Board Action/Rationale on & ICANN org Assessment of Competition, Consumer Trust, Consumer Choice Review (CCT) Pending Recommendations 14 and 15, and Second Security, Stability and Resiliency of DNS Review (SSR2) Recommendations 9.2, 9.3, 12.1, 12.2, 12.3, 12.4, 13.1, 13.2 and 14.2

10 September 2023

The Board takes action on DNS abuse related CCT Recommendations 14, 15 and SSR2 Recommendations 12.1, 12.2, 12.3, 12.4, 13.1, 13.2, 14.2.

The Board acknowledges the CCT and SSR2 Review Teams' concerns and input related to DNS security threats and DNS abuse, and wishes to highlight that the Board has placed significant focus on these issues both prior to and since the conclusion of each of these Review Teams' work. As a matter of fact, ICANN's Strategic Plan for 2021-2025, which feeds the Operating Initiatives in ICANN's annual operating plans, has a specific strategic objective related to security, "Strengthen the security of the Domain Name System and the DNS Root Server System", for whose achievement 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. In 2020 ICANN 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:

- 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.
- Interpreting and enforcing the contractual obligations related to DNS security threats and abuse generally in Registry Agreements, Registrar Accreditation Agreements, and ICANN consensus policies.

Since 2020 the org has initiated, advanced or deployed several important pieces of work related to combatting DNS Security Threats or DNS Abuse. They include:

- Publication of first DNS Abuse trends report, which was based on data from the Domain Abuse Activity Reporting System (DAAR). The report shows that DNS security threats have been trending downward over the prior four years.
- Enrollment of more than 20 Country Code Top Level Domains (ccTLDs) to voluntarily participate in DAAR.
- Securement of contractual changes with the gTLD Registries to enable ICANN access to data to extend DAAR-like reporting to the registrar level.
- Contribution to an environment where the contracted parties voluntarily initiated contractual negotiations to add obligations to mitigate DNS Abuse in both the Registry and Registrar Agreements.
- Creation of the Domain Name Security Threat Information Collection and Reporting (DNSTICR) tool to analyze domain name registrations related to COVID-19 to identify credible evidence of malware or phishing and notify the sponsoring registrars to help in their mitigation efforts.

The Board recognizes that the discussion and work on DNS abuse has evolved and will continue to evolve over time. Therefore, the Board is appreciative of any current and future ICANN org plan and initiative that contribute to sharing data, refining contracted parties' agreements, investigating actions that support the fight to deter and mitigate DNS abuse, and further enhancing the global stakeholder collaborative approach that is needed to achieve higher results.

These considerations have informed the Board's approach to the recommendations presented in this scorecard.

CCT REC# 14	**Recommendation language**: Consider directing ICANN organization, in its discussions with registries, to negotiate amendments to existing Registry Agreements, or in consideration of new Registry Agreements associated with subsequent rounds of new gTLDs, to include provisions in the agreements to provide incentives, including financial incentives for registries, especially open registries, to adopt proactive anti-abuse measures. **CCT priority:** High **CCT directed to**: The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization, and the Subsequent Procedures PDP WG.

Board action/rationale:

The Board has aligned on the following working baseline definition of DNS abuse for ICANN: "DNS abuse includes five broad categories of harmful activity: Phishing, Malware, Botnet Command and Control, SPAM when used as a vector, and Pharming."

The Board recognizes this working definition is neither an exhaustive list nor a criteria-based definition and may need adjusting in the future as DNS abuse evolves. However, it brings together a set of agreed upon DNS security threats to which policy and mitigation work within ICANN can take place immediately, while or if definitions continue to be debated.

The Board recognizes the progress of the proposed amendments to the Registrar Accreditation Agreement and Base gTLD Registry Agreement that plan to add obligations to mitigate DNS Abuse. Subsequent to the potential incorporation of these amendments into contracts, the community may determine, as appropriate, if policy work would be beneficial to further combat DNS Abuse. Preventative measures, as envisioned in this recommendation, are a possible topic of such community discussions.

The Board acknowledges that this recommendation was assigned a high priority level by the Review Team. For this reason, the Board appreciates the extensive work conducted by ICANN org to investigate financial incentives by and for registries. ICANN org's findings show that there are specific incentives that some registries, including ccTLDs, have introduced, especially towards their registrars, to support anti-abuse measures. However, at present there is no clear evidence that such incentives ICANN could offer to registries would have the desired impact of preventing DNS abuse from occurring within a TLD. Consequently, the Board believes that there are not sufficient grounds to direct ICANN org to implement this recommendation which, therefore, is rejected.

Additionally, the Board encourages ICANN org to continue its existing efforts to educate stakeholders on the importance of working together to prevent, mitigate, contain and act on possible DNS abuse, and to continue to remain vigilant on possible actions to further combat DNS Abuse.

