Staff Report of Public Comment Proceeding

Second Security, Stability, and Resiliency (SSR2) Review Team Final Report	
Publication Date:	10 May 2021
Prepared By:	Jennifer Bryce

Public Comment Proceeding	
Open Date:	28 January 2021
Close Date:	8 April 2021 (extended from 9 March 2021)
Staff Report Due Date:	10 May 2021 (extended from 23 March 2021 and 22 April 2021)

Important Information Links
Announcement
Public Comment Proceeding
View Comments Submitted

Staff Contact:	Jennifer Bryce	**Email:**	jennifer.bryce@icann.org

Section I: General Overview and Next Steps

The Security, Stability, and Resiliency (SSR) Review is one of the four Specific Reviews anchored in Section 4.6 of the ICANN Bylaws. These specific reviews are conducted by community-led review teams which assess ICANN's performance in reaching its commitments. Reviews are critical to helping ICANN achieve its mission as detailed in Article 1 of the Bylaws.

On 25 January 2021 the second Security, Stability, and Resiliency Review Team (SSR2) submitted its final report to the ICANN Board. The SSR2 Final Report contains 63 recommendations in the following areas:

- Implementation of the recommendations from the first SSR Review (SSR1), and the intended effects;
- Key stability issues within ICANN;
- Contracts, compliance, and transparency around Domain Name System (DNS) abuse; and
- Additional SSR-related concerns regarding the global DNS.

Next Steps

Per the Bylaws (Section 4.6(a)(vii)(C)), the Board shall consider the SSR2 Final Report within six months of receipt, by 25 July 2021. The Board will consider a feasibility analysis and impact assessment of the implementation of recommendations, which will take into account initial cost and resource estimates and dependencies with other ongoing efforts within the community, and the report of the Public Comment submissions received. The Board will then direct implementation of the approved recommendations and provide written rationale for the decision if any recommendations are not approved.

A comprehensive analysis of comments will be published in due course and appended to this document.

Section II: Contributors

At the time this report was prepared, a total of nineteen (19) community submissions had been posted to the forum. The contributors, both individuals and organizations/groups, are listed below in chronological order by posting date with initials noted. To the extent that quotations are used in the foregoing narrative (Section III), such citations will reference the contributor's initials.

Name	Submitted by	Initials
gTLD Registries Stakeholder Group	Elizabeth Bacon	RySG
Verisign	Burt Kaliski	Verisign
Public Interest Registry	Elizabeth Bacon	PIR
Security and Stability Advisory Committee	Danielle Rutherford	SSAC
Messaging, Malware, and Mobile Anti Abuse Working Group	Amy Cadagin	M3AAWG
Afnic	Marianne Georgelin	Afnic
Article 19	Ephraim Percy Kenyanito	Article 19
Internet Infrastructure Coalition	Christian Dawson	i2Coalition
International Trademark Association	Lori Schulman	INTA
Tucows	Reg Levy	Tucows
GNSO Council	Berry Cobb	GNSO
Noncommercial Stakeholder Group	Tomslin Samme-Nlar	NCSG
Namecheap, Inc.	Owen Smigelski	Namecheap
Crypto4A Inc.	Jim Goodman	Crypto4A
Intellectual Property Constituency	Dean Marks	IPC
Governmental Advisory Committee	GAC Support Team	GAC
Business Constituency	Steve DelBianco	BC
Registrar Stakeholder Group	Zoe Bonython	RrSG
At-Large Advisory Committee	ALAC Support Staff	ALAC

Section III: Summary of Comments

General Disclaimer: This section intends to summarize broadly and comprehensively the comments submitted to this Public Comment proceeding but does not address every specific position stated by each contributor. The preparer recommends that readers interested in specific aspects of any of the summarized comments, or the full context of others, refer directly to the specific contributions at the link referenced above (View Comments Submitted).

The SSR2 Final Report contains 63 recommendations, grouped into 24 issues. Some commenters chose to make comments on individual recommendations, while others made comments by recommendation group.

While comments on the report as a whole represent a significant diversity of views, many of the overarching comments touch on common themes. For ease of reference, overarching comments are summarized below by theme. Comments on individual recommendations are summarized below according to the recommendation groups.

Overarching comments summarized by theme

Comments on the SSR2 Final Report represent a significant diversity of views. In addition to comments on the individual recommendations and/or recommendation groups, most commenters made general or overarching comments about the report as a whole. These overarching comments are summarized here by the following themes:

- Statements of overall support for the recommendations
- Concern that some recommendations are contrary to ICANN's multistakeholder model
- Concern that some recommendations repeat or significantly overlap with ongoing work
- Concern about lack of contracted party representation on the SSR2 Review Team and consideration of prior input
- Other overarching comments

Statements of overall support for the recommendations

INTA: "INTA is generally supportive of the recommendations within the Final Report and provides…specific comments regarding certain individual recommendations of most importance to INTA members."

BC: "The BC strongly supports this review process and the productive suggestions it has yielded, in both SSR1 and SSR2. It now is critical that the Board accept SSR2 recommendations as documented and take responsibility for driving expeditious and effective implementation of all recommendations."

ALAC: "We are pleased to state our support for or lack of objects to each of the recommendations in the SSR2 Final Report. Our comments below are intended to highlight recommendations and other elements of particular importance or relevance, to help guide ICANN in adopting and implementing the Final Report."

"ALAC agrees with the adoption of SMART (Specific, Measurable, Assignable, Relevant and Trackable) criteria and objectives, and with the SSR2's observation that SMART criteria should be used by both the SSR1 implementation team and by future SSR Review Teams."

"ALAC notes an important theme that runs through most, if not all, recommendations: ICANN must strive to adopt industry standard and state-of-the-art practices for technical and technology-driven organizations. While ICANN is relatively small in size, it is a critical actor in global Internet security and thus in information security (InfoSec) more broadly. We recognize that ICANN has significantly professionalized its operations over the years, but more needs to be done to keep pace in a relentlessly evolving world."

IPC: "Overall, the IPC strongly supports the recommendations outlined in the Final Report."

Concern that some recommendations are contrary to ICANN's multistakeholder model

RySG: "As the RySG noted in response to the SSR2 Draft Report, several recommendations suggest direct changes to the Registry Agreement. Changes to Registry Agreements may

only be made through the policy development process or by triggering a formal negotiation and amendment process" [emphasis removed].

"We would like to urge the Board to consider the wealth of DNS Abuse work that is ongoing in the community and to not accept recommendations that would duplicate those efforts or risk to undo progress made in recent months" [emphasis removed].

"The Report includes recommendations directing the Board to mandate the inclusion of third party interests in contractual negotiations. The RySG encourages discussion and cooperation on issues of concern. This unilateral direction is outside the scope of the Board's power. In addition, implementation of recommendations to include or represent third party interests in contractual negotiations would violate existing terms in the Registry Agreement. The RySG urges the ICANN Board to reject recommendations where the implementation would represent a violation of contractual provisions or ICANN policy development processes" [emphasis removed]**.**

PIR: "Several recommendations in the Report recommend that ICANN attempt to make unilateral changes to the Registry Agreements. Changes to Registry Agreements of this sort should only be made via the GNSO Policy Development Process resulting in a Consensus Policy or via triggering a formal negotiation process under the terms of the Registry Agreement. Further, several SSR2 recommendations would represent violations of the terms of the Registry Agreement which governs the inclusion of third-party interests in contractual negotiations and how temporary policies/specifications may be used by ICANN… PIR does not support recommendations that suggest unilateral contractual changes by the ICANN Board as this action is not supported by a procedural or contractual mechanism."

Tucows: "The Tucows family of registrars notes the long-term efforts that the Registrars and Registries have undertaken with ICANN Org in order to attempt to negotiate new contractual clauses that other ICANN Community-led efforts have recommended including, but not limited to, the current renegotiation of the RAA and the ongoing discussions surrounding a data processing addendum to both the RAA and the RA. The existence and nature of these negotiations clearly indicates that ICANN Org and the Contracted Party House continue to work together to make necessary contractual amendments and that no other party should be involved in that process."

Namecheap: "Namecheap does not support any of the components of the SSR2 Final Report that contemplate any modification of the RAA (including but not limited to Recommendations 6 and 8), and urges the ICANN Board to completely reject any of these recommendations."

"Namecheap is concerned that the recommendations in the SSR2 Final Report appear to be a method of subverting the ICANN multistakeholder model- rather than focusing on ICANN's status and progress in the security and stability of the Internet's unique identifiers (as Specified in Section 4.6(c) of the ICANN By-Laws). Many of the recommendations are similar to repeated efforts by the groups on the SSR2 Review team to change ICANN policies- through government lobbying, litigation, or PDPs- that have not been successful. The ICANN Board should reject this attempt to subvert the ICANN multistakeholder model process- which if allowed would jeopardize the legitimacy of the very basis of ICANN. Instead of generating reports that are deeply flawed and lack support from constituencies that ostensibly will be bound by the recommendations, the participants in this review team should focus their efforts on finding consensus with the diverse participants of ICANN."

RrSG: "A number of the recommendations include specific instructions to ICANN to change the RAA and the RA. The RrSG notes that these recommendations are contrary to the negotiation process identified in the RAA (Section 7.4), and the RA (Article 7.7), and should be completely rejected by the ICANN Board."

Concern that some recommendations repeat or significantly overlap with ongoing work

RySG: "As the RySG noted in its comments to the SSR2 Draft Report, we cannot support recommendations that repeat, or represent significant overlap with, recommendations of other active reviews such as the CCT-RT and policy processes such as the EPDP [emphasis removed]. The RySG questions the value in implementing repetitive recommendations and urges the Board to consider the impact on the workloads of the community and Staff, and to reject those where implementation would circumvent the policy development process or where similar past recommendations have not been accepted by the Board."

PIR: "Finally, we note that several recommendations represent significant duplication of ongoing cross community work and recommendations from the CCT RT, many of which focus on the issue of DNS Abuse."

i2Coalition: "[W]e believe that recommendations that may lead to potential duplicative work should not be approved… The i2Coalition is in support of the community work already happening throughout the whole of ICANN, and believes that recommendations which are repetitive or directly duplicative are not in the best interest of ICANN. To that end, we urge the board to support recommendation 1 and take action on it by identifying potential duplicative work. For instance, Recommendation 17 is potentially duplicative with the existing Name Collision Analysis Project (NCAP) study. There are certainly several others throughout the report that merit thorough exploration before any action is taken on them."

Namecheap: "A number of the recommendations in the SSR2 Final Report address items or functions that ICANN org already provides- and in some cases is already dedicating significant resources toward. Specifically, Recommendations 2, 3, and 4.3 already exist within ICANN."

RrSG: "[A] number of these recommendations cover items that ICANN org is already dedicating significant resources- including the responsibilities of the Office of the Chief Technology Officer (OCTO) and Contractual Compliance. The RrSG struggled to consider recommendations that are duplicative of longstanding ICANN activities, which additionally led the RrSG to question the Review Team's other recommendations, which might be colored by a misunderstanding of the issues, data, and current contracted party abuse initiatives."

Concern about lack of contracted party representation on the SSR2 Review Team and consideration of prior input

Tucows: "The Tucows family of registrars notes the imbalance of the SSR2 team, as there were no members of the Contracted Party house available to participate in this working

group. Many of the concerns raised below would likely have been mitigated with a better balance of membership."

Namecheap: "Namecheap reviewed the participants of the SSR2 Review Team, and while there was some participation from certain ICANN community groups, not all SOs/ACs were represented in the team that drafted the SSR2 Final Report. There were no representatives from the RrSG, the RySG, the Internet Service Providers and Connectivity Providers Constituency (ISPCP), and the Not-for-Profit Operational Concerns Constituency (NPOC)... [S]ome constituencies (including the RrSG and the RySG), provided comments to the SSR2 Draft Report. These comments from these constituencies were strongly against, or completely disagreed with, some of the recommendations (based largely in part upon the RAA or RA). It appears that most (if not all) of this feedback was completely ignored, and in fact, it appears that the recommendations in the SSR2 Final Report are even stronger than in the SSR2 Draft Report- despite Appendix H repeatedly indicating that the feedback was incorporated into the SSR2 Final Report. In light of the biased participation and complete disregard of public feedback, Namecheap strongly cautions the ICANN Board that accepting the SSR2 Final Report will set a dangerous precedent of allowing minority groups to disregard and overrule other ICANN community members."

