evidence, to the sponsoring registrar, and the sponsoring registrar does not promptly take the appropriate mitigation action(s) that are reasonably necessary to stop or otherwise disrupt the domain name(s) from being used for DNS Abuse, the Registry Operator shall promptly directly take the appropriate mitigation action(s) that are reasonably necessary to stop or otherwise disrupt the domain name(s) from being used for DNS Abuse."