ICANN org assessment:

ICANN org notes that the Board has aligned on a working baseline definition of DNS abuse for ICANN: "DNS abuse includes five broad categories of harmful activity: Phishing, Malware, Botnet Command and Control, SPAM when used as a vector, and Pharming." It is understood that this working baseline is neither an exhaustive list nor a criteria-based definition. However, it brings together a set of agreed-upon DNS Security Threats to which policy and mitigation work within ICANN can take place immediately, while or if definitions continue to be debated. As established in the November 2022 exchange of letters between the Contracted Party House (CPH) and ICANN org, there are ongoing efforts between ICANN org, the Registrar Stakeholder Group (RrSG), and gTLD Registries Stakeholder Group (RySG) to pursue enhancements to the DNS abuse obligations contained in the Registrar Accreditation Agreement (RAA) and Base gTLD Registry Agreement (RA). A critical aspect of the proposal by the RySG and RrSG to strengthen existing abuse-related obligations is to arrive upon a definition of the forms of DNS abuse that fall within ICANN's mandate.

ICANN org has investigated existing practices that some registries, mostly ccTLDs, have introduced over the years to financially support registrar actions that can prevent and/or mitigate possible DNS abuses. Findings of this investigation show a range of measures with varying

success levels and costs on the registry. ICANN org concluded that at present there is no well-established practice for specific and effective incentives that might be offered to registries, including open registries, which could guarantee significant improvements to prevent and/or mitigate DNS abuse.

Furthermore, it is worth noting that this recommendation calls for changes to contracted party agreements which would be a matter of policy or a result of voluntary negotiations between ICANN org and contracted parties. Since January 2023, ICANN org has been actively engaged in a contract amendment process with the 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 may be presumptive for ICANN org to attempt to design and add anti-abuse incentives before the community has had a chance to consider what behaviours 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.

CCT REC #15	**Recommendation language**: ICANN Org should, in its discussions with registrars and registries, negotiate amendments to the Registrar Accreditation Agreement and Registry Agreements to include provisions aimed at preventing systemic use of specific registrars or registries for DNS Security Abuse. With a view to implementing this recommendation as early as possible, and provided this can be done, then this could be brought into effect by a contractual amendment through the bilateral review of the Agreements. In particular, ICANN should establish thresholds of abuse at which compliance inquiries are automatically triggered, with a higher threshold at which registrars and registries are presumed to be in default of their agreements. If the community determines that ICANN org itself is ill-suited or unable to enforce such provisions, a DNS Abuse Dispute Resolution Policy (DADRP) should be considered as an additional means to enforce policies and deter against DNS Security Abuse. Furthermore, defining and identifying DNS Security Abuse is inherently complex and would benefit from analysis by the community, and thus we specifically recommend that the ICANN Board prioritize and support community work in this area to enhance safeguards and trust due to the negative impact of DNS Security Abuse on consumers and other users of the Internet. **CCT priority:** Prerequisite (provisions to address systemic DNS Security Abuse should be included in the baseline contract for any future new gTLDs) **CCT directed to**: The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization and the Subsequent Procedures PDP WG

Board action/rationale:

The Board acknowledges the remit and roles of the different parts of the ICANN community and notes that since January 2023, ICANN org has been actively engaged in a contract amendment process with the Registries and Registrars to add a clearly defined obligation to mitigate or disrupt DNS abuse in each agreement. The recommendation calls for outcomes that are contingent on community work.

The recommendation states that ICANN should establish thresholds of abuse at which compliance inquiries are automatically triggered, with a higher threshold at which registrars and registries are presumed to be in default of their agreements. However, the Board notes 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 recognizes the ICANN org assessment that a potential DNS Abuse Dispute Resolution Policy would not be an effective means to enforce policies and deter against DNS Security Abuse as any action on DNS abuse should be enforced in a timely manner.

It is the view of the Board that the community should determine what policy work is needed and how it wishes to prioritize such efforts to enhance safeguards and trust due to the negative

impact of DNS Security Abuse on consumers and other users of the Internet. As discussed above, ICANN has included efforts to combat DNS abuse in partnership with relevant industry partners in ICANN's strategic plan, has made significant progress to date and is encouraged by the community dialogue.

Therefore, considering the outcome of the extensive analysis of each of the components of this Recommendation, while acknowledging that this Recommendation was marked as a "prerequisite" by the Review Team and remaining fully supportive of compliance actions towards registries and registrars who fail to meet their contractual obligations, as well as of any community work to enhance DNS abuse safeguards, the Board rejects this recommendation.

ICANN org assessment:

ICANN's working definition of DNS abuse is: "DNS abuse includes five broad categories of harmful activity: Phishing, Malware, Botnet Command and Control, SPAM when used as a vector, and Pharming." The Board recognized this working definition is neither an exhaustive list nor a criteria-based definition; however this definition brings together a set of agreed-upon DNS Security Threats to which policy and mitigation work within ICANN can take place immediately, while or if definitions continue to be debated. As established in the November 2022 exchange of letters between the Contracted Party House (CPH) and ICANN org, there are ongoing efforts between ICANN org, the Registrar Stakeholder Group (RrSG), and Registries Stakeholder Group (RySG) to pursue enhancements to the DNS abuse obligations contained in the Registrar Accreditation Agreement (RAA) and Base gTLD Registry Agreement (RA). A critical aspect of the proposal by the RySG and RrSG to strengthen existing abuse-related obligations is to arrive upon a definition of the forms of DNS abuse that fall within ICANN's mandate.