RrSG: "RrSG notes that the final Review Team does not appear to contain any representatives from the RrSG, the Registry Stakeholder Group (RySG), the Internet Service Providers and Connectivity Providers Constituency (ISPCP), and the Not-for-Profit Operational Concerns Constituency (NPOC), and some of the recommendations appear to be significantly biased against the interests of these constituencies. The absence of constituencies is not a justification for creating a Final Report that will significantly (and negatively) impact those constituencies. Some of these constituencies (including the RrSG and the RySG), provided strong comments against or outright disagreement (based upon the RAA or RA) with some of the recommendations in the Draft Report. Much of this feedback appears to be largely ignored, despite Appendix H repeatedly indicating that the feedback was incorporated into the Final Report. The RrSG strongly cautions the ICANN Board against adopting many of the recommendations in the Final Report, and recommends that the Board only approve recommendations that have the full support of the entire ICANN community."

Concern that recommendations do not consider cost

Namecheap: "[R]ecommendations in the SSR2 Final Report appear to be made without any consideration of cost to ICANN. At the very least, the abuse incentives contained in Recommendation 14 are not presented in a revenue-neutral manner- ICANN is left to determine how to pay for the recommendation. Other recommendations (e.g. Recommendations 3 and 10) propose a number of ICANN initiatives (reports, participation in conferences, duplicating peer-reviewed research, etc.) that will result in significant costs - without contemplating the impact on the limited ICANN budget."

RrSG: "[R]ecommendations appear to have been made without any consideration of how ICANN org will pay to implement the recommendations - either through additional funding or reprioritization within the existing budget. The RrSG notes that the vast majority of ICANN's budget is ultimately paid by domain name registrants, and the Final Report does not fully explain why registrants should bear this additional burden.

Other overarching comments

RySG: “In an effort to create SMART recommendations the Report focuses on tactics and actions and does not include adequate problem statements to support the recommended actions” [emphasis removed].

SSAC: “In general terms, we endorse to the ICANN Board the fundamental conclusion behind the detailed recommendations in this Final Report, namely that responses on the part of ICANN both as an organization and as a community are necessary as a matter of the highest priority.”

“The SSAC does however have a concern related to the capacity of the organization and community to implement these 24 comprehensive recommendations contained in the SSR2 Final Report in a meaningful and timely way. Irrespective of the details of each of the complete set of recommended actions, the Final Report is clearly indicating that there are some serious and longstanding issues relating to ICANN's execution of its security, stability, and resiliency (SSR) related commitments. The number of recommendations and the scale and set of actions proposed in the recommendations, when taken together indicate that in order to rectify this situation, the organization and community will need to prioritize these issues and the implementation of relevant remedial actions.”

M3AAWG: “We concur with the SSR2 RT assertion that systemic DNS abuse needs to be tackled. We continue to encourage the ICANN organization and community to take seriously the recommendations from the SSR2 report, and support the RT's position that implementing these recommendations is urgent, particularly when it comes to the issue of DNS abuse. M3AAWG recommends that the ICANN Board direct the organization and engages with the community to address the continuing harm created by DNS abuse. Due to its public interest commitments, ICANN should provide a plan to adopt clear indicators, measurements or other transparency and accountability mechanisms as quickly as possible.”

Afnic: “Afnic would like to take this opportunity to express its full support to the RySG's comment on ICANN's SSR2 Final Report.”

Article 19: “Our analysis shows that the ICANN Second Security, Stability, and Resiliency (SSR2) Review Team Final Report contains several positive and commendable provisions, including inclusion of recommendations encouraging transparency, accountability and privacy. However, it does not fully address the human rights implications of the recommendations, which propose mitigating DNS abuse and compliance enforcement of the same but do not provide clear guidance on their scope and limitations which may enable the extension of ICANN’s remit and scope beyond infrastructure to include content moderation.”

GNSO Council: “Based on preliminary and diverse reactions across the different stakeholders in the GNSO and the differing opinions in relation to the topic of DNS Abuse, the GNSO Council’s comments will refrain from signaling support or non-support for any of the SSR2 recommendations. The comments contained here are only based on the GNSO Council’s remit as managers of the GNSO’s Policy Development Process.”

NCSG: "It is imperative for us to emphasize the importance of keeping the ICANN mission technical and the definition of DNS abuse limited to technical issues at ICANN. The SSR2 report however falls short of that.

"Emphasis on intellectual property rights is wrong: The security and stability of the DNS is a technical function. It has nothing to do with intellectual property holders and their rights. They can protect their rights through other avenues. The report consistently brings intellectual property attorneys and their issues to the fore, which is irrelevant and can result in mission creep."

"Registration Data: The report discusses the Registration Directory Services and insists that it is important to provide access to domain name registrants personal and sensitive data. As the report mentions too, EPDP (a policy development group) has already provided a policy document to provide access to registrants personal and sensitive data and its work has not finished yet. But the review team is not satisfied with the work-in-progress of the policy group. It is not clear for us if it is even within the scope of the review team to get involved with providing a rather one-sided feedback for a bottom-up consensus policy that has not been even implemented.[1] …We believe this entire section on RDS and the comments related to EPDP need to be removed."

"Definition of DNS abuse: In the Annex, the team tries to provide a definition for DNS abuse: 'Intentional misuse of the universal identifiers provided by the DNS for cybercrime infrastructure and directed users to websites that enable other forms of crime, such as child exploitation, intellectual property infringement, and fraud' (p.60). This definition of DNS abuse is very objectionable. DNS abuse has a definition limited to technical threats and it should not under any circumstances address intellectual property or other similar non-technical issues. We recommend scraping this definition from this review."

Namecheap: **"**Namecheap acknowledges the significant efforts of the SSR2 Review Team, however in light of the concerns raised by Namecheap, the RrSG, and the RySG, Namecheap requests that the ICANN Board not adopt the recommendations contained in this report for the reasons provided by the respective groups."

Comments by recommendation

Not every contributor made a comment about each individual recommendation or recommendation group. Only comments made in specific reference to an individual recommendation or recommendation group are summarized below.

Recommendation 1.1: Further Review of SSR1

RySG "supports this recommendation. Identifying and avoiding duplicate work should be an important objective when rationalizing the plan to complete the implementation of SSR1."

[1] 1 The SSR2, page 37.

i2Coalition "is in support of the community work already happening throughout the whole of ICANN, and believes that recommendations which are repetitive or directly duplicative are not in the best interest of ICANN. To that end, we urge the board to support recommendation 1 and take action on it by identifying potential duplicative work."

GAC "notes the SSR2 Review Team's findings concerning the 28 SSR1 Review recommendations, out of which none was implemented fully, and all remained relevant. In this regard the GAC supports the development of measurable performance indicators that would enable, on the one hand, the identification of the underlying obstacles to full implementation and, on the other hand, would provide valuable measurement methods for the implementation of future recommendations. The GAC thus agrees with the Final Report's Recommendation 1 that ICANN org should perform a further comprehensive review of the implementation of the SSR1 recommendations, taking into account the findings offered by the SSR2 Review Team."

BC notes it "must again comment regarding its -- and the community's -- disappointment in the Board's refusal to oversee timely implementation of previous reviews, including SSR1. The independent review process demands tangible results, and not simply reports that sit idle. The BC commented on the draft SSR2 report in March 2020 and would like to reiterate those comments for the full report.[2]"

BC "does not favour an unending cycle of reviews that are occupied by measuring implementation of prior recommendations. As such, we strongly encourage ICANN and the community to turn their attention to implementation of all outstanding recommendations. Therefore, the BC thinks Recommendation 1 may be unnecessary."

RrSG "generally supports this recommendation."

IPC is "alarmed that not a single one of the 28 SSR1 recommendations has been implemented as of present—despite the assessment that every one of these recommendations remains relevant today. It is thus essential that the ICANN Board and Org put into place a plan for expeditiously implementing these delinquent recommendations. Both the health of the DNS, as well as faith in the multi-stakeholder model, rely on this important work product of the initial Review Team being implemented."

Recommendations 2.1 – 2.4: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management

RySG "supports these recommendations insofar as they represent strategic requirements for ICANN Org risk management.

"We do not support the creation of the new function to oversee security and risk management, as suggested per Recommendation 2.1., as we believe that these roles can (and currently are being) handled by existing members across different functional areas within ICANN Org, including OCTO.

[2] March 2020 BC comment on SSR2 Draft report, at https://www.bizconst.org/assets/docs/positionsstatements/2020/2020_03March_10%20BC%20comment%20on%20SSR2%20Report.pdf.

"One area of concern is Recommendation 2.4 where it seems to suggest that the CSO role should be required to sign off on all security related contractual terms, including registry and registrar agreements. The RySG notes that Section 7.7 of the Registry Agreement has explicit provisions regarding the renegotiation of the agreement and the implementation of this recommendation must take care not to violate those provisions. ICANN Org also has a history of including the appropriate members of the organization in contractual discussions with contracted parties, and as such there is no need for the SSR2 RT to explicitly include this responsibility in Recommendation 2.4."

i2Coalition believes that Recommendation 2.1 "without stating the problem that is to be solved, ask[s] for new roles that already seem to exist… This is a serious concern with recommendations that, once accepted by the Board, would create duplicative work, or even seem to expand ICANN's remit."

Namecheap states: "A number of the recommendations in the SSR2 Final Report address items or functions that ICANN org already provides- and in some cases is already dedicating significant resources toward. Specifically, Recommendations 2, 3, and 4.3 already exist within ICANN…It is not clear from the SSR2 Final Report whether the Review Team is aware of these ICANN activities, or how the Review Team finds these significant and beneficial activities to be insufficient.""

GAC "welcomes Recommendation 2". GAC notes: "While such a centralised role may have various benefits such as making ICANN's work more efficient, providing a single point of contact for reporting on all SSR-related matters or offering a single voice for the public interest (in this regard see also Recommendation 8.1 above), the GAC would not wish to presume expertise in ICANN's internal administration of executive functions. Notably, the centralization of powers within a single role should not be allowed to create a scenario in which resources put toward protection of ICANN org are incentivized over resources put toward protection of the DNS."

BC states: "To address the operational challenge of full implementation of the SSR1 report, the BC agrees that creation of a C-suite position is warranted, with that position responsible for both Strategic and Tactical Security and Risk Management. Further, that role should oversee SSR2 Recommendation 3: Improve SSR-related Budget Transparency for the SSR2 recommendations that expands upon the original SSR1 recommendation."

RrSG offers the following comments:

- 2.1: "RrSG notes that ICANN already has a Chief Security, Stability & Resiliency Officer- John Crain. It is not clear why this recommendation is needed in light of Mr. Crain's significant individual and team contributions to the security and stability of the Internet."
- 2.2: "It is the understanding of the RrSG that through OCTO generally, and John Crain specifically, ICANN already performs these functions."
- 2.3: "It is not clear to the RrSG how these roles and functions are not already being provided by various ICANN org and IANA staff. This recommendation appears to be redundant and thus the RrSG does not support adopting this recommendation."
- 2.4: "RrSG notes that the 2013 RAA makes no references to security-relevant items in the RAA, and it is inappropriate for a Review Team (without the participation of anyone in the RrSG) to suggest that such clauses are desirable or practical. It is not the purview of the Review Team to dictate who within ICANN Org shall perform what

functions, including the review and approval of any changes to the RAA. While such individual(s) may be consulted, ultimately it is up to the ICANN Org negotiating team (including the participation of ICANN Legal) to approve any terms on behalf of ICANN."