ICANN org strives to mitigate DNS abuse in accordance with ICANN Bylaws and policies. The org maintains a three-pronged approach to mitigating DNS abuse, which includes contributing data and expertise to fact-based discussions, providing tools to the ICANN community, and enforcing contractual obligations with registries and registrars.

ICANN's Contractual Compliance function actively enforces the relevant contracted parties agreement provisions and has conducted audits specifically focused on various anti-abuse provisions. Examples of the abuse-related provisions enforced by ICANN Compliance include Specification 6 4.1, Specification 11 3(a) and 3(b) of the Registry Agreement (RA), as well as Section 3.18 of the Registrar Accreditation Agreement (RAA). For example, both registrars and registries must publish on their website information about how to submit a report of abuse about a domain name and an email address to collect reports of abuse. Registrars are required to investigate and respond appropriately to reports of abuse.

Similarly, ICANN Contractual Compliance enforces other contractual obligations which often play a role in investigations related to DNS abuse. For example, those related to Registration Data (WHOIS) accuracy in Section 3.7.8 and the Whois Accuracy Program Specification of the RAA (ICANN Contractual Compliance often receives reports of inaccurate data associated with allegedly abusive domain names); and those related to zone file third-party access requests (often submitted by security researchers who investigate and help combat DNS abuse) in Specification 4, Section 2 of the RA.

ICANN is currently engaged in contractual negotiations with the registrars and registries to further strengthen requirements related to DNS abuse. A critical aspect of this work is to arrive upon a definition, for inclusion in contracts, of the forms of DNS abuse that fall within ICANN's mandate. "DNS Abuse" for the purposes of the contracts between ICANN and the contracted parties will be defined as malware, botnets, phishing, pharming, and spam (when spam serves as a delivery mechanism for the other forms of DNS Abuse listed prior) as those terms are defined in Section 2.1 of SAC115. One of the intended outcomes of the proposed amendments is for ICANN Contractual Compliance to expand its authority to enforce appropriate DNS Abuse mitigation actions by the Contracted Parties.

This recommendation suggests that ICANN org should trigger compliance inquiries based on the volume or percentage of names that appear via Reputation Block List (RBL) feeds. ICANN org notes that domain names and volumes that appear in RBLs as suspected cases of DNS abuse are not necessarily equivalent to those that are confirmed and evidenced. Additionally, as has been noted in the discussions of the proposed contractual amendments, DNS Abuse mitigation requires contextual analysis. When considering metrics, measurements or thresholds, there also should be consideration for the distinction between domain names that are being primarily used for DNS Abuse from those domain names where the website has been hacked or otherwise compromised and is being used as a vector for DNS Abuse without the knowledge or consent of the registrant. Collateral damage is a particularly important consideration for

compromised domains situations. In these cases, direct suspension of the domain by the registrar or registry operator may not be the appropriate mitigation, as suspension will cut off access to all legitimate content as well as render any associated email and other services with the domain inaccessible.

Setting such generalized "thresholds of abuse" 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. Moreover, the ability to collect independently verifiable metrics demarcating abuse thresholds is a core part of this recommendation. There is a distinction between reported cases of DNS abuse which might be sourced via (RBL) feeds, for instance, and evidenced DNS abuse which would be the outcome of a registry/registrar/law enforcement's abuse investigation. While the DNS industry has greatly progressed in its ability to generate independently verifiable metrics of suspected abuse, evidenced abuse metrics (i.e. involving cases of confirmed DNS abuse that should be mitigated) still predominantly require human intervention.

The concept of a DNS Abuse Dispute Resolution Policy (DADRP) that sets out the legal framework for the resolution of DNS abuse-related disputes between a domain name registrant and a third party, akin to the Uniform Domain Name Dispute Resolution Policy (UDRP), appears to clash with expediency required to address and mitigate validated claims of DNS abuse. Acting on DNS abuse should be done in a matter of seconds/minutes/hours/days whereas any Resolution Policy would require more time.

SSR2 REC #12.1	**Recommendation language**: ICANN org should create a DNS Abuse Analysis advisory team composed of independent experts (i.e., experts without financial conflicts of interest) to recommend an overhaul of the DNS Abuse Reporting activity with actionable data, validation, transparency, and independent reproducibility of analyses as its highest priorities. **SSR2 priority:** Medium **SSR2 directed to**: ICANN org

Board rationale/action:

The Board notes that the community continues its discussions over DNS abuse mitigation. The Board is fully supportive of this effort and remains committed to this important work through facilitation and the convening of diverse relevant groups with diverse viewpoints. Notably, the Domain Abuse Activity Reporting (DAAR) project is a system for studying and reporting on domain name registration and security threats across top-level domain (TLD) registries which was developed thanks to community input.

The Board notes the absence of issues that would justify an overhaul of DNS Abuse Reporting activity, as suggested by the SSR2, and rejects this recommendation. The Board encourages ICANN org to continue its work to evolve the DAAR initiative based on further community feedback.