ALAC "applauds Recommendation 2 for the creation of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) position, recommending that it take into account the best people, work, practices, and experience, including those who have already demonstrated foresight and are proactive in their work. This is, if anything, long overdue."

IPC "supports the SSR2 RT's recommendation that a C-Suite level executive officer position be created to coordinate and strategically manage ICANN's security and risk management objectives. This new role should effectively centralize previously decentralized roles related to SSR in a manner geared toward greater efficiency and responsibility. The need for this new position is particularly clear to the IPC in light of ICANN's failure to efficiently implement the SSR1 objectives that have been outstanding since 2012. It is the hope of the IPC that an experienced security executive designated as this officer, supported by a sufficient budget and staff, will be able to more efficiently prioritize and implement these critical security and risk management activities for which ICANN is responsible. Accordingly, the IPC is strongly supportive of the RT's recommendations related to this new position."

Recommendations 3.1 – 3.3: Improve SSR-related Budget Transparency

RySG "supports the recommended actions to improve SSR-related budget transparency, but cautions that briefings to the ICANN community on SSR strategy and projects should be high level and not disclose specific security practices, so as not to introduce potential attack vectors. We reiterate that, as per our previous comment, we do not support the creation of the Executive CSuite Security Officer referred to in Recommendation 3.1, as this role is already sufficiently being covered within ICANN Org."

i2Coalition cites Recommendation 3.1 in its statement that "[t]he Final Report is full of recommendations that, without stating the problem that is to be solved, ask for new roles that already seem to exist… This is a serious concern with recommendations that, once accepted by the Board, would create duplicative work, or even seem to expand ICANN's remit."

INTA "notes its strong support for, and encourages assigning High priority status" to Recommendation 3.

Namecheap notes: "A number of the recommendations in the SSR2 Final Report address items or functions that ICANN org already provides- and in some cases is already dedicating significant resources toward. Specifically, Recommendations 2, 3, and 4.3 already exist within ICANN…It is not clear from the SSR2 Final Report whether the Review Team is aware of these ICANN activities, or how the Review Team finds these significant and beneficial activities to be insufficient." Further, Namecheap states that "[some] recommendations (e.g. Recommendations 3 and 10) propose a number of ICANN initiatives (reports, participation in conferences, duplicating peer-reviewed research, etc.) that will result in significant costs without contemplating the impact on the limited ICANN budget… As the vast majority of ICANN's budget is ultimately paid for by domain name registrants, Namecheap recommends

that the ICANN Board reject any of the recommendations that will result in significant costs to ICANN."

GAC "welcomes Recommendations 2-7 on standard security practices and stresses the urgency for ICANN to implement them" in line with GAC's considerations noted under Recommendation 2.

RrSG offers the following comments:

- 3.1: "It is not clear from the Final Report how OCTO's current participation in the ICANN community, the Internet community in general, as well as existing OCTO publications are deficient. Specifically, OCTO publishes a number of reports authored by OCTO staff, ongoing research by the OCTO team, and Commissioned Documents. This is only a representative sample of the extensive activities conducted by the OCTO team (additional details are available at https://www.icann.org/octo). Before adopting this recommendation, the RrSG recommends that the ICANN Board consider existing (and significant) ICANN org activities."
- 3.2: "It is not clear to the RrSG how the current cadence of reports and substantial ICANN event participation by OCTO is deficient, and why the Review Team has designated this as a high priority item."
- 3.3: "It is not clear to the RrSG how ICANN's current public comment on its budget (including SSR-related items) and strategic planning is deficient to necessitate this recommendation, nor why the Review Team designated this as a high priority item."

Recommendations 4.1 – 4.3: Improve Risk Management Processes and Procedures

RySG "is generally supportive of risk mitigation management within ICANN and believe that this can be sufficiently addressed within the current ICANN staff structures without the addition of a C-Suite level position."

i2Coalition cites Recommendation 4.3 in its statement that "[t]he Final Report is full of recommendations that, without stating the problem that is to be solved, ask for new roles that already seem to exist… This is a serious concern with recommendations that, once accepted by the Board, would create duplicative work, or even seem to expand ICANN's remit."

Namecheap notes: "A number of the recommendations in the SSR2 Final Report address items or functions that ICANN org already provides- and in some cases is already dedicating significant resources toward. Specifically, Recommendations 2, 3, and 4.3 already exist within ICANN…It is not clear from the SSR2 Final Report whether the Review Team is aware of these ICANN activities, or how the Review Team finds these significant and beneficial activities to be insufficient."

GAC "welcomes Recommendations 2-7 on standard security practices and stresses the urgency for ICANN to implement them" in line with GAC's considerations noted under Recommendation 2.

BC highlights Recommendation 4 as "top priority."

RrSG offers the following comments:

- 4.1. “The goal of this recommendation is not clear to the RrSG, and thus does not support this recommendation.”
- 4.2: “The RrSG generally supports this recommendation, with the understanding that it will be narrowly tailored, specifically focused, and necessary to achieve the goals of the recommendation.”
- 4.3: “As of the date of this comment, ICANN’s Office of the Chief Technology Officer (OCTO) comprises approximately 20 staff. It is not clear to what extent the functions identified in this recommendation are not currently performed by OCTO, or why a new position is required to perform these functions. To the extent these functions are not currently performed by OCTO, the team should be capable of incorporating these items into their existing departmental structure.”

ALAC indicates “strong support” for Recommendation 4 and states: “Risk Management has become a core concern and core organizational goal for organizations of all sizes. Creating a centralized risk management function and adopting a recognized risk management standard (ISO 31000) would bring ICANN into alignment with best practices, both in technology-centric organizations and beyond. However, ICANN needs to recognize the unique risks and risk management challenges that ICANN faces due to its unique mandate and structure, in particular its policy development processes. ICANN’s risk management structure must ensure that all risks are considered, including community participation that is balanced in order to avoid risks of capture, disproportionate influence by parties with less at stake and/or the ability to stagnate processes.”

IPC “is supportive of this recommendation. The IPC concurs with the goals of this recommendation to prevent and address internal risks, and to adopt common industry standards.”

Recommendations 5.1 – 5.4: Comply with Appropriate Information Security Management Systems and Security Certifications

RySG “recommend[s] that the Board seek additional clarity from the SSR2 RT regarding what entities ‘beyond’ the ICANN community ICANN Org should report out regarding its security activities.”

GAC “welcomes Recommendations 2-7 on standard security practices and stresses the urgency for ICANN to implement them” in line with GAC’s considerations noted under Recommendation 2.

BC highlights Recommendation 5 as “top priority.”

RrSG notes: “As indicated in the RrSG comment to Draft Report, the RrSG generally supports certification, auditing, and reporting of ICANN.”

ALAC indicates “strong support” for Recommendation 5.

Recommendations 6.1 – 6.2: SSR Vulnerability Disclosure and Transparency

RySG states: “While the RySG supports its members adopting vulnerability disclosure policies as good business practice, it does not support ICANN acting as a clearinghouse, gatekeeper, or regulator of vulnerability disclosure policies.”

“Many RySG members do not operate just as registry operators. For example, dotBrands operate separate and distinct businesses unrelated to their registry. It is unreasonable to expect brands to disclose any vulnerabilities that they handle in the ordinary course of their business to ICANN, and out of ICANN’s remit to review the operational processes of brands. The RySG also has concerns about supporting the recommendation to implement such practices in contracts without knowing what specific practices the Review Team has in mind and without following the appropriate and limited processes for amending Registry Agreements…We would like to remind the Board, when considering this recommendation, that contractual changes can only be effected via contractual negotiations or Consensus Policies.”

Namecheap “does not support any of the components of the SSR2 Final Report that contemplate any modification of the RAA (including but not limited to Recommendations 6 and 8), and urges the ICANN Board to completely reject any of these recommendations. According to the RAA (which is binding on ICANN and each accredited registrar), the sole process to negotiate and modify the RAA is detailed in Section 7.4 of the RAA. It is a process between ICANN Org and the Registrar Stakeholder Group (RrSG), and can only be initiated by those parties. Those are the only parties that participate in the negotiations. Although any draft revisions are subject to public comment, the RrSG is under no obligation to accept any public comment.”

GAC “welcomes Recommendations 2-7 on standard security practices and stresses the urgency for ICANN to implement them” in line with GAC’s considerations noted under Recommendation 2.

RrSG offers the following comments

- 6.1: “The RrSG does not support this recommendation, for the reasons specified above in the general comments. Additionally, it is not the role of ICANN or the ICANN community to dictate the operational obligations of contractual parties especially without the participation, agreement, and approval of the contracted parties. The RrSG recommends that the ICANN Board reject this recommendation 6.1 entirely.”
- 6.2: “Reporting data breaches to ICANN is already a requirement in the Section 3.20 of the RAA. ICANN Compliance has the data/metrics to report on this. Additionally, it is extremely difficult for ICANN to effectively anonymize metrics due to the geography of the contracted parties. Some jurisdictions, such as the United States and China, include a large number of contracted parties so anonymization is possible. Other regions (such as Africa) or countries (such as Ireland), contain only a handful (at most) contracted parties so “anonymized” metrics could easily be reversed engineered to determine the underlying contracted part. To the extent that this recommendation contemplates changes to the RAA, the RrSG reiterates its previous general objection regarding contract modification via Review Team, and urges the ICANN Board to reject this recommendation.”

ALAC indicates “strong support” for Recommendation 6 and states: “Vulnerability disclosures are sensitive and subject to different norms of practice in different communities, among which are software, service providers, specialists, bounty hunters, and many others. Establishing

trust takes time and effort which should be expended constantly. In the end, the goal is the same - to promote the implementation of and (voluntary) adherence to standards for vulnerability reporting, by the contracted parties and by ICANN itself."

IPC "is supportive of this recommendation. However, the IPC believes the current language should not be read to require dotBrands to disclose all vulnerabilities in their business to ICANN. This goes beyond ICANN's remit. At a minimum, any vulnerabilities should be limited only to those systems directly related to the operation of the TLD. And in the case of a dotBrand or other single registrant TLD where even such vulnerabilities are, effectively, an internal matter, such disclosure may not be warranted."

Recommendations 7.1 – 7.5: Improve Business Continuity and Disaster Recovery Processes and Procedures

RySG states: "The RySG fully recognises the importance of Business Continuity (BC) and Disaster Recovery (DR) processes and procedures. BC and DR should be based on an inventory of critical systems and an expectation of the level of service to be provided. While the RySG supports the principle being highlighted in this set of recommendations, i.e., having a BC and a DR plan, the proposed scope of "all the systems owned by or under the ICANN org purview" is too broad, contrary to best commercial practice, and thus inappropriate. BC and DR development should be included as part of an overall risk management strategy as highlighted by the Report in recommendation 4 and elsewhere in existing policies and processes. Similar, for example, to the IANA risk management strategy for its services. We recommend that the Board seek additional clarity from the SSR2 RT regarding how Recommendation 7.2 feeds into the current Governance Working Group developing a governance structure for Root Zone Operators."

M3AAWG states: "ICANN's current lack of a Business Continuity and Disaster Recovery Plan is alarming and creating one should be a priority…We concur with the SSR2 RT that the creation of a strategic, executive security position within the ICANN organization is useful, and agree with the RT that ICANN should pursue best-practice approaches for risk management, information security management, business continuity and disaster recovery."

GAC "welcomes Recommendations 2-7 on standard security practices and stresses the urgency for ICANN to implement them" in line with GAC's considerations noted under Recommendation 2.

BC believes "ICANN's lack of a Business Continuity and Disaster Recovery Plan is especially concerning. Hence, SSR2 Recommendation 7 should be of highest priority."

RrSG notes: "Although the RrSG is generally supportive of this recommendation, it will defer to IANA regarding whether or not to create and maintain a KSK ceremony location outside of the United States."

ALAC indicates "strong support" for Recommendation 7 and states: "Recommendation 7, the adoption of business continuity and disaster recovery policies, plans and procedures, should be read in conjunction with Recommendations 2 and 5, discussed above. All of these recommendations (and others) support the overarching theme of bringing ICANN into alignment with InfoSec and operational security standards prevalent in technology-centric

organizations worldwide. Practices such as these have moved from 'nice to have' to 'must have' over the last several years; over the next several years, they will move to 'negligent to do without.'"

Recommendation 8.1: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties

RySG believes "Recommendation 8 is not consistent with the terms of the Registry Agreement and must be rejected. Section 7.7 of the Registry Agreement is the section that allows for the bilateral negotiation of a contemplated change to the Registry Agreement between Registries and ICANN itself, not third parties that are not a party to the Agreement, with one exception: The Registry Agreement considers the possibility of a 'Working Group' that may participate in these negotiations, but it is explicitly the registries that makes such an appointment, not ICANN. (See Registry Agreement Section 7.6, "'Working Group' means representatives of the Applicable Registry Operators and other members of the community that the Registry Stakeholders Group appoints, from time to time, to serve as a working group to consult on amendments to the Applicable Registry Agreements."). It should also be noted that the Registry Agreement explicitly states that there are no third-party beneficiaries to the Registry Agreement. (Registry Agreement, Section 7.8)."

PIR notes "Recommendations 8 and 14 are not consistent with the terms of the Registry Agreement. Recommendation 8 violates several provisions of the Registry Agreement. Section 7.7 of the Registry Agreement allows for the bilateral negotiation of a contemplated change to the Registry Agreement between Registries and ICANN itself, but not third parties that are not a party to the Agreement. The Registry Agreement does provide for the possibility of a 'Working Group' participating in these negotiations. Only Registries make such an appointment. Further, the Registry Agreement explicitly states that there are no third-party beneficiaries to the Registry Agreement."

M3AAWG notes: "ICANN has not fostered a contract negotiations process that is transparent, or open to participation from all affected ICANN constituencies…We fully support the commissioning of a negotiating team to renegotiate contracted party contracts as described in SSR2 Recommendation 8 with the objective of improving the SSR of the DNS for end-users, businesses, and governments."

Article 19 believes "the recommendation should be revised to ensure that the process of selecting the negotiating team should be a multi-stakeholder process, and that the composition of the negotiating team must comprise various stakeholders from the Empowered Community. Specifically, the recommendation should create open consultations and opportunities for stakeholders to submit public comments when renegotiating with contracted parties."

INTA notes: "Although the multi-stakeholder community is involved in developing policy that is used to craft registry and registrar contracts with ICANN, final contract language is generally a matter negotiated between ICANN and the contracted parties without involvement from the community - even though many aspects of the contracts impact the broader community, including with respect to matters like DNS abuse. INTA has seen time and time again that the specific and explicit language of the contracts is paramount - ICANN refuses to enforce obligations unless they have an express basis to do so under the terms of the contracts, even

if certain contracted party activity clearly violates the spirit of the provision and the intent of the community policy that was the basis for the contractual provisions. Therefore, it is equally paramount that ICANN include independent third-party negotiators that are free from conflicts of interest and represent the non-contracted participants of the ICANN community in contractual negotiations to ensure final contract provisions faithfully implement community policies and properly facilitate enforcement of these policies."

Tucows notes it is "concerning that the SSR2 saw fit to recommend amendments to contracts no member of the SSR2 is a party to… SSR2 Recommendation 8 is particularly problematic in this regard. It is vastly inappropriate for a third party to attempt to enter into contract negotiations for a contract they are not a party to. The Tucows family of registrars recognizes that DNS Abuse (as defined in the DNS Abuse Framework, to which Tucows is a signatory) is a topic of much interest right now. The Tucows family of registrars both leads and supports efforts to better combat such abuse, from within the ICANN remit and outside of it. The SSR2 recommendation, however, that 'abuse and security experts' affiliated with and paid by groups whose business it is to find abuse—but not to combat it—is in error. Not just because, as noted above, it is not acceptable for a third party to attempt to involve themselves in a contract they are not a party to, but also because when a party is paid to identify abuse, they are motivated to find it but not to resolve it."

Namecheap "does not support any of the components of the SSR2 Final Report that contemplate any modification of the RAA (including but not limited to Recommendations 6 and 8), and urges the ICANN Board to completely reject any of these recommendations. According to the RAA (which is binding on ICANN and each accredited registrar), the sole process to negotiate and modify the RAA is detailed in Section 7.4 of the RAA. It is a process between ICANN Org and the Registrar Stakeholder Group (RrSG), and can only be initiated by those parties. Those are the only parties that participate in the negotiations. Although any draft revisions are subject to public comment, the RrSG is under no obligation to accept any public comment."

GAC "agrees with the spirit of Recommendation 8, which seeks to incorporate the needs of the public safety and consumer interests into the contract negotiations. Clearly, these contracts have significance in terms of what might be done to counter DNS Abuse. We recognise though that contract negotiations between ICANN and the Contracted Parties do not currently include third parties and therefore would encourage ICANN to consult with independent security experts (i.e. non-contracted entities) for the purposes of developing and agreeing upon security-related provisions that can be incorporated into the contracts."

BC highlights Recommendation 8 as "top priority."

RrSG states: "As referenced in the RrSG general comment, this is not acceptable and a violation of the RAA. RAA negotiations are conducted solely as specified in Section 7.4 of the RAA. No matter how desirable to the limited interests in the Review Team, it cannot overrule established requirements in the RAA."

ALAC indicates "strong support" for Recommendation 8 and notes "representation of the 'public interest' in negotiations with contracted parties, is a recommendation of particular importance to the ALAC and the At-Large Community, which in many ways represents the public interest in the broadest sense within the ICANN structure. Independent abuse and security experts must have a voice in how these issues are represented in ICANN's contracts.

In addition, end users, who are often most affected (even if not always first affected) by abuse and security incidents need a voice as well. In each case, these additional 'seats at the table' must not be construed in ways that reduce efficiency, either in contract negotiations and adoption, or in performance."

IPC "is supportive of this recommendation, particularly as it applies to the base agreements for contracted parties. The IPC would be willing to assist with the negotiation process by supplying subject matter experts in the field of Intellectual Property. A key concern of the IPC is for contractual language in the base agreements with respect to abuse be clear and recognized as effective and enforceable by ICANN org and the Compliance team. In general, the IPC thinks that the participation of these experts is most relevant to the negotiation of base agreement contractual terms and not the bilateral contracts between ICANN and a contracted party."

Recommendations 9.1 – 9.4: Monitor and Enforce Compliance

RySG states: "The implication of Recommendation 9 is that ICANN Compliance is not enforcing the terms of the Registry Agreement or the Registrar Accreditation Agreement. The Registries disagree with this characterization and note that Registry Operators' compliance with their abuse obligations were recently audited by ICANN Compliance. In our comments on the Draft Report Recommendation 10, the RySG made it very clear that any recommendations regarding ICANN's Compliance functions should be linked to specific contractual terms and tied to a specific problem statement. As such, we are disappointed to see that Recommendation 9.1 remains extremely vague, and we reiterate that ICANN's Compliance team does not need to be reminded to generally enforce contracts with Registries and Registrars. Such a recommendation exceeds the scope of this Review."

PIR notes that some "recommendations imply that ICANN Compliance is not enforcing existing contractual obligations or encourage ICANN Compliance to undertake activities that are clearly outside of ICANN Compliance's scope and remit."

M3AAWG states: "As noted last year, M3AAWG member experience when dealing with ICANN Compliance continues to be unproductive. This is in part because ICANN's contracts provide few enforceable clauses related to mitigating abuse… We continue to concur with the SSR2 RT regarding ICANN's failure to request, enumerate, or to negotiate for enforcement tools, and therefore support all aspects of SSR2 Recommendation 9."

Article 19 "recognize[s] that malicious actors use the DNS as a tool to perpetrate criminal and unlawful activities. However, we strongly oppose the proposition to develop and deploy monitoring systems without strong due process procedures in place, including the creation of a clear timeline to take action against the domain name after providing the registrant with opportunities to explain their action. We also oppose any attempts to include content takedowns without due process, as mentioned above… [R]ecommendation 9 should be redrafted to make it explicit that due process would be followed and that any data collected during the monitoring and compliance enforcement process would not be used without the registrants explicit and informed consent that follows due process and subject to strict retention limits."

INTA offers the following comments:

- 9.1: “INTA strongly supports this recommendation and its assigned High priority level. INTA members have consistently and repeatedly voiced concerns about their substandard experiences with ICANN Compliance. These experiences have caused some members to refrain from filing compliance complaints at all because they have come to expect no meaningful engagement or assistance. Clearly, this is unacceptable and unsustainable where Compliance is tasked with the important role of ensuring that contracted parties fulfill the requirements set forth in their agreements with ICANN, particularly pertaining to SSR and abuse-related matters. As noted above, INTA believes stronger enforcement of existing registry and registrar contractual obligations (in addition to the negotiation of better contractual provisions) will be to the benefit of the health of the DNS, in service of ICANN’s mission to ensure the SSR of the DNS. Contracted parties are in a unique position to address DNS abuse and they must be held accountable when they fail to do so.”
- 9.2: “INTA strongly supports this recommendation and its assigned High priority level. Ensuring accurate registration data is of the utmost importance in ensuring the SSR of the DNS, which requires a meaningful level of accountability for domain name registrants. Verifying and validating registrant identities and contact information and the truthfulness of the data they use to register domain names is a fundamental component of such accountability. ICANN must ensure that its contracted parties are properly implementing existing data verification requirements (e.g. Section 3.7.8 and the WHOIS Accuracy Program Specification of the Registrar Accreditation Agreement). This is more important now than ever given the redaction of the majority of registrant data from public Registration Data Directory Services. INTA would go further than this recommendation in encouraging ICANN to implement even stronger data accuracy requirements, such as ID validation, to minimize the use of false or stolen data by bad actors.”
- 9.3: “INTA strongly supports this recommendation and its High priority level. Where ICANN org is tasked with ensuring that contracted parties are living up to their obligations and the expectations of the multi-stakeholder community fails to provide meaningful oversight, then it must be the subject of oversight by an independent authority.”
- 9.4: “INTA strongly supports this recommendation and its High priority level. If ICANN Compliance is not meeting the expectations of the multistakeholder community in its mandate to enforce contractual commitments by registry operators and registrars, it is important for the community to understand whether Compliance lacks the tools necessary to meet those expectations, up to and including changes to the contracts themselves.”

GNSO Council notes with regard to Recommendation 9.2: “As part of the continued EPDP policy deliberations regarding Registration Data, the GNSO Council has already anticipated, via its program management tools, additional work regarding the topic of accuracy. The GNSO Council just received a briefing document from ICANN Org, which will inform a scoping team for this policy topic and determine the appropriate next steps to ensure that any future work is properly scoped and cognizant of competing demands of other policy work and related activities.”

GAC “shares the concerns with SSR2 Review authors that faith in the ICANN multistakeholder model can suffer harm when community guidance on topics as important as the stability, reliability, resiliency, security, and global interoperability of the DNS is not clearly incorporated within enforceable provisions of the contracts between ICANN and Registries

and Registrars. It is particularly concerning that ICANN Contractual Compliance would assert to the SSR2 Review Team in April 2018 - that 'current contracts with registries and registrars do not authorize ICANN org to require registries to suspend or delete potentially abusive domain names and are thus ineffective in allowing them to pursue those engaged in systemic DNS Abuse.' This gap in the current contracts, identified by both ICANN Contract Compliance and the ICANN Board[3] demonstrates the need for improved and enforceable provisions to address DNS Abuse. The GAC strongly supports for implementation the recommendations put forward in Recommendation 9".

BC highlights Recommendation 9 as "top priority."