ICANN org assessment:

The community continues its discussions over DNS abuse mitigation. Discussions include questions around the definitions and scope of DNS security threats that can be considered as within ICANN's remit and the extent to which policy or other community work may be required to supplement efforts already underway, such as industry-led initiatives.

The recommendation language does not identify any specific issues that would justify an overhaul of DAAR or the value added by creating such a working group. Public comments from both the registry and registrar stakeholders question the value of the solution as proposed and share concerns as it relates to its cost and benefits. ICANN org concurs with this assessment. ICANN org continues to welcome and act upon detailed feedback that can help improve the project. In a May 2021 blog posting, for instance, ICANN org outlined current and planned evolution of the initiative based on concrete suggestions received on the DAAR project documentation, report coverage, and data visualization, among others.

SSR2 REC #12.2	**Recommendation language**: ICANN org should structure its agreements with data providers to allow further sharing of the data for noncommercial use, specifically for validation or peer reviewed scientific research. This special no-fee non commercial licence to use the data may involve a time delay so as not to interfere with commercial revenue opportunities of the data provider. ICANN org should publish all data-sharing contract terms on the ICANN website. ICANN org should terminate any contracts that do not allow independent verification of methodology behind blocklisting. **SSR2 priority:** Medium **SSR2 directed to**: ICANN org

Board rationale/action:

The Board notes the value of the Domain Abuse Activity Reporting (DAAR) project and that the majority of data feeds used in the DAAR reports can be accessed freely and directly by the academic/non-commercial community without ICANN org serving as an intermediary.

The Board also notes that the recommendation's suggested approach of terminating contracts or requiring specialized licensing terms may result in negative consequences impacting the total number of data feeds ICANN org is allowed to access going forward and the corresponding quality of data utilized to generate DAAR reports.

Therefore, the Board rejects this recommendation.

ICANN org Assessment:

The majority of the data feeds used in the DAAR reports are already freely and directly available to the academic/non-commercial community without ICANN org having to serve as an intermediary. The terms regarding these free data feeds are governed by the requirements of the individual data feed providers independently and apply to all licensees equally. Of note, the redistribution of such feeds (even with the introduction of any time-delays) extends beyond the terms of ICANN org's contract with the independent consultant hired to generate the DAAR reports, as would the release of the case-level data which would presumably be required for "independent verification of methodology behind blocklisting".

ICANN org uses multiple sources of reputation blocklist data for various purposes, DAAR being one of them. Some of these purposes, such as the Domain Name Security Threat Information Collection and Reporting (DNSTICR) project, are smaller scale projects and hence could benefit from using the Reputation Block Lists (RBL) free data streams. Due to its nature of publishing data on a daily basis, DAAR cannot benefit from that. However, most of the data used in DAAR can still be obtained by any user from its source provider, as most of them are for free.

While ICANN org could negotiate improved licensing terms to include redistribution or visibility to case-level data at no incremental cost for non-commercial use, this should not be treated as a precondition to data feed provider selection, as is being suggested in the recommendation language. The recommendation's suggested approach of terminating contracts or requiring specialized licensing terms may result in negative consequences impacting the total number of data feeds ICANN org is allowed to access going forward and the corresponding quality of data utilized to generate DAAR reports.

The reputation feeds used for the DAAR system must satisfy a number of stringent criteria, including their reputation in the operational security community and academia for accuracy and a very low false-positive rate, widespread adoption by large numbers of users, good practices for maintaining lists, high availability, size and quality of detection infrastructure, and use of classifications or sub-classifications to place domains into the applicable security threat categories.

As it relates to publishing all data-sharing contract terms on the ICANN website, this is an operational matter. No specific issue has been cited that would be solved through the publication of all data-sharing contract terms.

Moreover, when evaluating this component of SSR2 12.2, there appears to be a considerable degree of misalignment between the language of the recommendation and the measures outlined to indicate its successful implementation and effectiveness. Specifically, while the recommendation asks that the org focuses on the publication of data-sharing contract terms,

successful implementation is made contingent on the introduction of “metrics that produce actionable, accurate, and trustworthy data”. Effectiveness of the recommendation is further linked to a goal of having “all of the data available to ICANN org is also available to the community and independent researchers, perhaps with a time delay, to provide validation and feedback”.

SSR2 REC #12.3	**Recommendation language**: ICANN org should publish reports that identify registries and registrars whose domains most contribute to abuse. ICANN org should include machine-readable formats of the data, in addition to the graphical data in current reports. **SSR2 priority:** Medium **SSR2 directed to**: ICANN org

Board rationale/action:

The Board supports ICANN org’s assessment of this Recommendation, more precisely that the concept of abuse, as mentioned in the Recommendation language, goes beyond ICANN’s remit, that careful considerations are required to distinguish between reported cases of DNS Abuse and evidenced cases of DNS Abuse, that prior engagement with the community could be helpful in designing a procedure that supports positive outcomes, and that the successful implementation and effectiveness measures for this Recommendation imply additional actions. For those reasons, the Recommendation is rejected.

The Board encourages ICANN org to continue in its efforts to report security threat activity to the ICANN community, continue the dialogue with the contracted parties and support their actions in combating DNS Abuse, which may include publication of new reports and release of datasets that capture more specific aspects of the DNS Abuse landscape.

ICANN org assessment:

ICANN org assessed the key elements of the Recommendation 12.3 in depth.

First, the recommendation language suggests a much broader, undefined concept of “abuse”, as compared to DNS Abuse, which would go beyond ICANN’s remit, visibility, and competencies.

Secondly, when it comes to the possible publication of reports that identify registries and registrars, careful considerations are required to distinguish between reported cases of 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 the investigations by contracted parties or Law Enforcement and Investigations (LEI) agencies. While the DNS industry has greatly progressed in its ability to generate independently verifiable metrics of suspected abuse, evidenced abuse metrics (e.g., involving cases of confirmed DNS Abuse that should be mitigated) still predominantly require human intervention. It is worth highlighting that ICANN org does not have full visibility of 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, as well as any particulars with respect to the aspects of machine-readability and graphical presentation of outputs.

Lastly, the language of the recommendation and the measures outlined to indicate its successful implementation and effectiveness seem to be misaligned. While the recommendation refers to reports, successful implementation is made contingent on the data being actionable, while leaving unstated which parties would need to act upon the data, and in what specific manner. Effectiveness of the recommendation is further linked to a goal of having “all of the data available to ICANN org also available to the community and independent researchers, perhaps with a time delay, to provide validation and feedback.” For data to be actionable from a DNS Abuse mitigation perspective, it must be provided in a timely manner, supported by evidence, and would only be “actionable” to the relevant contracted parties where the said instance of DNS Abuse is occurring. Per ICANN org’s assessment, this is a different challenge and task than producing public reporting.

It is worth noting that enhancing the transparency and accountability of any DNS Abuse analysis and reporting, as intended by Recommendation 12.3, remains a key objective for ICANN org. Over the years, org has put into place several initiatives to help inform community discussions and support the contracted parties in combating DNS Abuse, as appropriate.

More specifically, ICANN Compliance has been publishing detailed metrics on DNS abuse complaints since 2020 and continues to evolve its reporting. Most recently, in March 2022, ICANN Compliance released new reports on ICANN.org to better capture the current landscape of complaint volumes and related compliance actions. Data tables are accessible on ICANN.org for review and available for extraction and further analysis.

In addition, the Domain Abuse Activity Reporting (DAAR) project offers a platform for studying concentrations of security threats (DNS abuse) in domain names within the gTLD space in an aggregated and anonymous manner, and provides coverage of those ccTLDs that have voluntarily adhered to the project. In a 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. 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.

SSR2 REC #12.4	**Recommendation language**: ICANN org should collate and publish reports of the actions that registries and registrars have taken, both voluntary and in response to legal obligations, to respond to complaints of illegal and/or malicious conduct based on applicable laws in connection with the use of the DNS. **SSR2 priority:** Medium **SSR2 directed to**: ICANN org

Board rationale/action:

The Board notes that there are existing efforts within ICANN org as well as by third-parties to collect and provide some of the data similar to what the recommendation suggests. Recognizing that the recommendation requires changes to the contractual obligations, would create challenges for ICANN org, the registries, and registrars to define a reporting schema that would be globally applicable, and that the benefits and value of producing such reports are unclear, the Board rejects this recommendation.

ICANN org assessment:

SSR2 12.4 overlaps with CCT recommendation 20, which the Board has already previously indicated lies beyond ICANN org's "authority to demand information that registries are not required to collect or submit to ICANN org".

It was determined that an alternative means of data collection, as suggested by CCT Recommendation 20, could be conducted via a voluntary pilot survey amongst contracted parties. ICANN org has already engaged the RySG about voluntary reporting of DNS Abuse handling, though those efforts were tabled to prioritize the development of contractual amendments to obligate registries and registrars to mitigate DNS Abuse. That scope would be significantly less than the recommendation provides and should not be conflated with achieving all aspects of this recommendation or its success criteria.

Considerations for this effort may include the following: a large subset of reported DNS abuse relates to content and "content layer" related services which fall beyond ICANN's remit. Further, representative datasets at the scale of millions of DNS abuse reports and impacted domain names are currently already available via cross referenced third-party sources such as Trusted Notifier programs, Reputation Block Lists (RBLs), or abuse feeds.

The scope outlined in this recommendation requires reports on actions taken in response to voluntary and legal obligations from more than 1,400 distinct gTLD registry operators, and registrars operating across a minimum of 84 countries. The recommendation also assumes the willingness of the registries and registrars to share this kind of data as well as that this kind of sharing would be possible under their legislative environment.

Beyond the wide variety of international, national, and local legal obligations to which gTLD registry operators and registrars are subject, collation and reporting of such data would be complicated by a lack of consistency in the definition of regulatory framework across countries as to what constitutes “illegal and/or malicious conduct” pertaining to the use of the DNS.