RrSG offers the following comments:

- 9.1: "ICANN Contractual Compliance already performs this function through complaint processing, reviews, and audits. It is not clear to the RrSG what problem this recommendation is intended to fix."
- 9.2: "ICANN Compliance already proactively monitors compliance through audits and review, and additionally in light of complaint processing, does this. Regarding validation of address fields, the RrSG notes that the Across-field Address Validation Working Group (AFAV) is currently paused in light of concerns over GDPR, and additionally that global solution that includes lesser served regions has not been identified. This recommendation is thus premature. ICANN Contractual Compliance already reviews accuracy of registration through complaint processing, and prior to GDPR, ICANN org conducted periodic WHOIS Accuracy Reporting System (ARS) reviews. The most recent WHOIS ARS report (June 2018) determined that 98% of domain names have an operable email address or telephone number. It is not clear what the accuracy reviews intend to address. Regarding the arbitrary selection of 50 complaints as a trigger for additional compliance review, the RrSG rejects this arbitrary determination as it fails to incorporate proportionality. For example, while 50 complaints might be substantial for a registrar with only 10,000 domains under management (DUM), it is an insignificant number for a registrar with 10 million (DUM). Failure to appreciate this basic understanding of sampling leads the RrSG to question other recommendations in the Final Report. Finally, it is not the role of the ICANN community to instruct an independent Contractual Compliance department how to conduct its activities."
- 9.3: "Any audit of Contractual Compliance should focus on its structure, staffing, activities, systems, processes, and the overall efficiency and effectiveness of this function. Contractual Compliance team already has significant resources within its team and ICANN org to oversee and ensure consistent and accurate complaint processing."
- 9.4: "As part of ongoing collaboration between the RrSG and ICANN Contractual Compliance, the RrSG has requested ICANN Contractual Compliance make its needs for additional tools known to the RrSG on several occasions. The RrSG is not aware of any specific recommendations from ICANN Contractual Compliance. Additionally, the RrSG supports an independent Contractual Compliance team that does not react to instructions from a Review Team."

[3] Botterman (ICANN Board Chair) Letter to Selli (Business Constituency Chair) https://www.icann.org/en/system/files/correspondence/botterman-to-selli-12feb20-en.pdf.

ALAC indicates "strong support" for Recommendation 9 and believes the recommendation is "critical, particularly in connection with Recommendation 8. A contract without compliance is only words on a page, with little or no value except as 'contractual theatre.' This must be seen as a core SSR concern and not merely a legal one."

IPC "is supportive of this recommendation. The IPC finds the current state of contractual compliance is inadequate and strongly recommends that the Board and ICANN org immediately embrace and implement this recommendation."

Recommendations 10.1 – 10.3: Provide Clarity on Definitions of Abuse-related Terms

RySG "agrees on the importance of clarity in terminology and definitions around DNS Abuse. However, we stress that any discussion around a definition of DNS Abuse in the ICANN context must bear in mind ICANN's remit as outlined in the Bylaws. A resulting definition cannot exceed the Bylaws. This said, the RySG would welcome a culture of open discussions aimed at further evolving the definitions of DNS Abuse in the future, as suggested in Recommendation 10.2. We would, however, recommend acknowledging the traditional stakeholders in a CCWG, including Contracted Party representatives, in the recommendation, in addition to the stakeholders named. As noted in these comments, Contracted Parties have worked to establish a definition of DNS Abuse as part of existing community efforts and discussion."

M3AAWG "welcome[s] clarification of key terms and definitions around the issue of DNS abuse as used at and by ICANN, and therefore support[s] all aspects of SSR2 Recommendation 10."

Article 19 believes "the recommendation should be redrafted to ensure that the process proposed in the recommendation for coming up with a working definition of DNS abuse is only carried out after engaging in a multi-stakeholder process such as public comments or consultations that considers all positions on DNS abuse from across the ICANN Empowered Community. This responsibility should not be left only to the section of stakeholders listed under section 10.2 and should also include internet end user communities".

INTA offers the following comments:

- 10.1: "INTA supports this recommendation and its High priority level. As many recent community discussions have demonstrated, there have been numerous overlapping and potentially conflicting efforts to define 'DNS abuse' in a unified, consistent, and authoritative way that would allow for more frictionless reporting, responses, prevention and mitigation solutions, and consequences for abuse and contracted parties who fail to appropriately address it. INTA is concerned that a lack of a unified definition serves as an excuse for some parties to minimize or ignore obligations and best practices to address abusive activity that uses domain names as a vector."
- 10.2: "INTA supports this recommendation, although it could probably be reduced to a Medium priority. It is still important that definitions of DNS abuse evolve over time to keep pace with technological and other developments, and that the entire multi-stakeholder community be involved in such evolution."
- 10.3: "INTA supports this recommendation and its High priority level. For reasons outlined above, having a consistent and authoritative definition of DNS abuse (and other terms for that matter) is critical in ensuring an appropriate common

understanding and expectations throughout the community, ensuring appropriate enforceability of commitments relating to such concepts, and of any policy development, structural reviews, or other community activities relating to such concepts."

Tucows states: "The SSR2's Recommendation 10 that DNS Abuse ought to be defined is apt. There are many complaints about 'DNS Abuse' that fall outside of anything governed by an ICANN contract, including content abuse and purported improper use of registered trademarks in domain names. The DNS Abuse Framework provides a definition that has been used by ICANN in its DAAR reporting[4], was referenced by the GAC in its ICANN70 Communique[5], and is used by most Contracted Parties—even those who are not official signatories to the Framework: 'DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS Abuse)'. The Tucows family of registrars encourages ICANN to formally adopt this definition.[6]"

GNSO Council notes with regard to Recommendations 10.1 and 10.2: "Without expressing an opinion on the formation of a CCWG, the GNSO Council asks the ICANN Board to consider present and near-term demands of other policy work on the ICANN Org, staff, and larger ICANN community. Without a common and agreed upon definition, any additional policy work on a topic as broad as 'DNS abuse' would therefore appear extremely challenging and limiting the remit of any such policy related work both in scope and timeline would be a prerequisite."

Namecheap notes "[some] recommendations (e.g. Recommendations 3 and 10) propose a number of ICANN initiatives (reports, participation in conferences, duplicating peer-reviewed research, etc.) that will result in significant costs - without contemplating the impact on the limited ICANN budget… As the vast majority of ICANN's budget is ultimately paid for by domain name registrants, Namecheap recommends that the ICANN Board reject any of the recommendations that will result in significant costs to ICANN."

---

[4] "What types of security threats does DAAR observe?", accessed 8 April 2021.

[5] ICANN70 GAC Communiqué, accessed 8 April 2021.

[6] The Tucows Family of Registrars acknowledges that, in 2012, the RAP WG's Final Report defined "abuse" as follows:

> Abuse is an action that:
> a. Causes actual and substantial harm, or is a material predicate of such harm, and
> b. Is illegal or illegitimate, or is otherwise considered contrary to the intention and design of a stated legitimate purpose, if such purpose is disclosed.

This is a reasonable definition of abuse broadly but not of DNS Abuse specifically. Attempts to use this definition to apply narrowly to DNS Abuse are misguided and demonstrate a lack of differentiation between domain registration abuses and domain use abuses. Indeed, this was specifically highlighted in that report, on page 4, where

> The RAPWG agreed that understanding and differentiating between domain registration abuses and domain use abuses is essential in the ICANN policy context, and a failure to do so can lead to confusion.

The Tucows Family of Registrars believes that formal adoption by ICANN of the definition of DNS Abuse as defined in the Framework is in accord with the 2012 RAP WG Final Report.

GAC states: “Recent ICANN sessions discussed and debated the meanings of terms such as ‘DNS Abuse’. Some stakeholders view these disagreements as an obstacle to taking meaningful action to combat threats to the security, stability, reliability, and resiliency of the DNS. Consequently, the GAC welcomes and supports Recommendation 10’s request that ICANN Org establish and maintain a web page containing working definition of DNS Abuse and related terminology, to include clear categorization of which security threats ICANN org sees as within - or outside - its remit, and to make consistent and referenced use of the terms contained therein.”

“The GAC Public Safety Working Group would be happy to participate in the proposed Cross-Community Working Group to be tasked with annually updating the abuse-related terminology, to ensure that existing and future cybersecurity threats, abuse, and criminal activity can be adjudicated by ICANN org as within - or outside - its remit.”

“Many in the GAC take the view that too much time has already been spent in arguing about the definition of DNS Abuse, rather than in tackling it. All manifestations of DNS Abuse – be it cybersecurity threats to the internet infrastructure or the distribution of harmful or illegal material on the internet - have adverse effects on the security of and trust in the internet. From that perspective, a problem-based approach, mapping the issues affecting the security of the DNS, could serve as a starting point for operational solutions to address those.”

BC highlights Recommendation 10 as “top priority.”

RrSG offers the following comments:

- 10.1: “It is not clear why the Review Team has made this recommendation. This recommendation implies that ICANN is not already doing all of the activities within the recommendation, whereas these activities are already ongoing. For example, ICANN already has a working definition of DNS abuse (see https://www.icann.org/octo-ssr/daar), and already tracks and reports on DNS abuse levels on a monthly basis. Additionally, it is very easy to review the RAA and the RA to determine the existing contract language regarding abuse. This recommendation is superfluous and duplicates existing ICANN efforts.”
- 10.2: “The formation of a CCWG as described in this recommendation is outside of the ICANN Bylaws and the GNSO Operating Procedures. Additionally, the directions are overly prescriptive, do not allow for realistic timelines, and do not clearly state the problem that the recommendation is attempting to solve. The fact that the recommendation fails to include registrars and registries as participants (the very parties that would be bound by any outcome) reveals that this recommendation is solely intended to dictate additional obligations on contracted parties without their very participation in the process. For these reasons, the ICANN Board should completely reject this recommendation.”
- 10.3: “This oblique reference is likely referring to the definition of ‘abuse’ from the 2012 RAP WG Final Report. It is not clear why this was not articulated directly in the SSR2 Final Report. The definition of abuse from the 2012 RAP WG Final Report is a reasonable definition of abuse broadly but not of DNS Abuse specifically. This is, in fact, directly stated by the same report, which stated that “understanding and differentiating between domain registration abuses and domain use abuses is essential in the ICANN policy context, and a failure to do so can lead to confusion.”

ALAC indicates "strong support" for Recommendation 10 and notes the recommendation "echoes one of the ALAC's current major topics -- the proper definition of DNS abuse. ICANN needs to take the lead in this area, rather than ceding this critical standard-setting activity to the contracted parties, no matter how well meaning they may be. If ICANN is to support the full implementation of the multistakeholder model, it must ensure that the full panoply of stakeholders are engaged and it must facilitate such engagement. However, Recommendation 10.2 should include a voice for end-users directly and not merely indirectly via consumer protection stakeholders. While end-users are in many cases consumers, they are much more than that."

IPC "is supportive of this recommendation. The IPC further notes that the definition of abuse should be expansive and that illegal activity, such as copyright infringement and distribution of child sexual abuse material, not be erroneously conflated with or equated to content regulation. ICANN's mission and responsibility for adequately ensuring 'the stable and secure operation of the Internet's unique identifier systems' is dependent upon an expansive concept of DNS Abuse, such as reflected in the Specification 11 Public Interest Commitments of the Registry Agreement."

Recommendation 11.1: Resolve CZDS Data Access Problems

RySG notes: "In our comment on the Draft Report, the RySG voiced concerns with the inclusion of this recommendation because the current system for access to CZDS data not only provides sufficient access but was also the result of lengthy negotiations taking into account the varying needs of different members of the ICANN community, including the registries that provide this access. We continue to believe that this recommendation is both superfluous and out of scope."

M3AAWG "concur[s] that access to the CZDS remains problematic, particularly for researchers who use CZDS data longitudinally. This is evidenced by a large number of complaints and anecdotal evidence of issues with renewing credentials/access…We concur with the SSR2 RT and support measures are taken to ensure access to Centralized Zone Data Service (CZDS) data is available, in a timely manner and without unnecessary hurdles to requesters."