Both the Registry and Registrar Stakeholder groups have questioned the incremental value of the report being proposed in this recommendation. Indeed, there are already efforts from within ICANN org (i.e., via the DAAR initiative) and by third-parties (e.g., via the efforts of the DNS Abuse Institute, IQ Global, and Realtime Registrar, among others) to collect and provide information and functionality similar to that noted in the recommendation text.

Likewise, public comments from both the registry and registrar stakeholders question the value of the solution as proposed and share concerns as it relates to its cost and benefits. ICANN org concurs with this assessment and concludes that at least some of the data required to fulfil this recommendation would be infeasible or impractical to not only collect but also to organize for analysis either by ICANN org or the community. Thus, the value added is questionable and the costs would be considerable.

SSR2 REC #13.1	**Recommendation language**: ICANN org should establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties. The system would purely act as an inflow, with ICANN org collecting and processing only summary and metadata, including timestamps and types of complaint (categorical). Use of the system should become mandatory for all generic top-level domains (gTLDs); the participation of each country code top-level domain (ccTLD) would be voluntary. In addition, ICANN org should share abuse reports (e.g., via email) with all ccTLDs. **SSR2 priority:** High **SSR2 directed to**: ICANN org

Board rationale/action:

The Board notes that this recommendation calls for ICANN's gTLD registries and accredited registrars to be required to use a centralized DNS abuse complaint portal. Such an obligation would necessitate a change to ICANN’s current contracts with registries and registrars which the ICANN Board cannot unilaterally dictate.

The Board also notes that ICANN org does not view a central abuse complaint processing system as an existing gap that it needs to fill in the marketplace and expend its resources upon at this time, and that per the ICANN org assessment, there is an existing tool that offers a service of centralized intake and distributing abuse reports. Therefore, the Board rejects this recommendation.

ICANN org assessment:

Establishing a centralized abuse complaint reporting system that is mandatory for use by the gTLD registries and registrars would best be a topic for consideration by the GNSO as a potential outcome of policy development. A Review Team cannot mandate binding obligations on Contracted Parties unlike approved outcomes of GNSO PDPs, and the ICANN Board cannot unilaterally dictate policy. When the GNSO considered and recommended the implementation of a centralized system for requesting registration data on an interim basis (the Registration Data Request System currently in development), the GNSO chose to not mandate the use of the tool by all registries and registrars.

This recommendation is similar to a recommendation by the SSAC in SSAC 115, that was put forth to the community as a whole for consideration rather than to the ICANN Board for action.

Moreover, the Registries Stakeholder Group (RySG) and the Registrars Stakeholder Group (RrSG) expressed concerns regarding the scoping and incremental value of the proposed portal.

Since this recommendation was made by the SSR2 and a similar recommendation for a centralized abuse reporting tool by the SSAC, the Public Interest Registry's DNS Abuse Institute has developed a tool, Netbeacon, that provides a similar service of centralized intake and distributing abuse reports.

As noted by the RrSG: “As the deficiency this proposal will address has not been identified, and the average operational cost could be many multiple millions of dollars annually, the ICANN Board should reject this recommendation.” ICANN org would concur with the assessment, as it does not view a central abuse complaint processing system as an existing gap that it needs to fill in the marketplace and expend its resources upon at this time.

SSR2 REC #13.2	**Recommendation language**: ICANN org should publish the number of complaints made in a form that allows independent third parties to analyze the types of complaints on the DNS. **SSR2 priority:** High **SSR2 directed to**: ICANN org

Board action/rationale:
The Board acknowledges ICANN Compliance’s publication of detailed metrics on DNS abuse complaints and the evolution of such reporting, including the new reports that better capture the current landscape of complaint volumes and related compliance actions.

The Board notes that the existing publication format of data and metrics on ICANN.org fulfils the intent of the recommendation. The Board remains fully supportive of further initiatives that can inform community work and discussions by providing relevant datasets where available.

Therefore, the Board approves the recommendation as fully implemented.

ICANN org assessment:
The Recommendation’s success measures appear to cover elements that go beyond the Recommendation. Board action should be taken on the recommendation language per se.

Since 2020, ICANN Compliance has published detailed metrics on DNS abuse complaints and continued to evolve its reporting. Most recently, in March 2022, ICANN Compliance released new reports on ICANN.org to better capture the current landscape of complaint volumes and related compliance actions.

This enhanced reporting, which was made possible by the expanded data available in the newly launched Salesforce-based ticketing system (NSp Compliance), provides monthly-level data on the complaints received, the obligations enforced, and the process through which the obligations are being enforced. Additional reporting on DNS abuse complaint type details is also available on a rolling twelve month period. The data tables are accessible on ICANN.org for review and available for further analysis.

SSR2 REC #14.2	**Recommendation language**: To enable anti-abuse action, ICANN org should provide contracted parties with lists of domains in their portfolios identified as abusive, in accordance with SSR2 Recommendation 12.2 regarding independent review of data and methods for blocklisting domains. **SSR2 priority:** High **SSR2 directed to**: ICANN org

Board action/rationale:

The Board notes that since January 2023, ICANN org has been actively engaged in a contract amendment process with the Registries and Registrars to add a clearly defined obligation to mitigate or disrupt DNS abuse. Progress in this regard will support the evolution of ICANN Compliance’s toolkit to appropriately respond to contracted parties’ failures to address DNS Abuse.