NCSG notes: "Centralized Zone Data Service: Brand protection and intellectual property protection are not security and stability issues.[7] But in this section 'brand protection' is again invoked. This is a risky path to take and can lead to extending the ICANN mission and the definition of DNS abuse."

GAC states: "Without commenting on the specifics of this recommendation, the GAC acknowledges the importance and utility of cybersecurity researchers' and academics' work, noting that Public Safety officials regularly benefit from such work. To the extent that access to such data as the Centralized Zone Data Service (CZDS) has been promised - but not realized - the GAC would welcome improvements to such processes."

BC highlights Recommendation 11 as "top priority."

[7] Ibid, page 39.

IPC "is supportive of this recommendation. However, the IPC also supports retaining checks and balances on access to CZDS data, given that it could be used to interrupt legitimate business operations. The IPC also notes that many dot Brands are opposed to having to disclose their zone file data since it could be time-sensitive commercial information, for example, if there are names registered in the dot Brand for a new product launch."

Recommendations 12.1 – 12.4: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review

RySG "objects to this recommendation set as it lacks a statement of what problem it is trying to solve. ICANN Org has produced DAAR as a means of informing the community of the apparent existence of DNS Abuse. There are other organizations that produce similar types of reports within the context of their own mission and purpose.[8] The RySG's DNS Abuse Working Group (and its predecessor the DAAR Working Group) has been working collaboratively with OCTO to ensure that DAAR provides the community with the best information available. Without a stated objective or observable problem this recommendation prescribes a solution with dubious value."

"Specifically, the notion of a time-delay in data-sharing is antithetical to the goal of mitigating abuse as quickly as practical and would appear to be competitive with ICANN Org's compliance responsibilities that also occur after-the-fact."

"Also, in our comments on the Draft Report, we objected to Recommendation 12.3 (13.1.1 in the Draft Report), noting that publishing lists of Registries and Registrars whose domains have been targeted for perpetrating security threats does not accomplish the goal of curbing or decreasing actual instances of DNS abuse. The fact is that neither Registries nor Registrars control the source of most DNS abuse and thus the quantity of alleged DNS abuse is not actionable by itself. The Final Report again fails to make a compelling argument for how publishing such information will have a meaningful impact on the overall levels of DNS abuse."

M3AAWG notes "ICANN policy needs to be created around the issue of DNS abuse, clarifying expectations, requirements, and processes. As noted previously, a small number of actors is associated with the majority of security-related registrations. Defining clear policies would lead to a clearer playing field where all relevant actors are aware of, and can pursue the same objectives. While a temporary specification is not ideal, it is an appropriate stop-gap measure…M3AAWG concurs that ICANN policy needs to be created around the issue of DNS abuse, clarifying expectations, requirements, and processes."

Article 19 states: "While we welcome the recommendations, similar to the above comments under recommendation 10, we caution that any process of dealing with DNS abuse should be done through a public consultation process and should not expand ICANN's mandate beyond infrastructure to include content regulation."

INTA offers the following comments:

[8] The APWG has been producing a Phishing Activity Trends Report every quarter https://apwg.org/trendsreports/ for many years.

- 12.1: “INTA strongly supports this recommendation and would see it elevated to a High priority status rather than a Medium priority status given the importance of DNS abuse reporting activities to our members and the full ICANN community. It is critical that DNS abuse mitigation and reporting activities within ICANN be conducted free of conflicts of interest and in an open and transparent manner to the extent possible without jeopardizing the effectiveness of such efforts.”
- 12.2: “INTA supports this recommendation as is, including its proposed priority level (Medium).”
- 12.3: “INTA strongly supports this recommendation and recommends elevating it to a High priority level. While INTA supports incentives for registry operators and registrars who are proactive in combating abuse, it also supports publicly identifying registry operators and registrars who allow abusive domain names to persist and proliferate within their namespaces. ICANN Compliance must also use this data to impose meaningful consequences on registry operators and registrars who do not act in good faith to address abusive domain names. Finally, it is not clear from the recommendation itself what data or metrics will be used to measure which domain names are contributing to abuse - INTA would recommend a variety of internal and external sources be used, including ICANN’s own data (e.g. DAAR) as well as any sources available from government/law enforcement, industry associations, abuse and security threat analysis groups, and other trusted public or private entity sources.”
- 12.4: “INTA strongly supports this recommendation and would see it elevated to a High priority level. Transparency with respect to anti-abuse activities will enable a better understanding of the landscape by all parties. INTA would go a step further and suggest incentives to encourage registry operators and registrars to be proactive in their anti-abuse efforts, in terms of meeting existing obligations under ICANN contracts and applicable law as well as through voluntary measures, in addition to negative consequences for registry operators and registrars that are not taking appropriate anti-abuse steps as noted above.”

Tucows states: “Regarding Recommendation 12.3, any attempt to identify Contracted Parties that ‘contribute to abuse’ is fraught with impossibility: mere numbers and percentages do not tell the whole story. The Tucows family of registrars notes the good work of the Registrar of Last Resort, for example, as well as the fact that the majority of abuse occurs in the .com registry—which speaks to its popularity, not to its permissive or welcoming nature towards abusive registrations. The problems with Recommendation 12.3 should be obvious but, to avoid doubt: attempting to identify registries and registrars that ‘contribute to abuse’ by quantifying the number of abusive registrations or clients on their platform instead simply indicates a high-volume business. Instead, attention should be given to business practices which allow for abusive behaviour or clients with indicators of abusive intent.”

NCSG states: “The review team argues that DAAR is inadequate for research. Because it believes that: ‘Identifying registries and registrars harboring disproportionate levels of abuse would facilitate informed policymaking and add a measure of transparency and accountability to the domain name registration system that does not exist today’[9] DAAR was never set up for the purpose of auditing registries and registrars. It is not a ‘punishment mechanism’ but a research mechanism. It should never have a mission such as identification of registries and registrars that harbor a disproportionate level of abuse. DAAR was recommended by GAC in multiple communiques and it provides useful statistics that can be helpful for security

[9] Ibid, page 40.

research. So it should not be discontinued at the request of the review team but the community as a whole should decide which direction it should take."

GAC "welcomes the recommendations put forward in Recommendation 12 which seek to improve usability, transparency, and reproducibility of existing DNS Abuse Reporting, while noting that such ideals should not allow the perfect to become the enemy of the good."

"In particular, while the recommendation (12.1) to create a DNS Abuse advisory team without financial conflict of interest [emphasis in original] - who would set as priorities 'actionable data, validation, transparency, and independent reproducibility'- is worthy of consideration, there exist potential improvements to the usability/actionability of DNS Abuse reporting mechanisms which may nonetheless require concessions in terms of independent reproducibility. The GAC would urge the Board to consider the use case of Bulk Registrant Data Access ('BRDA'), access to which could enable ICANN researchers to improve their DNS Abuse reporting granularity to the level of Registrar/Registry operator (as sought by 12.3), by mirroring all future contracts to the language recently adopted in Verisign's .com RA provision.[10] This language specifically allows for ICANN to use BRDA data to 'analyze the operational stability of the DNS'. Granting ICANN research staff broad access to BRDA data would enable them to overcome existing rate-limits to WHOIS lookups, which have thus far made registrar/registry specific reporting (12.3) infeasible. While external researchers who would seek to confirm the validity of ICANN reporting would still potentially be constrained by such rate-limits, the 'actionability' of registrar/registry specific abuse reporting could reasonably be seen to be of such importance as to supersede the concerns of 'independent reproducibility' in this specific use case."

"Further, the GAC recognizes that seeking to provide greater transparency and non-commercial sharing of the source data behind ICANN's DNS Abuse reporting (12.2) may require nuance and compromise when obtaining the rights to share such data non-commercially. Specifically, the source data is understood to be commercially valuable only for a limited time, but valuable for ICANN DNS Abuse analysis and reporting indefinitely. If the data providers were to agree to contracts enabling non-commercial sharing of their data feeds, but only after a set delay, this would be viewed by GAC as an acceptable compromise (e.g. if the data providers and ICANN agreed to non-commercial sharing after a delay of 30 days from the date the data was obtained by ICANN). The GAC agrees that Contracted Parties should be recognized for their efforts to fight DNS Abuse (12.4), and that published reports of the actions taken (such as metrics on time-to-response to abuse reporting) are valuable, and would provide such Contracted Parties with a platform to highlight their contributions and successes. Finally, the GAC considers that Recommendation 12 could further specify actions foreseen under Draft Recommendation 13.1.4, i.e. assistance activities to the Board and all constituencies in interpreting Domain Abuse Activity Reporting (DAAR)."

BC highlights Recommendation 12 as "top priority."

RrSG offers the following comments:

- 12.1. "ICANN already operates the DAAR, and it is not clear what limitation or oversight this recommendation intends to address. Without identifying the specific

[10] .COM Registry Agreement Appendix 5A Registration Data Publication Services Specification, section 2.1 https://itp.cdn.icann.org/en/files/registry-agreements/com/com-appx-05a-pdf-27mar20-en.pdf

deficiencies, the Review Team should not instruct ICANN to spend significant money to accomplish unidentified goals. The RrSG recommends that the ICANN Board reject this recommendation."

- 12.2: "It is not clear what issue this recommendation is attempting to address. Before recommending changes to the DAAR, the Review Team should specify the exact problems it is trying to address. Additionally, there is potentially a significant amount of personal and/or confidential data within the DAAR, and it is not clear to the RrSG how the data sharing contemplated in this recommendation will comply with applicable privacy laws in California, the EU, and elsewhere. The RrSG is also concerned how ICANN will offset the cost of this service, as this recommendation implies the use of the data at no cost."
- 12.3: "To the extent that a registrar or registry receives a notice of breach regarding abuse, then this information can be reported by ICANN Contractual Compliance publicly. Otherwise, this recommendation includes a number of unresolved questions: how will abuse be measured? What abuse will be measured? How is 'most contribute' defined? What harm should be considered? The recommendation also implies that the domains belong to registries or registrars, rather than the registrants who use the services and then host a domain name elsewhere. There is also a concern that such 'naming and shaming' will lead to contracted parties gaming their numbers to not appear on the list, and further ostracize contracted parties from participating in DNS abuse mitigation issues and ICANN in general."
- 12.4: "It is not clear how ICANN should implement this recommendation. If through the ICANN Compliance process, then this will have a chilling effect on the forthright collaboration registrars and registries in the Compliance Process unless the reported data is 100% anonymized. Part of this obligation (in response to applicable laws) is outside of ICANN's remit. As this recommendation is overly broad, outside of ICANN's remit, and could reduce overall compliance, the RrSG recommends that the ICANN Board reject this recommendation."

ALAC indicates "strong support" for Recommendation 12.

IPC "is supportive of this recommendation. The IPC further notes that ICANN org should look to other sources of information relating to DNS abuse such as governments, industry trade groups and individuals."

Recommendations 13.1 – 13.2: Increase Transparency and Accountability of Abuse Complaint Reporting

RySG "has serious concerns about the quality of the output of the proposed solution. Any such reporting system would need to include a process to qualify the accuracy and legitimacy of the complaints submitted before they are passed on for required action by Contracted Parties or aggregated and published in a report."

M3AAWG notes: "Our members on either end of the process are affected by issues with the current abuse reporting approach. Contracted parties receive large volumes of misdirected abuse reports, while complainants report that reactions, time lines, and responses are inconsistent. By providing a centralized system, the former can be reduced, while the latter could be made more transparent…M3AAWG welcomes the proposed streamlining of abuse complaint processes as outlined in SSR2 Recommendation 13."

Article 19 "welcome[s] the recommendation, but recommend[s] reviewing the data collection process to ensure that only the necessary and minimum available data (excluding personally identifiable information) is collected prior to increasing transparency and accountability of this data. Additionally we would recommend redrafting the recommendation to ensure that once the data collection that this data in the portal is accessible to academic and security researchers."