While the Board encourages ICANN org to continue to innovate and find ways to support the contracted parties in combating DNS Abuse, which may include reporting instances of well evidenced DNS Abuse to registrars and registries, the Board acknowledges the remit and roles of the different parts of the ICANN community.

However, as the language in SSR2 14.2 is not confined to DNS abuse, but rather to much more broadly defined forms of abuse, which may encompass forms of abuse that go beyond org's remit (as well as its visibility and competencies), the Board rejects this recommendation.

ICANN org assessment:

The language in SSR2 14.2 is not confined to DNS abuse, but rather to much more broadly defined forms of abuse, i.e."ICANN org should provide contracted parties with lists of domains in their portfolios identified as abusive", which would encompass those which would be beyond org's remit (as well as its visibility and competencies). The RrSG called for the Board to reject this recommendation as it is "not within ICANN's remit to police the Internet for abuse."

While the standalone recommendation 14.2 asks that the org "provide contracted parties with lists of domains in their portfolios identified as abusive", successful implementation is made contingent on an entirely unaligned goal of ICANN Compliance having "the tools to appropriately respond to contracted parties failing to respond to DNS abuse, specifically the existence of anti-abuse related obligations in all relevant contracts and agreements", as well as the "use of those tools to deal with egregious policy violations on the part of contracted parties".

ICANN org measures specific security threats related to domain names through several projects, including the Domain Name Security Threat Information Collection and Reporting (DNSTICR) project, and Domain Abuse Activity Reporting System (DAAR), both of which have a publication/reporting element. Commercial solutions with DNS Abuse reporting capabilities at the individual domain level are also being offered by private sector entities, including by ICANN contracted parties.

--

The Board takes action on contractual compliance activities related SSR2 Recommendations 9.2 and 9.3.

SSR2 REC #9.2	**Recommendation Language**: ICANN org should proactively monitor and enforce registry and registrar contractual obligations to improve the accuracy of registration data. This monitoring and enforcement should include the validation of address fields and conducting periodic audits of the accuracy of registration data. ICANN org should focus their enforcement efforts on those registrars and registries that have been the subject of over 50 complaints or reports per year regarding their inclusion of inaccurate data to ICANN org. **SSR2 priority:** High **SSR2 directed to:** ICANN org

Board action/rationale:

The Board notes that ICANN org can pursue accuracy of registration data according to the provisions included in the Registry Agreement and Registrar Accreditation Agreement, and that at present extensive checks are conducted to verify the accuracy of registration data. The SSR2 recommendation seeks the enforcement of specific compliance requirements (i.e., address fields) regarding data accuracy that are not part of the current registry and registrar contractual framework. The recommendation calls for work or outcomes that would require the Board to unilaterally modify ICANN's agreements with registries and registrars, or would be contingent on community work. Changes to contracted party agreements would be a matter of policy or a result of voluntary negotiations between ICANN org and contracted parties.

The Board wishes to note the extensive provisions on data accuracy already in place in the current Registry and Registrar agreements, and ICANN Contractual Compliance actions that are independent from the number of yearly complaints.

The Board notes the SSR2 Implementation Shepherds' clarification that ICANN org should provide details of what Compliance does in this area, with supporting public documentation and summary results of audits, and that ICANN's Contractual Compliance reports are available at https://www.icann.org/resources/compliance-reporting-performance .

The Board also acknowledges that there are ongoing community discussions on registration data accuracy that may lead to the introduction of further data accuracy checks.

As a result, the Board rejects SSR2 Recommendation 9.2.

ICANN org assessment:

Relevant requirements related to the accuracy of registration data in the contracted parties' agreements include:

- Base Registry agreement (RA) Art. 2.11 and Art. 2.2;
- Registrar Accreditation Agreement (RAA) Art 3.7.8. in addition to complying with the provisions of the WHOIS Accuracy Program. Moreover, the RAA requires registrars to take steps to ensure the accuracy of registration data associated with their sponsored gTLD domain names. In particular, the RAA includes obligations relating to the investigation of allegations of inaccuracy, contact information verification, and data format validation.

ICANN org enforces Registry and Registrar obligations through its Contractual Compliance team. Data accuracy obligations and ICANN org's enforcement of these obligations have not changed post-GDPR. However, the volume of complaints has diminished significantly post-GDPR.

Following the Board's adoption of the Temporary Specification for gTLD Registration Data, many contracted parties now redact personal data within gTLD registration data in public Registration Data Directory Services. As a result, there is less visibility of registrant contact data in public RDDS, and potential complainants often lack direct access to registration data as a result of the GDPR, making it much more difficult to identify instances of registration data inaccuracy or to take action to correct them.