INTA offers the following comments:

- 13.1: "INTA strongly supports this recommendation, including its proposed High priority level. INTA notes that this type of system could be leveraged for an eventual, standardized system for access to non-public domain name registration data (and both systems could leverage existing ICANN reporting systems such as the Centralized Zone Data Service [CZDS] to minimize build costs and timelines). INTA members have noted that it can often cause delay and confusion when DNS abuse reports must be provided to individual registry or registrar points of contact, which are often difficult to find especially for contracted parties operating in languages other than those of the reporting party."
- 13.2: "INTA strongly supports this recommendation, including its proposed High priority level. Additional public data regarding DNS abuse reports and related complaints (e.g. Compliance complaints) will be helpful in increasing transparency and accountability of contracted parties and ICANN in its oversight role."

Namecheap states: "Recommendation 13 proposes a central abuse complaint processing system for the entire Internet. Without considering the likelihood of abuse of such as system (registrars and registries are already inundated with spurious and unsupported abuse complaints), the proposed system contemplates integration with ccTLDs (which are outside of ICANN's mandate), and fail to include an integral component of the Internet ecosystem that is best positioned to address abuse: hosting providers. The biggest concern about this system is the likely cost. ICANN Org recently estimated that the cost to create the Standardized System for Access/Disclosure (SSAD) as recommended by EPDP Phase 2 is approximately $9 million. The SSAD is projected to cost an additional $9 million annually to operate (which should be paid for by the SSAD users in a cost recovery manner). It is quite possible that the proposed abuse complaint system will cost more than the already substantial SSAD estimates- and the SSR2 Final Report fails to contemplate the source of funds for these initiatives. As the vast majority of ICANN's budget is ultimately paid for by domain name registrants, Namecheap recommends that the ICANN Board reject any of the recommendations that will result in significant costs to ICANN."

GAC "strongly supports the creation of a centralized DNS Abuse complaint portal capable of automatically routing all abuse reporting to the relevant parties. While the GAC would be supportive of ICANN org taking responsibility for such a system, and thereby collecting directly the non-personally identifying metadata and complaint category data associated with such reporting, the GAC is aware that other organizations seeking to contribute toward the fight against DNS Abuse have shown interest in the creation of similar tools. Therefore as long as the tools are easy to locate, use, and are adopted readily by all gTLD contracted parties, and generate independently verifiable reporting based on complaints received, the GAC is agnostic as to the party operating such a complaint portal."

BC highlights Recommendation 13 as "top priority."

RrSG offers the following comments:

- 13.1: "Other than spending a substantial amount of money, it is not clear what this recommendation is attempting to accomplish. There are already existing contractual obligations for accepting abuse complaints for registrars and registries, and if third parties are not able to submit abuse complaints, then they should report the noncompliance to ICANN Contractual Compliance. Any automated system has the potential for abuse - even ICANN Compliance complaints that are reviewed by a human before processing are sometimes deficient. Additionally, this proposed system will involve a number of non-contracted parties: hosting providers, registrars accredited for ccTLDs (but not gTLDs), etc. Why this should be fully funded by ICANN, and the source of this funding, is not adequately explained. 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."
- 13.2: "The RrSG recommends that the ICANN Board reject recommendation 13.1, so this recommendation is superfluous."

ALAC indicates "strong support" for Recommendation 13 and believes it is "a necessary companion to … Recommendation 10."

Recommendations 14.1 - 14.5: Create a Temporary Specification for Evidence-based Security Improvements

RySG "does not object to Recommendation 14.2. ICANN does not currently provide registries with the lists of domains that it identifies using DAAR and believes it to be a sensible recommendation that could be a valuable tool to provide contracted parties more data and better enable us to identify alleged DNS Abuse. The remaining items in Recommendation 14 must be rejected as they would violate the terms of the Base gTLD Registry Agreement (the 'Registry Agreement') that govern how temporary policies/specifications may be utilized by ICANN."

Further, RySG notes "Recommendation 14 fails to meet the requirements for temporary specifications contained in the Registry Agreement and the Registrar Accreditation Agreement in fundamental ways:
(1) The Recommendation fails to meet the requirement that a temporary specification be as 'narrowly tailored' as feasible to achieve its defined purposes; and
(2) Temporary Specifications must address an immediate need to preserve the Security or Stability of the DNS and not be used to undermine cross Community discussions on longstanding policy issues."

PIR states that Recommendation 14 is "not consistent with the terms of the Registry Agreement. Recommendation 8 violates several provisions of the Registry Agreement. Section 7.7 of the Registry Agreement allows for the bilateral negotiation of a contemplated change to the Registry Agreement between Registries and ICANN itself, but not third parties that are not a party to the Agreement. The Registry Agreement does provide for the possibility of a 'Working Group' participating in these negotiations. Only Registries make such an

appointment.[11] Further, the Registry Agreement explicitly states that there are no third-party beneficiaries to the Registry Agreement.[12] Recommendation 14 violates the terms of the Registry Agreement that govern how temporary policies/specifications may be utilized by ICANN.[13] In addition, the terms Stability and Security are not amorphous or generic concepts in the Registry Agreement, but rather are defined terms.[14]"

M3AAWG states: "ICANN policy needs to be created around the issue of DNS abuse, clarifying expectations, requirements, and processes. As noted previously, a small number of actors is associated with the majority of security-related registrations. Defining clear policies would lead to a clearer playing field where all relevant actors are aware of, and can pursue the same objectives. While a temporary specification is not ideal, it is an appropriate stop-gap measure…M3AAWG concurs that ICANN policy needs to be created around the issue of DNS abuse, clarifying expectations, requirements, and processes."

Tucows "supports SSR2's commitment to evidence-based improvements but is not clear on why a Temporary Specification is recommended rather than a standard PDP. The SSR2 does not make clear why this might be an emergency of the type envisioned by the IANA transition team; in the absence of such clarity, a standard PDP is the appropriate choice. Furthermore, the Tucows family of registrars notes that DNS Abuse has objectively decreased, as evidenced by data collated and published by ICANN itself as 'Identifier Technology Health Indicator' metrics. The SSR2 does not take this into account, which unfortunately detracts from the good recommendations it has. Any policy work relating to DNS Abuse would benefit from a clear Issues Report and should be approached as a standard PDP; a Temporary Specification and expedited process are neither required nor appropriate in this context."

GNSO Council notes with regard to Recommendations 14.1 and 15.1: "The GNSO Council does not consider itself the appropriate body to opine on creation of a Temporary Specification, as the determination of whether the criteria for such a measure has been met is solely the responsibility of the ICANN Board. However, the follow-on required formation of an EPDP does directly impact the GNSO, and one that is a decision made by only the GNSO Council."

"The GNSO Council asks the ICANN Board to consider present and near-term demands of other policy work on the ICANN Org, staff, and larger ICANN community."

"Further, the GNSO Council takes note of in-flight activities around the topic of DNS Abuse. The GNSO Council requests that if activities continue forward regarding this topic, that future

[11] See .ORG Registry Agreement Section 7.6, "'Working Group' means representatives of the Applicable Registry Operators and other members of the community that the Registry Stakeholders Group appoints, from time to time, to serve as a working group to consult on amendments to the Applicable Registry Agreements." https://www.icann.org/sites/default/files/tlds/org/org-agmtpdf-30jun19-en.pdf

[12] .ORG Registry Agreement, Section 7.8, https://www.icann.org/sites/default/files/tlds/org/org-agmt-pdf-30jun19-en.pdf

[13] .ORG Registry Agreement, Specification 1, Section 2, https://www.icann.org/sites/default/files/tlds/org/org-agmt-pdf-30jun19- en.pdf

[14] As stated in the .ORG Registry Agreement, Section 7.3: "[A]n effect on "Security" shall mean (1) the unauthorized disclosure, alteration, insertion or destruction of registry data, or (2) the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards.

work be positioned in a planned manner versus the reactive, unplanned activities the GNSO are experiencing today."

Namecheap notes "the recommendations in the SSR2 Final Report appear to be made without any consideration of cost to ICANN. At the very least, the abuse incentives contained in Recommendation 14 are not presented in a revenue-neutral manner- ICANN is left to determine how to pay for the recommendation… As the vast majority of ICANN's budget is ultimately paid for by domain name registrants, Namecheap recommends that the ICANN Board reject any of the recommendations that will result in significant costs to ICANN."

GAC states: "While the GAC has not yet taken a view on whether or not a Temporary Specification is necessary to accomplish the goals set forth in Recommendation 14, it nonetheless wishes to flag constructive specific recommendations contained therein."

"The GAC in particular stresses the importance of urgent action on those security improvements-related recommendations, calling for concrete de-accreditation steps based on observable conduct and for creating incentives for DNS Abuse prevention and mitigation, in line with the ICANN org task as non-profit public benefit corporation to ensure oversight of DNS security, stability, and policymaking in the public interest."

"The GAC also notes that CCT Review Recommendation 12 also saw value in the financial incentivisation (SSR2 Recommendation 14.5) of contracted parties encouraging them to reach certain DNS Abuse milestones. Such financial incentives, of course, are only possible when there first exists a shared understanding of which domains within a contracted party's portfolio are perceived to be abusive (SSR2 Recommendation 14.2)."

BC highlights Recommendation 14 as "top priority."

RrSG makes the following comments:

- 14.1: "The ICANN Board should reject this recommendation as it is outside of the ICANN process, and specifically against the procedures for creating a Temporary Specification as specified in Section 2 of the Consensus and Temporary Policy Specification of the 2013 RAA. This recommendation fails to identify the background necessitating additional requirements on registrars and registries without their participation in creating such a Temporary Specification."
- 14.2: "The ICANN Board should reject this recommendation as it is not within ICANN's remit to police the Internet for abuse. If third parties have concerns or identify specific and verifiable cases of abuse, they should report them to the appropriate contracted party."
- 14.3: "In addition to recommending that the ICANN Board reject this recommendation, the RrSG is concerned that the Review Team recommends reviewing the veracity of data leading to abuse reports (that could ultimately lead to RAA or RA termination) AFTER the reports have been sent to the contracted party. Additionally, ICANN Contractual Compliance already has a robust abuse complaint process, so it is not clear why an additional process and system is required."
- 14.4: "The ICANN Board should completely reject this recommendation. It was created without the participation of the contracted parties, and appears to be significantly biased against contracted parties. It completely ignores the ICANN multistakeholder approach, existing ICANN Compliance processes, and it is not proper to use a Review Team to create such overbearing restrictions on contracted parties. Registrars and

registrars already conduct significant amounts of anti-abuse activities, OCTO reports show that abuse is decreasing, so this recommendation appears to be vindictive rather than collaborative."
- 14.5: "While the RrSG is generally supportive of such a framework, there are complex issues that need to be properly addressed. This includes how to ensure that any thresholds are not exploitable or subject to gaming by parties, and how to offset any revenue loss by ICANN."

ALAC indicates "strong support" for Recommendation 14 and notes it is "aligned with another oft-stated concern of the ALAC -- that ICANN must actively define and promote metrics for actions and inactions in the DNS, including those of contracted parties. ALAC also notes that this is another necessary element of the suite of recommendations dealing with DNS abuse."

Recommendations 15.1 – 15.2: Launch an EPDP for Evidence-based Security Improvements

RySG "objects to this recommendation set as it lacks a statement of what problem it is trying to solve. ICANN Org has produced DAAR as a means of informing the community of the apparent existence of DNS Abuse. There are other organizations that produce similar types of reports within the context of their own mission and purpose.[15]"

PIR states: "In line with our concern that Recommendation 14 would inappropriately create a Temporary Specification, PIR doesn't support the formation of a related EPDP. Not only does this recommendation not meet the requirements for an EPDP, it represents an attempt to bypass the existing policy development process."

M3AAWG states: "ICANN policy needs to be created around the issue of DNS abuse, clarifying expectations, requirements, and processes. As noted previously, a small number of actors are associated with the majority of security-related registrations. Defining clear policies would lead to a clearer playing field where all relevant actors are aware of, and can pursue the same objectives. An established consensus policy would be most useful for achieving this end…M3AAWG concurs with the SSR2 RT and recommends launching an Expedited Policy Development Process to create an anti-abuse policy."

Tucows believes "[a]ny policy work relating to DNS Abuse would benefit from a clear Issues Report and should be approached as a standard PDP; a Temporary Specification and expedited process are neither required nor appropriate in this context."

GAC "supports Recommendation 15 to develop an EPDP on anti-abuse policy and in particular of abuse, time-frames for contracted party actions like abuse report/response report timelines, and ICANN Contractual Compliance enforcement actions in case of policy violations. In line with this Recommendation, the GAC stresses the importance for ICANN org to insist on the power to terminate contracts in the case of a pattern and practice of harboring or ignoring abuse by any Contracted Party."

BC highlights Recommendation 15 as "top priority."

[15] The APWG has been producing a Phishing Activity Trends Report every quarter https://apwg.org/trendsreports for many years.

RrSG offers the following comments:

- 15.1: "The RrSG does not support this recommendation. There is no need for an EPDP regarding abuse. The only difference between a PDP and an EPDP is that an EPDP does not have an issues report. Otherwise, and EPDP does not operate 'faster' than a normal PDP. As the RrSG disputes that any PDP regarding abuse is necessary (because no issues to be resolved have been clearly and articulately identified, as well as defined goals), it is imperative than any abuse PDP start with an issues report, and only then can the GNSO Council determine whether a full PDP is necessary to address the specific issues."
- 15.2: "In addition to reiterating that the ICANN Board should reject the proposed EPDP for the reasons above, the community does not get to define how contracted parties operate. That is subject to negotiation between ICANN and the contracted parties, and limited to within ICANN remit. These proposals are outside of ICANN's remit. There are also existing structures and processes to terminate registrars and registries in the RA/RAA, no need for additional (and subjective rather than objective) methods of termination. Additionally, conducting updates every two years can be a significant community burden, and further exceeds the community's role (e.g. only ICANN and the contracted parties negotiate the contracts). Finally, making the requirements binding within 45 business days completely ignores the realities of operating a registrar or registry, and the significant resources required to make such substantial changes in a short timeline that will remove resources from supporting core business functions (e.g. provision of domain name registration services to customers)."

ALAC indicates "strong support" for Recommendation 15 and notes it is "aligned with another oft-stated concern of the ALAC -- that ICANN must actively define and promote metrics for actions and inactions in the DNS, including those of contracted parties. ALAC also notes that this is another necessary element of the suite of recommendations dealing with DNS abuse."

Recommendations 16.1 – 16.3: Privacy Requirements and RDS

RrSG notes: "As noted in our comments to Recommendation 9 and in our comments to the Draft Report, any recommendation regarding ICANN's Compliance functions should be linked to specific contractual terms and tied to a specific problem statement. We also reiterate that ICANN's Compliance team does not need to be reminded to generally enforce contracts with Registries and Registrars."

"In particular, 16.3 suggests that ICANN Compliance should audit Registry and Registrar compliance with a Registry or Registrar's own internal policies and procedures as opposed to its contractual obligations with ICANN. Such a recommendation exceeds the scope of ICANN Compliance's role to enforce contractual requirements."

GAC "considers that Recommendation 16 should specify clearly the need for balancing GDPR-type privacy considerations with the need to ensure access to non-personal data in line with the efforts under EPDP phase 2.A to ensure appropriate access to WHOIS registration data. Furthermore, the GAC considers that Draft Recommendation 16.2 (institutionalizing training and certifications for all parties in measuring, tracking, detecting, and identifying DNS Abuse) is an important awareness- building channel that could contribute

to a common understanding of issues related to DNS Abuse; as such, it would have merited a place in the final report."

RrSG offers the following comments:

- 16.1: "This recommendation attempts to override an existing ICANN initiative (ITI). As the ITI has been in process for a number of years, and is currently focusing on high volume and high priority items, the ITI should be allowed to continue its existing timeline as the Review Team has not provided any rationale for why RDS data should be prioritized over other action items in the ITI."
- 16.2: "The ICANN Community should not be able to dictate the composition, scope, and function of ICANN Contractual Compliance. It is an independent department within ICANN and should remain that way. Additionally 'privacy requirements' are outside of ICANN Contractual Compliance's limited contractual scope. Finally, it is not the role of ICANN (or ICANN Contractual Compliance) to facilitate law enforcement needs. The RrSG recommends that the ICANN Board reject this recommendation."
- 16.3: "Along with the rest of this recommendation, this is outside of ICANN's scope. ICANN is not a DPA, and the audit would need to cover a number of countries and jurisdictions around the world, and it is unclear how ICANN has the expertise or resources to conduct such an audit. As with many other recommendations in this Final Report, it is not clear what issue this recommendation intends to resolve."

ALAC indicates "strong support" for Recommendation 16.

Recommendations 17.1 – 17.2: Measuring Name Collisions

RySG notes: "The Final Report mentions the work of the Name Collision Analysis Project (NCAP) but fails to explain how that work is distinct from what is being proposed by this recommendation. While the RySG is supportive of the NCAP work, as noted in the overarching comments, we cannot support recommendations that repeat or represent significant overlap with other active work. Absent a clear and compelling problem statement, we urge the Board to reject this recommendation."

Article 19 states "While we welcome the recommendation, we urge that the section is redrafted so that it is not in contradiction with the recommendations outlined under the GNSO New Subsequent Procedures Draft Final Report. We specifically note that the recommendation heavily relies on the Name Collision Analysis Project (NCAP) Studies I without reference to the rest of the ongoing work carried out by the NCAP studies group including NCAP Studies II and III… We would thus like to recommend that recommendation 17 is revised to note that measuring name collisions should be carried out under the ongoing framework pending full completion of the work carried out by the NCAP studies group."

GAC "appreciates the SSR2 Review's highlighting of DNS Name Collisions as a significant security concern, and supports recommendation 17's request for a clear policy for avoiding gTLD-related name collisions to be implemented prior to further gTLD expansion."

ALAC "agrees emphatically with… Recommendation 17, on the avoidance of name collisions, which is particularly important for a diverse, global user base. During the 2012 New gTLD round, ICANN was somewhat taken by surprise with regard to name collisions and cannot afford for that to happen again."

IPC "notes that this recommendation appears to overlap with both the outputs from SubPro on Name Collision, and the Board's recent resolution requesting the second NCAP study."

"The IPC has diverse opinions on Name Collision. The IPC supports a gating mechanism for high risk strings. Some in the IPC support maintaining the existing Controlled Interruption. Others in the IPC support the NCAP and SubPro IRT working in tandem to develop a new mechanism to prevent name collisions."

Recommendations 18.1 – 18.3: Informing Policy Debates

RySG states: "In much the same way that ICANN monitors and offers neutral summary reports on legislative developments and identifier technology issues, it is reasonable for ICANN to do so for other topics related specifically to ICANN's mission and scope. However, it is unclear how recommending that ICANN offer an interpretation or analysis (including proposing additional studies) of these third-party efforts by specifically targeting only one part of the ICANN community is within either the Review Team's scope of work or ICANN's."

RrSG offers the following comments:

- 18.1: "ICANN Org should determine which staff attends or participates in research, networking, and security conferences on behalf of ICANN Org, and how to report and/or share this information with the ICANN Community- not a Review Team. Utilizing this information to influence contracted party behaviour is outside of ICANN's remit, and the ICANN Board should reject this recommendation."
- 18.2: "As repeated elsewhere, contract negotiations are between contracted parties and ICANN as detailed in the RAA and RA, and are not subject to public discussion and feedback from the ICANN community, including recommendations from peer-reviewed literature."
- 18.3: "The RrSG recommends that the ICANN Board reject this recommendation, as it is not clear how the studies will be paid for, and how confirming peer-reviewed studies are beneficial or within ICANN's remit."

ALAC "agrees emphatically with…Recommendation 18, informing policy debate, for which increased engagement, attendance to meetings, and mutual participation are recommended, with organizations such as the IETF, IEEE, ACM, ISOC, and many other national and regional bodies, including universities and research centers. ICANN needs to take an active role in bringing information into the policy debates from the I* and other organizations relevant to the work of ICANN."

Recommendations 19.1 – 19.2: Complete Development of the DNS Regression Test Suite

RySG states: "The report fails to explain why the development of the DNS Regression Test Suite is a requirement of ICANN Org. Similar to the context for Recommendation 18, it is reasonable for ICANN to track and report on the behavior of DNS resolvers since they are a significant client of the DNS services that registries are required to support. However, the RySG considers making this an obligation or requirement of ICANN out of scope and objects to Recommendation 19."

i2Coalition believes that Recommendation 19 "seem[s] to be pushing ICANN into the realm of policing DNS protocols (19). This is a serious concern with recommendations that, once accepted by the Board, would…seem to expand ICANN's remit."

RrSG notes Recommendations 19.1 and 19.2 "are both outside of ICANN's remit, and it is also not clear how ICANN will pay for this."

Recommendation 20.1 – 20.2: Formal Procedures for Key Rollovers

ALAC "support[s] recommendation 20 on the key rollover, recommending further that the experience gained from the COVID-19 pandemic be carefully considered."

Recommendation 21.1: Improve the Security of Communications with TLD Operators

RySG "is supportive of enhancing security in the Root Zone System and efforts in that direction."

Recommendations 22.1 – 22.2: Service Measurements

RySG "strongly supports Recommendation 22."

Recommendations 23.1 – 23.2: Algorithm Rollover

Verisign notes: "While the report (p. 55) has outlined advantages and disadvantages of the hash-based family of signature algorithms under consideration by NIST, the relevant post-quantum cryptography specifications are still evolving. Indeed, the findings quoted have no corresponding recommendation. Although Recommendation 23, which appears immediately following the quoted statements, advises PTI operations to prepare for a rollover to a new signature algorithm, the recommendation leaves the algorithm unspecified. We encourage ICANN to continue to track developments without prematurely concluding for or against any candidate."

Crypto4A states: "Recommendation 23.1 identifies the need to prepare for the transition to some form of postquantum signature algorithm, but doesn't provide specific details regarding the likely timing of this transition, or potential candidate algorithm. Furthermore, current root and top-level domain DNSSEC practice statements[16] explicitly state the need to use Hardware Security Modules validated by NIST's FIPS 140-2/3 certification process. In the past NIST has discussed potential methods for transitioning from classical (e.g., RSA or ECDSA) to post-quantum algorithms in a FIPS-compliant manner via the use of a dual signature method that signs objects with both a post-quantum and a classical FIPS-compliant signature method[17]. This approach is intended to serve as a stop-gap until NIST's PQC

[16] For example: https://www.iana.org/dnssec/procedures/ksk-operator/ksk-dps-20201104.html

[17] Referenced as part of NIST's PQC FAQ at https://csrc.nist.gov/projects/post-quantum-cryptography/faqs

standardization process identifies, and standardizes, an appropriate PQC signature mechanism. If the dual signature method were considered for adoption by DNSSEC then it would lead to combined signature sizes on the same order as HBS (e.g., RSA4096 + Falcon Level 1 ≈ 512 + 666 = 1178 bytes whereas LM-HBS(h/w/n = 20/8/24) = 1144 bytes). This may help motivate further study/consideration of HBS-based techniques."

"Recommendation 23.2 highlights the complexities and difficulties associated with the DNSKEY algorithm rollover process. ICANN may want to consider looking at some of the key rotation mechanisms and concepts being proposed for decentralized key-management infrastructure (DKMI)."

Recommendations 24.1 – 24.2: Improve Transparency and End-to-end Testing for the EBERO Process

Section IV: Analysis of Comments

A comprehensive analysis of comments will be published in due course and appended to this document.