For valid complaints received, Contractual Compliance initiates an investigation into the registrar's compliance with the contractual requirements explained above, including the obligation to take reasonable steps to investigate the claimed inaccuracy. Contractual Compliance will typically close an inaccuracy case when the registrar demonstrates compliance with the investigation and validation or verification requirements, which may include the suspension or cancellation of the domain name registration.

ICANN Compliance conducts regular audits of Registries and Registrars to ensure their compliance with the Registry Agreement (RA) and Registrar Accreditation Agreement (RAA). The RAA audit program includes a review of the requirements of RAA 3.7.8 relating to Registrar compliance with the Whois Accuracy Program Specification. Information regarding Contractual Compliance audits can be found here https://www.icann.org/resources/pages/audits-2012-02-25-en. The latest audit reports are published at https://www.icann.org/resources/pages/compliance-reports-2023 while the latest contractual compliance dashboard is available at https://features.icann.org/compliance/dashboard/2023/0423/report. The audits include confirming that registrars comply with their Whois Accuracy Program Specifications obligations (validation and verification).

With reference to the complaint threshold suggested by the Recommendation, ICANN Contractual Compliance's role is to bring registrars into compliance with the Registrar Accreditation Agreement (RAA), regardless of the number of yearly complaints. Once a complaint has been determined to be valid, ICANN Compliance follows ICANN's Contractual Compliance Approach and Processes. The Informal Resolution process allows ICANN's contractual compliance team to work closely with Registrars and Registries to help them understand their contractual obligations and overcome any contractual compliance challenges and issues they may have. ICANN attempts to resolve contractual compliance matters informally before pursuing formal remedies available under the agreements. ICANN does not provide details regarding contractual compliance activities in the informal resolution phase, in the interest of facilitating open dialogue and resolution. In certain cases, when ICANN determines that a contracted party must resolve a critical issue immediately, an escalated notice is sent. Failure to adequately respond to an escalated notice may result in a breach notice.

The Formal Resolution process, also known as the Enforcement Process, commences when contracted parties have either failed to sufficiently collaborate during the Informal Resolution process or otherwise continue to be noncompliant after attempts at informal resolution. Notices sent during the Formal Resolution process are published, and ICANN updates the progress of each enforcement action.

SSR2 REC #9.3	**Recommendation Language**: ICANN org should have compliance activities audited externally at least annually and publish the audit reports and ICANN org response to audit recommendations, including implementation plans. **SSR2 priority:** High **SSR2 directed to:** ICANN org

Board action/rationale:

The Board acknowledges that Recommendation 9.3 could have benefited from more clarity, as confirmed by SSR2 Implementation Shepherds.

The Board appreciates the Recommendation's intent, as well as ICANN Compliance's continued commitment to transparency, including through publishing detailed metrics on its operations on a regular basis, and its commitment to continuous improvement through internal reviews to assess and improve on its operations.

The Board also acknowledges the Registry Stakeholder Group's views, as expressed in the public comment on the SSR2 Final Report, that any recommendations related to ICANN Contractual Compliance should be connected to specific contractual terms and tied to a specific problem statement. In addition, the Board notes the Registrar Stakeholder Group's comment that ICANN Contractual Compliance has resources in place to oversee and ensure consistent and accurate complaint processing.

The Board recognizes that Compliance's objectives include fully and efficiently addressing third-party complaints, proactive enforcement of contractual obligations, and registry and registrar audits against their contractual obligations. The Board recognizes ICANN org's assessment that the time and resources requested for running yearly, external audits will not lead to any desired improvement of procedures and processes that at present are running in accordance with the principles set in the contracted parties' agreements.

As a result, the Board rejects SSR2 Recommendation 9.3.

ICANN org assessment:

As prompted by the July 2021 Board action on the SSR2 Final Report, ICANN org reached out to the SSR2 Implementation Shepherds to obtain clarification on what would be envisioned for an audit, including against which criteria and the rationale for an external auditor.

The Shepherds acknowledged that the recommendation could have been clearer and indicated that they had the ISO 9000 set of quality management systems standards in mind for setting goals and strategies, and that the main objective is to have third-party audits conducted against the relevant quality management program.

Community input on this Recommendation included supportive comments as well as concerns. The Registry Stakeholder Group' views expressed in the public comment on the SSR2 Final Report stated that any recommendations related to ICANN Contractual Compliance should be connected to specific contractual terms and tied to a specific problem statement. In addition, the Registrar Stakeholder Group commented that ICANN Contractual Compliance has resources in place to oversee and ensure consistent and accurate complaint processing.

ICANN Compliance demonstrates its commitment to transparency by regularly publishing reports with detailed metrics on its operations. While these reports do not currently include data on performance against internally-developed operational goals, they do provide clear visibility into the day-to-day operations of ICANN Compliance. ICANN Compliance will look for ways to publish more information on its operational goals, its performance in meeting them as well as its efforts to continuously improve its operational effectiveness.

However, looking at the objective of this Recommendation both from an operational and cost/benefit perspective, ICANN org believes that the time and resources requested for running yearly, external audits will not lead to any desired improvement of procedures and processes that at present are running in accordance with the principles set in the contracted parties' agreements.